Pre-University Cyber Security Education: A report on developing cyber skills amongst children and young people

February 2022

Krysia Emily Waldock, Vince Miller, Shujun Li and Virginia N.L. Franqueira
Institute of Cyber Security for Society (iCSS), University of Kent, UK

GFCE

University of Kent | Institute of Cyber Security for Society (iCSS)

Preface

This report provides results from a research project about cyber security education and skills development for children and young people (up to the age of 18) in a pre-university setting. The research work was commissioned by the **Global Forum on Cyber Expertise** (**GFCE**, https://thegfce.org/), as a recently identified priority of the GFCE's **Working Group D: Cyber Security Culture and Skills**.

Traditionally, cyber security is often considered a topic that sits within more technological subjects, such as ICT (information and communications technology), computing or computer science, or informatics. However, for the wider cyber security community (researchers, practitioners, policy makers, etc.), cyber security has been increasingly recognised as a highly inter-disciplinary subject, covering knowledge areas such as risk management and governance (CyBOK, 2021a), cyber law and regulations (CyBOK, 2021b), human factors (CyBOK, 2021c), privacy protection and online rights (CyBOK, 2021d), and adversarial behaviours (CyBOK, 2021e). For the research conducted, we followed the inter-disciplinary approach to include a wide range of cyber security topics.

Some people and organisations use the term 'cyber security' to mean protecting computer systems (software, hardware and networks) and digital data, and use a different term, like 'online safety' (or other similar terms, such as 'cyber safety' or 'internet safety'), to mean protecting people when they are online or using computing systems. For this report, we consider online safety to be part of the broader definition of cyber security, since there are many overlaps between the two (e.g., protecting people often requires securing computer systems they use and personal data they share online, and many online safety solutions are effectively cyber security technologies). In other words, for this report, when we refer to 'cyber security education' only, we cover both online safety and the more narrowly defined cyber security education, but when we refer to 'online safety' we mean the 'protecting people' elements of the more broadly defined cyber security education. In some places, there is a need to refer to the more technical, narrowly defined cyber security education separately to online safety education. Therefore, we sometimes use 'cyber security' and 'online safety' together, where the former refers to the narrower definition of cyber security.

In terms of education, we consider not just formal educational activities at schools and other types of pre-university educational institutions (e.g., A-level colleges in the UK and pre-university vocational colleges in many countries), but also extra-curricular activities designed for and participated in by children and young people. This enlarged scope is important especially for countries where cyber security has not been made a mandatory part of formal education activities in pre-university settings. In addition, many extra-curricular activities are led, organised, guided, supported, or encouraged by school teachers, staff, sometimes officially by educational institutions themselves and mostly with support of external helpers, as an important supplement to the formal education provided by following official curricula. Note that some extra-curricular activities are self-organised efforts of pupils and/or parents, which can be considered supplementary 'home' education that helps enlarge what pupils learn at school or other pre-university educational institutions. Therefore, for the research conducted, we looked at such 'home' educational activities, too.

Our research was conducted in the following three stages:

- **Stage 1**: a **systematic literature review (SLR)** to get a more in-depth understanding of the research literature on pre-university cyber security education;

- **Stage 2**: **desk research** on gathering relevant **public information** on the internet, focusing on related policy documents, projects, initiatives and events in 13 selected countries, from a wide range of relevant organisations in both public and private sectors, including some important international and multi-national organisations;
- **Stage 3**: a number of **semi-structured interviews** with 21 interviewees from 11 countries (out of the 13 studied in Stage 2) and three additional interviewees from the UN agency ITU (International Telecommunication Union), for confirming information we collected from the first two stages and gathering more information directly from key experts.

Results from Stage 1 are reported in a separate document (Sağlam et al., 2021), and this report focuses more on results from Stages 2 and 3. Our key findings and recommendations in the last section of this report, and the executive summaries, are drawn based on the results from all three stages.

Based on the results and key findings of the reported research work, we have started some follow-up research activities, including an online survey organised jointly with SWGfL and Bitdefender to gather more information about cyber security educational activities at schools in the UK.

We hope that you will find the report useful. You are welcome to contact us to discuss the content of this report and the SLR document, our future research work, or explore collaboration in this important topic. Our contact details can be found at the end of this preface.

We also hope the key findings and recommendations in the report can help stimulate more discussions on pre-university cyber security education, and that some positive actions and new initiatives will be taken by relevant stakeholders as a consequence of reading this report. We are keen to hear about impacts of the report, so please inform us via the email address at the end of the preface if you find the report useful or decide to take actions based on the key findings and recommendations given in the report.

With best regards,

Krysia Emily Waldock, Vince Miller, Shujun Li and Virginia Franqueira (report contributors)

School of Computing & Institute of Cyber Security for Society (iCSS) (Franqueira and Li)
School of Social Policy, Sociology and Social Research & Institute of Cyber Security for Society (iCSS) (Waldock and Miller)
University of Kent, Canterbury, Kent, UK

https://cyber.kent.ac.uk/

cyber-info@kent.ac.uk

February 2022

Acknowledgements

First of all, the work would not have been possible without continuous support from the Global Forum on Cyber Expertise (GFCE). In addition to providing the research funding for the project, many people from the GFCE, especially those on the general secretaria and the Working Group D, helped provide feedback, participate in discussions, and connect the research team with people and organisations who could help provide useful information or act as interviewees. Particularly, we would like to thank the following three individuals for their continuous help throughout the project:

- Kathleen Bei, Advisor and Facilitator of Working Group A on Cybersecurity Policy and Strategy, GFCE Secretariat
- Giouli Lykoura, Advisor and Facilitator of Working Group D on Cyber Security Culture & Skills, GFCE Secretariat
- Tereza Horejsova, Chair of Working Group D on Cyber Security Culture & Skills, GFCE / Director of Project Development and Partnerships, DiploFoundation

In addition, the authors of the report would like to thank the 24 interviewees who participated in the semi-structured interviews in Stage 3 of the project's research work. Their knowledge and expert opinions on pre-university cyber security education in different areas helped consolidate our understanding from Stages 1 and 2, and provided direct input for many parts of the report. Many of the interviewees also helped proofread an earlier version or versions of this report. Their feedback helped improve the completeness and accuracy of the content of the report, including but not limited to accuracy of their direction quotations. For a full list of all the 24 interviewees with their name, role and affiliation, please see Appendix A of the report.

Many other people and organisations helped the project team in different ways, e.g.. providing useful information and advice, recommending and helping connect with potential organisations and interviewees, and providing feedback on the final report of the project. Some expressed the willingness to be interviewed, but the project team could not arrange an interview due to the limited duration of the project. Some provided useful information, but it was too late for the project team to include it in the report. The project team thank all of them for their help and support.

Last but not the least, the project team would like to thank many of their local colleagues at the Institute of Cyber Security for Society (iCSS) and the University of Kent, who provided help on different matters, including but not limited to project management and general discussions that helped inform the research. Particularly, we would like to thank Laura Medlock, the iCSS's Administration Officer, who helped proofread the final report.

Executive Summary

This report summarises research results from a research project, sponsored by the GFCE, on pre-university cyber security education in a global context. The research was conducted in three stages: a systematic literature review; desk research on gathering relevant public information on the internet; and a number of semi-structured interviews with sampled stakeholders. The results learned from the research led to the following key findings and main recommendations, which we hope can help stakeholders around the globe to improve cyber security education in a pre-university setting.

Key Findings

The key findings from our research can be summarised below:

- **Two main approaches to embedding cyber security and online safety content in the curriculum** were identified for countries covered in this report: content added as part of a technological subject area such as computing / computer science / ICT / (digital) technology, and content added to a range of non-technological subjects.
- For both approaches identified above, especially the first one related to more technological subjects, there tends to be **a lack of practical cyber security skills**, **a lack of security mindset** and **a lack of enough skill-set coverage built-in**, towards a cyber security related career path.
- There was a concern across the board regarding **lack of teacher training**, which led to **insufficient teacher skills** in delivering cyber security education with sufficient coverage. In addition, **teachers struggled with finding enough time** to cover cyber security content in class.
- For many countries studied, **multiple stakeholder organisations in different sectors** are active in different aspects of pre-university cyber security education, but as a result, their activities are **often fragmented** and tend to **operate quite disjointly**, and **confusion** could arise regarding which organisations should take the main responsibility on a particular matter, e.g., **standards** on pre-university cyber security education.
- **Economics has a direct impact** on pre-university cyber security education. Given limited resources, teaching more traditional subjects, including survival-focused skills, is often a higher priority than teaching cyber security skills.
- **Different levels of development/maturity of pre-university cyber security education** were identified among the countries studied (see Section 7.1 of the report for more details about the different levels).
- **A top-down approach to curriculum design is the norm** adopted across countries studied, whether this is in the formal education sector or by extra-curricular bodies.
- In some countries studied, even where a national cyber security curriculum is in place, **teachers and schools have a lot of control over what cyber security content they teach**. This creates **freedom and autonomy for teachers**, but there are often concerns about a **lack of direction**.
- There is a **perceived general lack of interest and awareness among children** in developing cyber skills and cyber security **as a potential career path**. One key problem is a **lack of diversity in terms of student enrolment in optional courses and training events**.

Main Recommendations

The following are main recommendations we would like to give to different stakeholders for better developing pre-university cyber security education in the future.

- For governments in countries and regions managing its own educational affairs: **setting up a national or regional steering body or working group with overall responsibility for cyber security and online safety education**, covering both pre-university stages and the higher education stage. See Section 7.2 of the report for what we believe such a body or working group can help achieve.
- For all stakeholders: **strengthening collaborations and communications between different sub-communities**, particularly those focusing on pre-university education, higher education, and cyber security profession; **setting up a single community-wide body covering all stages (per-university ones and higher education) of cyber security education**, which will help avoid gaps between different stages.
- For organisations setting school curricula and/or qualification standards: **embedding cyber security and online safety skills more widely across school curricula, qualification and exam specifications**. This will help enhance the cyber security skills among more pupils and raise awareness more widely throughout the curriculum, and to address the diversity issue in a longer term.
- For all stakeholders: **making more effort to attract more young people to cyber security education**, especially from **less-covered and 'non-traditional' groups** (such as girls, ethnic minorities, and pupils from low income backgrounds). This will help create a more diverse knowledge and skills pipeline in different professions where cyber security plays a role (not just the more technical cyber security profession).
- For all stakeholders: **covering different aspects of cyber security and online safety education more systematically beyond pure technology-centric content**. The following **six broad aspects of content related to cyber security and digital literacy education** can help as a systematic categorisation scheme of the different aspects: technological awareness, procedural awareness, data awareness, identity awareness, socio-cultural awareness, and consumer awareness.
- For organisations setting or participating in setting school curricula and/or qualification standards: **designing school curricula and qualification standards on cyber security and online safety by incorporating a more bottom-up (participatory) approach**, engaging with **a wider range of stakeholders**, including parents, legal guardians, carers, school teachers and staff, and employers with a need of cyber security workforce.
- For stakeholders conducting or funding cyber security, online safety and/or education-related research and innovation activities: **conducting and funding more research that can help inform policy makers and educators about how to better conduct pre-university cyber security and online safety educational activities**, following **a participatory (co-creation) approach to engage with a wider range of stakeholders**, especially pupils, parents and legal guardians, school teachers and staff, who can then contribute actively throughout the process. See Section 7.2 of this report for some concrete example research and innovation activities related to this recommendation.
- For solution providers and other stakeholders: **developing, encouraging, rewarding and adopting new innovative solutions to support cyber security and online safety educational activities**, where the solution development should involve **cross-sectoral collaboration** and **a participatory (co-creation) approach to engaging with end users**.

Table of Contents

List of Acronyms

The following list shows important acronyms used in this report (in alphabetic order).

- A-Level: Advanced Level (Singapore; UK)
- A.YCEP: Advanced YCEP (Singapore)
- ACARA: Australian Curriculum, Assessment and Reporting Authority
- A.C.E.S: Activities in Cybersecurity Education for Students (Australia)
- ACM: Association for Computing Machinery
- ACSC: Australian Cyber Security Centre
- ACT: Association for Citizenship Teaching (UK)
- AFA: Air Force Association (US)
- AMCA: Australian Communications and Media Authority
- AOC: Association of Colleges (UK)
- APWG: Anti-Phishing Working Group
- AQA: Assessment and Qualifications Alliance (UK)
- ASCL: Association of School and College Leaders (UK)
- BC: British Columbia (Canada)
- BCS: BCS, The Chartered Institute for IT (formerly known as British Computer Society)
- BTEC: Business and Technology Education Council (UK)
- CAS: Computing At School (UK)
- CCE: Character and Citizenship Education (Singapore)
- CCEA: Council for the Curriculum, Examinations & Assessments (Northern Ireland, UK)
- CCMP: Cybersecurity Career Mentoring Programme (Singapore)
- CCSSO: Council of Chief State School Officers (US)
- CDN: College Development Network (Scotland, UK)
- CEOP: Child Exploitation and Online Protection (UK)
- CEPIS: Council of European Professional Informatics Societies
- CERT NZ: National Computer Emergency Response Team New Zealand
- CIISec: Chartered Institute of Information Security
- CIRT: Computer incident response team
- CISA: Cybersecurity and Infrastructure Security Agency (US)
- CNCS: Centro Nacional de Cibersegurança (Portuguese National Cybersecurity Centre)
- COP: Child online protection (a standard term, but Child Online Protection is also the name of a programme of ITU)
- CoSP: Collaborative Social Programme (Singapore)
- CPD: Continuing and professional development
- CRC: Cyber Resillence Centre (UK)
- CSA Singapore: Cyber Security Agency of Singapore
- CSIRT: Computer security incident response team
- CTF: Capture the flag
- CW: Cyber Wellness (Singapore)
- CyBOK: Cyber Security Body Of Knowledge (UK)
- CYPCS: Children's and Young People's Commissioner Scotland
- DCMS: Department for Digital, Culture, Media and Sport (UK)
- DESE: Department of Education, Skills and Employment (Australia)

- DESI: Digital Economy & Society Index (EU)
- DIGI: Digital Industry Group Inc (Australia)
- DRWG: UKCIS Digital Resilience Working Group
- ECSC: European Cyber Security Challenge
- ECSO: European Cyber Security Organisation
- EEA: European Economic Area
- ENISA: European Union Agency for Cybersecurity
- ERO: Education Review Office (New Zealand)
- ESA: Education Services Australia
- ESCEI: Elementary School Cyber Education Initiative (US)
- ESEA: Elementary and Secondary Education Act (US)
- ESEE (Ε.Σ.Ε.Ε.): Hellenic Confederation of Commerce and Entrepreneurship (Εθνική Συνομοσπονδία Ελληνικού Εμπορίου) (Greece)
- ESFA: Education and Skills Funding Agency (UK)
- EU: European Union
- FCT: Fundação para Ciência e a Tecnologia (Foundation for Science and Technology) (Portugal)
- FIRST: Forum of Incident Response and Security Teams
- FLU: Funded Learning Unit (Northern Ireland, UK)
- FPB: Film and Publications Board (South Africa)
- GCA: Global Cybersecurity Agenda (ITU)
- GCHQ: General Communications Headquarters (UK)
- GCI: Global Cybersecurity Index (ITU)
- GCSE: General Certificate of Secondary Education (UK)
- GDPR: General Data Protection Regulation
- GFCE: Global Forum on Cyber Expertise
- GIAC: Global Information Assurance Certification
- GSO: Go Safe Online (Singapore)
- HASS: Humanities and Social Sciences (a learning area of the Australian Curriculum)
- HAVO: Senior general secondary education (The Netherlands)
- IAPS: Independent Association of Prep Schools (UK)
- ibid: ibīdem (used in citations to indicate that the previously cited reference is repeatedly used)
- ICC: (NICE) Interagency Coordinating Council (US)
- ICO: Information Commissioner's Office (UK)
- ICT: Information and communications technology
- ICTC: Information and Communications Technology Council (Canada)
- IFIP: International Federation for Information Processing
- ISA: Independent Schools Association (UK)
- ISC: Independent Schools Council (UK)
- $(ISC)^2$: International Information System Security Certification Consortium
- ISCED: International Standard Classification of Education
- ISTE: International Society for Technology in Education (US)
- IT: Information technology
- ITT: Initial teacher training
- ITU: International Telecommunication Union (UN)

- ITU-D: ITU Telecommunication Development Sector
- IWF: Internet Watch Foundation (UK)
- N5: National 5 (Scotland, UK)
- NASS: National Association of Independent Schools & Non-Maintained Special Schools (UK)
- NCA: National Crime Agency (UK)
- NCAP: National Cybercrime Action Plan (Singapore)
- NCCE: National Centre for Computing Education (UK)
- NCEA: National Certificate of Educational Achievement (New Zealand)
- NCES: National Center for Education Statistics (US)
- NCPF: National Cybersecurity Policy Framework (South Africa)
- NCPO: National Cyber Policy Office (New Zealand)
- NCSA: National Cybersecurity Authority (Greece), National Cybersecurity Agenda (The Netherlands), or National Cyber Security Alliance (US)[1]
- NCSC (used in Chapter 4 only): National Cyber Security Centre (UK)
- NCSC-NL: National Cyber Security Centre (The Netherlands)
- NCSC-NZ: National Cyber Security Centre (New Zealand)
- NCSC-UK: National Cyber Security Centre (UK)
- NCSI: National Cyber Security Authority (Greece)
- nd: no date (used in citations and references to indicate that a particular reference has no specified date or we could not identify the precise date)
- NETS: National Educational Technology Standards (US)
- NFER: National Foundation for Educational Research (UK)
- NGA Center: National Governors Association Center for Best Practices (US)
- NGO: Non-government organisation
- NI: Northern Ireland
- NICCS: National Initiative for Cybersecurity Careers and Studies (US)
- NICCY: Northern Ireland Commissioner for Children and Young People
- NICE: National Initiative for Cybersecurity Education (US)
- NICE Community: NICE Community Coordinating Council (US)
- NIST: National Institute of Standards and Technology (US)
- NPCC: National Police Cadet Corps (Singapore)
- NSA: National Security Agency (US)
- NSF: National Science Foundation (US)
- NSPCC: National Society for the Prevention of Cruelty to Children (UK)
- NZQA: New Zealand Qualifications Authority
- O-Level: Ordinary Level (Singapore)
- OADSI: Ontario Association of School Districts International (Canada)
- OCR: Oxford, Cambridge and RSA Examinations (UK)
- OECD: Organisation for Economic Co-operation and Development
- Ofcom: Office of Communications (UK)

[1] We decided not to introduce different acronyms for these organisations' names because in this report the acronym is always referred to in a clear national context so no confusion can arise. When necessary (e.g., in references), we add the country's name into a pair of parenthese to differentiate these bodies with the same acronym.

- Ofqual: Office of Qualifications and Examinations Regulation (UK)
- Ofsted: Office for Standards in Education, Children's Services and Skills (UK)
- ONS: Office for National Statistics (UK)
- PD: Professional development
- PD&MU: Personal Development and Mutual Understanding (Northern Ireland, UK)
- PfS: Partnerships for Schools (UK)
- PHE: Physical and Health Education (Canada)
- PHE-BC or PHE BC: Physical and Health Education in British Columbia (Canada)
- PRISMA: Preferred Reporting Items for Systematic Reviews and Meta-Analyses
- PSHE: Personal, Social and Health Education (UK)
- PTSIC: Portuguese Safer Internet Centre (Centro Internet Segura in Portuguese)
- RSB: Regional Strategic Body (Scotland, UK)
- S/CCI: Office for the Co-ordinator for Cyber Issues (US)
- SCQF: Scottish Credit and Qualifications Framework
- SFC: Scottish Funding Council
- SID: Safer Internet Day
- SLR: Systematic literature review
- SME: Small and medium-sized enterprise
- SQA: Scottish Qualifications Authority (Scotland, UK)
- STEM: Science, technology, engineering, and mathematics
- STEM-L: Science, technology, engineering, mathematics, and foreign language (US)
- SVRP: Student Volunteer & Recognition Programme (Singapore)
- SWGfL: South West Grid for Learning (UK)
- TEA: Texas Education Agency (US)
- TEKS: Texas Essential Knowledge and Skills (US)
- UK: United Kingdom (of Great Britain and Northern Ireland)
- UKCCIS: UK Council for Child Internet Safety
- UKCIS: UK Council for Internet Safety
- UN: United Nations
- UNESCO: United Nations Educational, Scientific and Cultural Organization
- UNICEF: United Nations Children's Fund
- US: United States (of America)
- VET: Vocational education and training
- VMBO: Preparatory vocational secondary education (The Netherlands)
- VWO: University preparatory education (The Netherlands)
- WJEC: Welsh Joint Education Committee (Wales)
- YCEP: Youth Cyber Exploration Programme (Singapore)

1. Introduction

This Section provides important information about the general background and several important contexts of pre-university cyber security education, explains the motivation of the research work that made the report possible, and at the end briefly introduces the structure of the rest of the report.

1.1. Digital experience of children and young people

Young people are using technology to access online resources more frequently and at progressively younger ages. While this is a global phenomenon (ITU, 2020a), let us use the UK as an example country to see what the digital age for children and young people looks like. According to recent statistics from Ofcom (2021), the UK's telecommunications regulator, 55% of 5-15-year-olds use social media (e.g., Facebook, Instagram, TikTok and Snapchat) and 97% use video sharing platforms. Even children as young as 3 and 4 years old use social media applications (18%) and instant messaging applications (20%) (Ofcom, 2021). This is in spite of many of these applications and platforms (including many of those listed above) requiring a minimum registration age of 13. Furthermore, according to 2021 statistics from the UK's Office for National Statistics (ONS), 89% of children aged 10-15 reported going online or using the internet at least daily (ONS, 2021).

In addition to the increasing use of the internet, the ownership of computing devices by children and young people has also been increasing. For example, according to the same 2021 statistics from the UK's Ofcom (Office of Communications), 48% of 3-4-year-olds have their own tablet and this figure increases to 61% for 5-15-year-olds, and 55% of 5-15-year-olds have their own smartphone (Ofcom, 2021). The high percentage of children and young people's ownership of computing devices has led to ubiquitous access to the internet (Smahel et al., 2020). This is especially pertinent with the overall internet usage being increased since the start of the COVID-19 pandemic (ITU, 2020a).

This ubiquitous access to the internet, coupled with advances in technology, provide plenty of entertainment and educational opportunities, such as watching live broadcast TV (56% of 5-15-year-olds), on-demand video content (91% of 5-15 year-olds) or playing games online (71% of 5-15-year-olds), according to the UK's Ofcom (Ofcom, 2021).

1.2. Online safety

While the use of the internet and computing devices benefit children and young people greatly, it also leads to online safety challenges caused by cyber crime and other forms of online harms. Many such risks are well known by parents and teachers, e.g., talking to strangers online; over-sharing personal information; sharing illicit content; accessing inappropriate content (including sexual content inappropriate for children and young people, and content that can lead to radicalization or anti-social behaviours); sexting; online fraud; identity theft; and exposure to cyber bullying. Recent statistics have repeatedly shown the severity of online safety issues for children and young people. For example, the UK's ONS recently reported that 29% of children aged 10-15 had accepted a friend request from someone they did not know and that roughly 11% of children aged 13-15 had reported receiving one or more sexual SMS messages in the last 12 months (ONS, 2021a). Some recent research also showed that children are more likely to have a bad experience online as they achieve adolescence, and

cyber threats such as misuse of data and malicious software appeared to be a risk in terms of children's wellbeing and safety online (Smahel et al., 2020). Many stakeholder groups (e.g., parents, teachers, schools) remain concerned about detection and prevention of online harms and cyber risks affecting children and young people.

Online safety risks occur despite many parents having some sort of involvement in their children's internet usage. According to the UK's ONS, 64% of children aged 10-15 had parent-set rules controlling their internet usage, and 85% of children aged 10-15 reported that their parents knew a fair amount or a lot of what they got up to online (ONS, 2021). Smahel et al. (2020) reported that parents were often the main source of support for children and young people when something went wrong online.

To address online safety risks, it is important that children and young people themselves also have the necessary awareness of such risks and the right knowledge about how to mitigate them. As shown later in this report, online safety education and awareness activities have been taking place in most countries, particularly in pre-university settings. In addition, there has been some evidence showing that children and young people do appear to have some level of awareness and knowledge. For instance, the UK's Ofcom found that 70% of surveyed children aged 12-15 are aware of mechanisms for reporting inappropriate and illicit online content (Ofcom, 2021). Despite the good level of awareness, the Ofcom report also found that only a small minority (14%) of the surveyed children had ever reported inappropriate or illicit content, indicating that most children do not actively leverage their awareness and knowledge to help protect themselves and others from online harms. In order to improve the situation, online safety education for children and young people still needs strengthening.

1.3. Cyber security capacity building

In addition to the need for online safety education, the ubiquitous use of the internet and computing devices by people of all ages and organisations of all kinds calls for wider and more in-depth cyber security capacity building beyond simply protecting against online harms. Such cyber security capacity can not only help protect computer systems and organisations from cyber attacks, but also help provide better tools that can protect people, including children and young people, more effectively and efficiently in the cyber space. In the context of cyber security capacity building, there are two relevant phenomena happening worldwide.

First, there is a widely reported shortage of cyber security professionals to fulfil market demands. For instance, a recent study commissioned by the UK's Department for Digital, Culture, Media & Sport (DCMS, 2021a) estimated an annual cyber security workforce gap of around 10,000 in the UK alone, and it predicted that this gap would likely worsen since demand has consistently exceeded supply between 9-14% since 2016. Similarly, International Information System Security Certification Consortium or (ISC)², an international cyber security professional certification body, conducted a study with 3,790 of its member organisations based in Europe, North America, Latin America and the Asian-Pacific region in 2019, and estimated an overall cyber security workforce gap of around 3.12 million globally ((ISC)², 2020). Cyber security education from a young age would obviously help attract more children and young people to consider a cyber security career pathway, therefore helping address the global cyber security capacity gap.

Second, although being a more technical subject in its early years, it has been increasingly acknowledged that cyber security is a highly inter-disciplinary subject, e.g., see the definition of cyber security in the Cyber Security Body Of Knowledge (CyBOK) developed by the UK's National Cyber Security Centre (NCSC-UK) (CyBOK, nd). Socio-technical aspects of cyber

security, such as risk management and governance (CyBOK, 2021a), cyber law and regulations (CyBOK, 2021b), human factors (CyBOK, 2021c), privacy protection and online rights (CyBOK, 2021d), and adversarial behaviours of malicious entities (people, criminal groups and organisations) (CyBOK, 2021e), are very important for any technical cyber security solutions to work in the real world. Therefore, cyber security awareness (e.g., security implications of smart 'things') and socio-technical aspects of cyber security have become increasingly important for a wide range of professionals in different career paths, e.g., healthcare, engineering, law enforcement, and finance. However, relevant inter-disciplinary cyber security skills have not been embedded into most university courses of wider subjects, and adding such skills to university courses is not likely to happen in the near future. Therefore, it becomes important to expose children and young people to cyber security knowledge and embed cyber security-oriented thinking (e.g., threat modelling and risk mitigation) in per-university education to better equip them for the future, regardless of their choices of career path and their personal interests.

1.4. Cyber security education

In the previous sections, we have shown it is necessary and important to offer children and young people online safety and cyber security education from a young age. As mentioned in the preface, traditionally, cyber security is regarded as a topic that fits within more technological subjects such as IT (information technology) and ICT (information and communications technology), computing or computer science, or informatics. As shown later in this report, key terms used in such related subjects vary across countries and regions. For instance, some relevant cyber security skills may be covered as part of 'digital skills' or 'online safety' education. Some of the commonly used related terms and their definitions are summarised below:

- **Cyber security (narrow sense):** This refers to protection of systems, devices, data, networks. Similar (and often even narrower) terms include information security, computer security, data security, network security, systems security.
- **Online safety:** This refers to protection of people, especially self. Equivalent terms include internet safety, e-safety, cyber safety, and digital safety.
- **Cyber security (broad sense):** This refers to both cyber security (narrow sense) and online safety as listed above.
- **Related terms used within technological subjects:** Different countries and regions name their computing-related subjects with different terms, e.g., computing, computer science, digital skills, digital literacy, ICT, IT, informatics. Cyber security relevant content may be embedded into different topics within these subjects, such as programming, software engineering, and computer networks. When referring to such subject names, we will use 'Computing' more generally and the more specific term chosen by a specific country or region.
- **Related terms used within non-technological subjects**: As made clear later in this report, online safety education is often taught in the context of protecting children and young people from online harms such as cyber bullying and online sexual abuse, so terms such as privacy, behaviour, citizenship, wellbeing, (mental) health, and sexual education are often used in less technological subjects to cover online safety and cyber security education. Some countries and regions choose to use even broader terms, e.g., those used in the UK for education on Personal, Social, Health and Economics (PSHE). In addition, the term 'media literacy' is also frequently used mostly in the

context of mis- and dis-information online, but sometimes also used to refer to the cover broader online safety issues, especially those related to mis- and dis-information online (DCMS, 2021c).

As explained in the preface, for our research we cover cyber security in the broad sense, and will use the term 'cyber security' in both its narrow and broad senses – which one we are following is normally self-explanatory based on the context, e.g., when we use the term alone it refers to the broader sense, and when we use the phrase 'cyber security and online safety' this term has a narrower meaning. This mixed use of terms is important to cover the diverse terms, different levels of cyber security related education, and overlaps between cyber security and online safety related education in different countries and regions.

1.5. Education in a global context

In order to better understand how cyber security education is embedded in pre-university education worldwide, it is vital to understand the various education systems in different parts of the world and how they are to be compared. Particularly, the names and the age ranges of different pre-university educational stages often differ between countries and cultural contexts. For our research, we opted to use two important benchmarks concurrently when discussing school years and ages.

The first benchmark is the ISCED (International Standard Classification of Education) levels, defined by the Institute of Statistics of the UN (United Nations) agency UNESCO (United Nations Educational, Scientific and Cultural Organization) (UNESCO, 2011). It describes the five standardised stages of pre-university education, as shown in Table 1.

Table 1: ISCED levels mapped onto length of each education stage.

ISCED level	Stage of Education	Length of Stage (Years)
0	Pre-primary	Not defined
1	Primary	4-7
2	Lower secondary	2-5
3	Upper secondary	2-5
4	Post-secondary non-tertiary	0.5-3

Since different countries and regions diverge in terms of lengths of each stage of education, the ISCED stages are more a relative benchmark of where a child or a young person under the age of 18 can sit within their pre-university educational journey. Note that due to our focus on pre-university education, Table 1 does not include the last stage of education, 'tertiary' or 'higher' education, which is about education at a degree-awarding educational institution such as a university. In other words, the term 'pre-university education' in this report refers to ISCED levels 0-4.

The second benchmark is the (biological) age of a pupil, a more absolute benchmark corresponding to the biological developmental stage of a pupil. It will be used to contextualise the ISCED levels for a fairer comparison of educational stages across countries. Using age as a second benchmark allows for discussion of nuances in different school systems with mis-aligned stage years. It also identifies changes and outcomes at a higher level of detail, for example, at what age are certain teaching outcomes expected. Table 2 shows how the pre-university educational stages compare among some countries covered in our research, using

both benchmarks. The table shows that the pre-university education systems in different countries have some general alignment, although there are significant differences as well, including on the naming of the different educational stages (e.g., Year 1 refers to different biological ages in different countries). Such differences highlight the importance to use both benchmarks for fair and clearer comparison across different countries.

Table 2: The named school year and pupil ages in some of the countries included in this report

Age range	5	6	7-11	12-17	18
England (UK Government, nd-a)	Year R	Year 1	Years 2-6	Years 7-12	Year 13
Wales (TheSchoolRun.com, nd-a)	Year R	Year 1	Years 2-6	Years 7-12	Year 13
Scotland (Scottish Government, 2018)	Year P1	Year P2	Years P3-P7	Years S1-S6	Year S6
Northern Ireland (Department of Education (Northern Ireland), nd)	Year 1	Year 2	Years 3-7	Years 8-13	Year 14
US (U.S. Department for Education, nd)		K*	Years 1-5	Years 6-11	Year 12
Australia (Department of Foreign Affairs and Trade (Australia), 2017)		K*	Years 1-5	Years 6-11	Year 12
Canada (Government of Canada, 2021a)		K*	Years 1-5	Years 6-11	Year 12
New Zealand (Ministry of Education (New Zealand), 2021a)		Year 1	Years 2-6	Years 7-12	Year 13
Singapore (Ministry of Education (Singapore), nd-a, nd-b)			Years P1-P5	Years P6, S1-S5	Junior College 1/ Polytechnic 1

* In the US, kindergarten is mandatory only in 19 states and the District of Columbia (Education Commission of the States, nd). This is also the case in Canada and Australia. However, they do remain part of the formal education system.

1.6. Structure and standard styles of the report

The rest of the report is structured as follows. Section 2 presents our chosen approach and methodology. Section 3 examines the inter- and multinational context of cyber security education, in terms of policies, initiatives and guidance. Section 4-6 explore cyber security in different groups of countries: the UK in Section 4; Australia, Canada, New Zealand, Singapore

and the US in Section 5; and Estonia, Greece, Mexico, Norway, Portugal and South Africa in Section 6. The last section (7) discusses the findings, and draws conclusions and recommendations. Finally, a number of appendices give additional details useful to understand the research conducted and results presented.

We follow some standard styles throughout the report to help enhance readability. We highlight names of countries and stakeholders **in boldface** when they are mentioned for the first time or when the highlighting helps indicate a dedicated discussion on a country or a stakeholder. In addition, we highlight titles of important documents and activities ***in boldface and in italic***, and put them in single quotation marks if the title is long and can be confusing if not quoted (e.g., '***Education for a Connected World***' and '***Charting Your Course: Cyber Security Governance***'). When the same document is referred to again, it is normally *in italic* only (e.g., '*Education for a Connected World*') to avoid unnecessary repeated highlights. Similarly, short direct quotations from relevant documents, especially those used as part of a sentence, will also be put in single quotation marks and normally *in italic* only ('*a short quotation*'). Longer quotations, especially those including more than one sentence, mainly direct quotations of interviewees, are marked with double quotation marks ("…"), and shown in the following style with their source (either a document or an interviewee):

> *"[direct quotations]" – [source/interviewee's role, affiliation, country]*

The content of Sections 3-6 is based on results of our desk research in Stage 2 and from interviews in Stage 3. Selected direct quotations of interviewees are used when necessary to support reported observations or summarised results in this report.

2. Research Approach

This Section explains the terminology this report uses and outlines the methodology we followed throughout the various stages of the research project, including our selection of countries and the rationale behind such selections.

2.1. Terminology

In addition to some of terms that have already been explained in the preface and the previous section, in this section we clarify some other terms and spellings we use throughout the report.

There are different spellings of the term '**cyber security**'. Other forms include '**cybersecurity**' and '**cyber-security**'. In the research literature and in the UK, the term 'cyber security' is dominating, although 'cybersecurity' is also popular in other contexts or countries/regions. Throughout this report, we will use 'cyber security' as the standard spelling, but when referring to names of organisations, documents or other entities, we will follow their official spelling in the original source.

In a similar manner to the above, we will also use standard spellings for other cyber related terms in the form of 'cyber' followed by a white space and another noun, e.g., '**cyber bullying**' and '**cyber crime**'. This is because the form of spelling is more often used in the UK: when we searched into the website of the ONS on 25th January 2022, 435 results were returned for 'cyber crime' (ONS, nd-a), but only 2 returned for 'cybercrime (ONS, nd-b). Another alternative forms of spelling, where 'cyber' is followed immediately by the next noun without a white space, e.g., '**cyberbullying**' and '**cybercrime**', are kept in some contexts, e.g., in some of the documents referred to in this report (for which we need to follow the official spelling in the original source).

In this report, the term '**children and young people**' refers to anyone eligible for pre-university education (ISCED levels 0-4, typically under the age of 18), outside of an educational context. Inside of an educational context, the term that will be used is '**pupil**' (differencebetween.net, nd). We avoid using the more confusing term '**student**' that is often used for an attendee of education at the ISCED levels 5 (higher education) and above.

Pre-university educational institutions also have a variety of ways they are referred to within different countries and contexts. In this report, we use the term '**schools**' for primary and secondary educational institutions and also pre-schools or nurseries (ISCED levels 0-3), and the term '**colleges**' for post-secondary educational institutions which are not considered higher educational institutions (ISCED levels 4, e.g., vocational colleges offering pre-university courses). Note that some higher educational institutions use the term 'school' in their names, but they offer education at the ISCED level 5 or above.

In this report, the term '**teacher**' refers to an individual whose job role includes teaching, and sharing knowledge and understanding to pupils within a pre-university educational institution. Occasionally, the term '**educator**' may be used in place of teacher if referring to the name adopted by a specific documentation. A different term '**school staff**' is used to refer to all staff in a pre-university educational institution, whether they have a teaching qualification and partake in activities which have an educational purpose, or not. School staff more broadly may include: teaching assistants; IT support staff; and administrative staff.

The terms '**country**', '**nation**', '**state**' and '**region**' all refer to different concepts within this report. We are aware of the nebulous nature of these terms, therefore, we decided to use a

standardised application of these terms throughout the report in order to minimise unnecessary confusion. A '**country**' refers to the territory that comprises an independent political unit and its population (Cambridge Dictionary, 2021) at a higher level, whereas in this report, we describe a '**nation**' as referring to the collective group of individuals with shared traditions, culture, language and potentially devolved government at a lower level (which is also governed by a government at country level). One example of this is the UK, which is considered one country made of four nations (England, Wales, Scotland, and Northern Ireland).[2] For many of the countries included in this report, both the terms '**nation**' and '**country**' refer to the same concept and, in this case, we will use the word '**country**'. A '**state**' or '**province**' refers to a territory with its own government inside a country, which is not counted as a country (e.g., the State of California). A '**region**' in this report refers to a part of a country or a group of countries, without specific borders. For example, Estonia is in the Eastern region of the EU (European Union). The term '**national**' is often used in regards to school curricula and other documentation. Unless it is used as a proper noun (for example, the English *National Curriculum*), the term 'national' refers to the country level. In the case where 'national' is used as a proper noun or in the title of a document, clarification will be given as to its definition or limits (e.g., which country or nation it is relevant to).

The terms '**international**' and '**multi-national**' refer to different levels of multi-country groupings. '**International**' refers to a global approach, with countries from multiple continents involved or included, whereas '**multi-national**' refers to groups of countries that are in one continent or a more limited geographic region. One example of a multi-national group would be the EU, and another is the EEA (European Economic Area).

2.2. Methodology

The methodology followed for this study comprised of three stages:

1. **Stage 1**: a **systematic literature review (SLR)** to get a more in-depth understanding of the research literature on pre-university cyber security education;
2. **Stage 2**: **desk research** on gathering relevant **public information** on the internet, focusing on related policy documents, projects, initiatives and events in 13 selected countries, from a wide range of relevant organisations in both public and private sectors, including some important international and multi-national organisations;
3. **Stage 3**: a number of **semi-structured interviews** with 21 interviewees from 11 countries (out of the 13 studied in Stage 2) and three additional interviewees from the UN agency ITU (International Telecommunication Union), for confirming information we collected from the first two stages and gathering more information directly from key experts.

For Stages 2 and 3, we needed to select a number of representative countries to contextualise our desk research and interviews. How we selected the countries is explained in Section 2.2.4. Note that in addition to a number of selected countries, we also covered a number of

[2] Officially, England, Wales, Scotland, and Northern Ireland are often referred to as four 'countries in a country' (Prime Minister's Office (UK), 2003) or four 'constituent countries' of the UK (ONS, 2021b). Legally, they are referred to more as 'parts' of the UK in various legislations or no specific terms are used other than their names (Wikipedia, nd-a). Since calling them 'countries' can cause unnecessary confusion for the purpose of this report (e.g., the number of countries covered), we decide to call them four 'nations' of the UK, following the more commonly used term 'home nations' in sectors such as sports (Six Nations Rugby Ltd, 2021) and broadcasting (BBC, 2022).

international and multi-national organisations to capture useful information beyond single countries (see Section 3 for results on such organisations).

This report is based on findings from all three stages, but we decided to put detailed results from Stage 1 into a separate document (Sağlam et al., 2021). Therefore, the following four sections (3-6) summarise results mainly from Stages 2 and 3, but the final section (7) draws key findings and recommendations from all the three stages.

2.2.1. SLR

An SLR was carried out along the research project with the aim to find and aggregate the body of knowledge on cyber security education in pre-university settings. The review followed the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) procedure (PRISMA, nd) and made use of the scientific indexing database Scopus (Elsevier B.V, nd). Articles published between January 2015 and June 2021 were considered following the methodology. Findings were reported in terms of the themes: *what to teach*, *how to teach* and *who should teach*. See (Sağlam et al., 2021) for more details of the SLR.

2.2.2. Desk research

We next undertook desk research in order to better understand how pre-university cyber security education has been conducted in different countries worldwide, which also helped prepare the needed contextual information for the semi-structured interviews in Stage 3. In total, 13 countries included in this stage of the research were (in alphabetical order): Australia; Canada; Estonia; Greece; Mexico; the Netherlands; New Zealand; Norway; Portugal; Singapore; South Africa; the UK; and the US. We also reviewed provisions and activities of a number of relevant international and multi-national organisations, including ITU (International Telecommunication Union), ENISA (European Union Agency for Cybersecurity), Informatics for All, OECD (Organisation for Economic Co-operation and Development), and the project's funder GFCE (Global Forum on Cyber Expertise).

For this stage, we adopted a hybrid approach for our methodology. We took a top-down approach using the organisational typology outlined in Table 3 to guide which organisations to search and how to search their websites, and a bottom-up approach based on keyword searches in Google to discover more potentially relevant organisations and activities. Note that we did not find any relevant activities for some organisations we searched for and studied (including some shown in Table 3), so they do not appear later in this report.

Table 3: An overview of the organisational typology followed for the desk research

Organisational Category	Example Organisations in the UK
National and devolved nations' public bodies covering pre-university education	Department of Education; Ofsted (Office for Standards in Education, Children's Services and Skills); Ofqual (Office of Qualifications and Examinations Regulation)
National and devolved nations' public bodies covering cyber security	National Cyber Security Centre (NCSC-UK); NI Cyber Security Centre
National and devolved nations' public bodies authorities covering digital technologies	Department for Digital, Culture, Media and Sport (DCMS)
Exam boards and teaching standard bodies	AQA; Council for the Curriculum, Examinations & Assessment (CCEA); Oxford, Cambridge and RSA (OCR); Pearson Edexcel; Welsh Joint Education Committee (WJEC)

National public bodies covering online safety	UK Council for Internet Safety (UKCIS); UKCCIS: UK Council for Child Internet Safety (UKCCIS); Information Commissioner's Office (ICO); Ofcom; Home Office; law enforcement agencies such as National Crime Agency (NCA)
Public bodies serving children and young people	Children's Commissioner for England; Children's Commissioner for Wales; Children and Young People's Commissioner Scotland; Northern Ireland Commissioner for Children and Young People
Relevant funding bodies	Education and Skills Funding Agency (ESFA)
Associations of schools and colleges	Association of School and College Leaders (ASCL); Association of Colleges (AOC); Independent Schools Association (ISA); Independent Schools Council (ISC); National Association of Independent Schools & Non-Maintained Special Schools (NASS); Independent Association of Prep Schools (IAPS); Partnerships for Schools (PfS)
Associations of cyber security-related teaching, learning or teachers	Computing At School (CAS) Working Group; National Centre for Computing Education (NCCE); BCS Academy of Computing; PSHE Association
Cyber security related professional bodies	Chartered Institute of Information Security (CIISec); UK Cyber Security Council; BCS, The Chartered Institute for IT (formerly known as British Computer Society)
Cyber security training, CTF (capture the flag) competitions, and cyber security certification bodies	International Information System Security Certification Consortium or (ISC)[2:] EC-Council; HackTheBox
Cyber security and online safety awareness bodies	Childnet; Better Internet for Kids; Safer Internet Centre; Parent Zone; ThinkUKnow

During this stage, contacts from each organisation in each selected country covered were also established, and further information was gathered directly from key contacts who were knowledgeable in the provision of pre-university cyber security and online safety education in their respective nations. This supplemented the findings identified using the above typology. Contacts were found through connections of the research team, or contacts shared by the GFCE, and initial contact was made by a member of the research team. Following the retrieval of information relevant to cyber security and online safety education aimed at a pre-university level, the findings from this policy review guided the semi-structured interviews.

2.2.3. Semi-structured interviews

For 11 countries (out of the 13 ones covered in Stage 2), we managed to secure at least one semi-structured interview (with Krysia Waldock). Two countries from the desk research (Canada and the US) were not included in this stage because relevant contacts were not identified, or there was not a timely response to our request for an interview. Additionally, an interview was undertaken with ITU as an international provider of cyber security related services worldwide.

An interview guide (see Appendix B) informed the main structure of the interviews. Additional questions were added in regards to some bodies and organisations to gain contextual information on where the body/organisation sits in regards to cyber security and online safety. The interview guide covered: current initiatives; strategies and policies within the nation/organisation; development of (national) curricula and extra-curricular activities; challenges in regards to provision and future aspirations (see Appendix B). Questions on

current initiatives, strategies and policies also served as confirmation or further clarification of findings from the desktop research. Each interview lasted between 30 and 70 minutes and was undertaken remotely using the MS Teams platform conducted by Krysia Waldock. All interviews were audio recorded, and transcripts were generated using the automatic online transcription service Trint (https://app.trint.com/). The transcripts were read by Krysia Waldock and Vince Miller to fix any obvious errors made by Trint. Selected quotations appearing in the report were sent to all interviewees for feedback, which was used to further refine the wording.

The data from these interviews was used in two ways. Firstly, the data was reviewed for examples to support the policy review to triangulate findings, and to elicit broad trends. Quotations were extracted and used to support the relevant country or nation to triangulate findings from the policy review. Secondly, the data was analysed using Thematic Analysis (as per (Braun & Clarke, 2006)). Two members of the project team (Krysia Waldock and Vince Miller) read the interview transcripts, and a coding scheme was constructed to facilitate the interpretation of interviewees' opinions and information provided. The coding scheme was then applied throughout all of the transcripts to ensure the extracted information was consistent across all interviews. Appendix C shows the coding scheme used in detail.

2.2.4. Sample countries

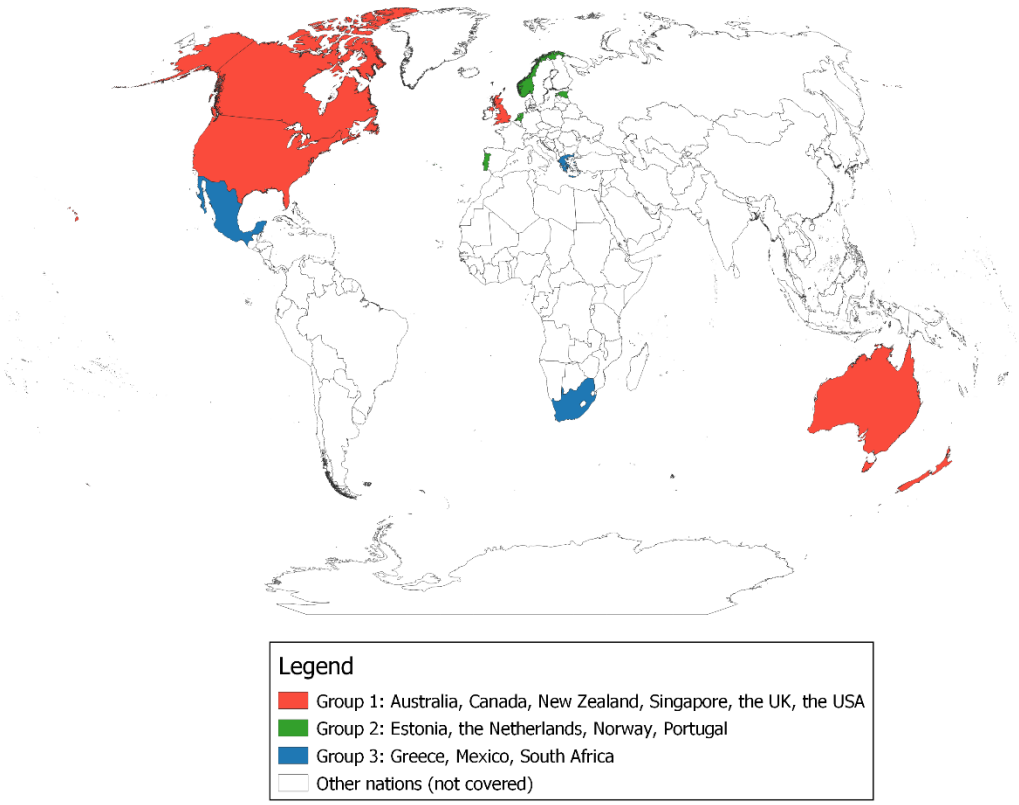
This report brings together the findings from 13 countries. These countries were grouped according to two main criteria: (1) if English is the official language or one of the official languages; (2) the predicted maturity of pre-university cyber security education. The first criterion was used because the research team and the funder have English as the common working language, which would allow for more access to policy documents and potential interviewees. The second criterion was used in an attempt to extend our coverage to countries at different levels of maturity in terms of pre-university cyber security education. In addition to these two criteria, we also endeavoured to cover a wide variety of countries in different continents, with different populations, and across different cultural and socio-economic contexts.

A short overview of the groupings used is outlined below.

- **Group 1:** This is a sample of economically developed countries where English is the official language (therefore, relevant documents will be accessible to the research team in English), and a cyber security educational program for schools is likely to be more established.
- **Group 2:** This is a sample of European and Asian countries where English is not the official language, and a pre-university cyber security educational program for schools is either established or is being developed. Supporting documents may or not be in English.
- **Group 3**: This is a sample of countries which are unknown in terms of their current and planned activities in developing a pre-university cyber security educational program. Supporting documents may or may not be accessible in English, and are likely to be in draft format, therefore not available online.

It was decided to split Group 1 into two different sections, as the UK contains four nations and we cover them in substantial detail. Groups 2 and 3 were grouped together for the purposes of reporting, due to the small number of participating countries from Group 3. Figure 1 illustrates the geographic coverage of Stages 2 and 3 of our study.

Figure 1: Countries covered in our study



3. International and Multi-national Contexts

This section focuses on pre-university cyber security education at an international and multi-national level, with specific focus on the **ITU** (**International Telecommunications Union**) as an important international body in the context of the **UN** (**United Nations**) and the **ENISA** (**European Union Agency for Cybersecurity**) as an important multi-national boy in the context of the **EU** (**European Union**). We also briefly cover relevant policies and initiatives run by the following other international and multi-national bodies: **GFCE** (**Global Forum on Cyber Expertise**), **UNICEF** (**United Nations Children's Fund**), **OECD** (**Organisation for Economic Co-operation and Development**), and **Informatics for All**. Interview data supplements the findings from desk research in the case of the ITU. Focusing on international and multi-national contexts first allows us to show what is occurring currently in terms of sharing best practices across multiple countries, and to identify gaps in current provisions at the international and multi-national levels.

3.1. ITU

The **ITU** is the agency of the **UN** for information and communication technology. 193 UN states are currently members of ITU, as well as some 900 international and regional organisations including companies and universities (ITU, nd-a). The main arm of the ITU in regards to cyber security is the **ITU Telecommunication Development Sector** (**ITU-D**). ITU-D manages ITU's ***cyber security thematic priority***, which include a number of programmes. The majority of the focus upon cyber security programmes targets those who are over the age of 18, and/or those in higher education, and much of the cyber security offering has a distinct organisational focus, with the exception of the ***Child Online Protection (COP) programme***, which targets children and young people. Table 4 gives an overview of the ITU's cyber security programmes.

Table 4: An overview of the different cyber security programmes of the ITU

Cyber Security Programme	Description
Global Cybersecurity Agenda (GCA) (ITU, nd-b)	The GCA launched in 2007 is a framework for international cooperation. Cooperation and efficiency are at the heart of its aims, with input from various global stakeholders as key. There are five working areas, including capacity building relevant to pre-university cyber security education. The GCA has advanced initiatives like Child Online Protection (ITU, nd-c, nd-d) (see below).
Global Cybersecurity Index (GCI) (ITU, nd-e, 2021a)	The GCI measures a UN member state's commitment to cyber security. It demands a collaborative approach as it required a variety of organisations to work together. The pillars of the CGI include: Legal Measures, Technical Measures, Organizational Measures, Capacity Development, and Cooperation. The ITU GCA provides a foundation for the GCI. Capacity development does include and cover pre-university cyber security education, however it is not delineated from university level cyber security education.
Child Online Protection (COP) programme* (ITU, nd-b, nd-c)	This is a part of the ITU GCA framework. The key objectives are to create awareness, identify the risks children face online, share knowledge, and develop capacity and tools.
CyberDrill events (ITU, 2021b)	The events are organisation-focused events compromising of training programmes in the form of simulations of cyber attacks, where organisations can test their policies and procedures. These allow organisations to build capacity and resilience.

Women in Cyber Mentorship Programme (ITU, nd-f)	This is run jointly with the Forum of Incident Response and Security Teams (FIRST) and EQUALS, and serves to increase the diversity within cyber security, notably in regards to gender.
National Computer Incident Response Teams (CIRTs) (ITU, nd-g)	ITU-D is assisting member states to form their own CIRTs and improve the responsiveness of the CIRTs. CIRTs (currently 118 worldwide) co-ordinate responses to cyber incidents. The aim of these CIRTs, through the support of ITU-D, is to improve cyber capacity at both national and regional levels. ITU-D has completed CIRT assessments for 79 countries, and established CIRTs in 14 countries.

*Relevant to cyber security skill development for children and young people under 18 years old.

An interview with the ITU confirmed that pre-university education for children and young people is more focused on child protection (online safety) rather than on developing a cyber security career pathway:

> *"The thinking behind this is that, looking into like cyber security to possible career, …, under 18, they're not really mature enough into thinking what career they can pursue. So trying to target undergraduates and maybe get them interested in the field, that's where the target group sort of differs from the protection side." – Cybersecurity Policy Officer, ITU*

And further iterations of the GCI having clearer focus on the impact of pre-university education, in particular ISCED levels 1-4:

> *"In the next iteration of the Global Cybersecurity Index, we're actually planning on being a little bit clearer about what primary, secondary and higher mean that can differ by countries." – Cybersecurity Lead Researcher, ITU*

The COP work at the ITU targets under 18 year-olds, and sits under the cyber security header on the ITU website. The key COP activities are around the recent '***Child Online Protection (COP) Guidelines***' (ITU, nd-d), part of the wider ***Global Child Online Protection Project*** (ITU, nd-c, nd-d), with different guidance for parents, carers and educators, industry and policy makers, as well as children of different age groups, accounting for differences in guidance between stakeholders. These guidelines replace earlier guidance published in 2009. The benefits of a ***national strategy*** are outlined in the guidelines, including ***national checklists for individual countries and companies*** to 'mark' themselves against as a form of self-assessment. Elements of cyber security education are built into the guidelines, for example antivirus and firewall protection software, and privacy & information sharing as well as cyber safety (ITU, nd-d). The cyber safety focus of the child protection work at the ITU was confirmed at our interview with three ITU interviewees:

> *"So on child online protection, which is the work I'm leading, … the question is really more [on]: are children, so if we look at the target group of children and young people, are they aware of the risks and potential harms that they can face online? Do they have the literacy and the resilience to stay safe online? Do they know what respectful behaviours [are]? Do they know how to access support systems if they see something they feel uncomfortable with? And so on." – Child Online Protection Officer, ITU*

Advice for schools and educators in the guidance for parents and educators takes a preventative stance in terms of infrastructure (e.g., advice to appoint an online safety co-ordinator, advice to ensure the school IT network is safe) with a small mention of contributing to the digital literacy and skills of children and young people with digital citizenship education (ibid). There is a list of resources for each of the respective set of guidelines (ibid) and on its website (ITU, nd-h). In addition, ITU also has ***guidelines for children*** (ITU, nd-i), mainly the

activities book for children of 9-12-year-olds (ITU, nd-j), and a corresponding ***teacher's guide*** that provides very clear methodology and activities to do with children (ITU, 2020b).

For children specifically, a ***COP mascot*** named ***Sango*** (also called ***Sangophone***) has been developed (ITU, nd-c, nd-d). Sango is a part of the wider ***Global Child Online Project***. Children can follow Sango through videos and workbooks in a self-directed manner, or teachers can use the resources containing Sango in their lessons using the teacher's guide (ibid). Current content available includes advice on password security, data privacy, information on apps, social media and YouTube (ibid). At our interview with three ITU interviewees, a related social media campaign aimed at 13-18 year-olds was also noted, with differing participation and activeness across different countries:

> *"Then there was a social media campaign for all the children, 13 to 18, that we launched through different channels. And all resources, of course, available in all official UN languages and partly have actually been translated into [other] national languages. So we have a few countries that are very active in localising these resources and yet working with these materials at the country level." – Child Online Protection Officer, ITU*

A multiplicity approach appeared to be endorsed by the ITU in regards to routes into cyber security careers, but also the need for multiple stakeholders to input into online safety of children and young people, and in terms of a model curriculum. What was made clear was that without collaboration and cross-sector working, ensuring the online safety of children and young people would be very challenging, and multiple stakeholders need 'buy in' to ensure any chance of success, especially in an international context:

> *"This is where we are having this multi-stakeholder initiative on child protection because we cannot do it alone. UNESCO cannot do it alone. UNICEF [United Nations Children's Fund] cannot do it alone. No one can. Right, [so] we need the different aspects. We need the industry and … the ministries … also the Ministry of Education, the Ministry of Social Welfare, Children, Families. Um, we need also the families around. We need the educators. So, …, there's all those different layers." – Child Online Protection Officer, ITU*

This idea of multiple routes and multiple stakeholders requiring buy in for success also appeared to be present in regards to cyber security careers, which was discussed in regards to a current project underway at the ITU:

> *"We did an exploratory project in Vietnam looking at if we take an ecosystem approach, a systems approach to this and looking at where cyber security educational interventions are possible, given that some systems that it might not be as much of you go to university and then you pursue your career rather than options where there can be interventions earlier or through vocational paths, apprenticeships and so forth. So we're going to publish a paper on it all again, very in the conceptual stage. By taking that ecosystem approach … cyber security might be sparked earlier and you need maybe some foundations to build on for that, to then lead to a full on cyber security career." – Lead Cybersecurity Researcher, ITU*

The idea of a model curriculum, with the potential problems of having a model curriculum in terms of varying socio-cultural contexts across countries, was also discussed:

> *"We also know and this comes with a lot of challenges to provide something, …, a model, a model curriculum, because in particular, when we work with children, when we work at the school system, apart from, …, all the other areas where this is also as important, but the local and the national context is key, and you cannot develop a curriculum that is in the same way adaptable in*

the UK, in Nigeria and in Cambodia. Right, this is just very, very challenging." – Child Online Protection Officer, ITU

Therefore, any global cyber security education guidance at a pre-university level should be sufficiently flexible to account for differences in socio-cultural context across different countries.

The ITU provide an international context of provision. Although there is some cyber security educational provision, closer examination has found, the provision which targets pupils at a pre-university level has an online safety focus and a preventative child protection stance. Work undertaken within cyber security more generally by the ITU highlights the need for multiple stakeholders to buy in, and the importance of multiple routes into cyber security careers.

3.2. ENISA and EU-Wide Policies and Initiatives

The **ENISA** is the EU's agency committed to improving cyber security across the EU (ENISA, nd-a). One of the aims of the ENISA is 'capacity building' at all levels. Children and young people are not explicitly mentioned, however, given the broad levels mentioned of '*non-expert to the highly skilled professional*', children and young people are included in some of the ENISA's cyber security educational and awareness activities.

The ENISA and the European Commission's contributions to cyber security skill development lie in both policy and initiatives. Notably in regards to policy, the '***Cybersecurity Skills Development in the EU*** (2020) resulted in the higher education database, and the EU Digital Education Action Plan (2021-2027) has the priority area *'developing digital competencies and skills'*. *'Cybersecurity Skills Development in the EU'* (2020) focuses on university-level cyber security skill development, but the ***EU Digital Education Action Plan*** (2021-2027) does focus on primary and secondary aged pupils in regards to how online learning should operate and how to make online learning more effective. Guidelines and common frameworks are also called for in relation to teaching digital literacy. Furthermore the ***Digital Competence Framework 2.0*** (***DigComp 2.0***) (Vuorikari et al., 2017) specifically has a competence on 'safety', however, this is for the general population and not solely targeted at pre-university education. The competence on 'safety' is outlined in Table 5.

Table 5: The 'safety' competence within the EU Digital Competence Framework 2.0 (Vuorikari et al., 2016)

Competence	Description
Protecting devices	*"To protect devices and digital content, and to understand risks and threats in digital environments. To know about safety and security measures and to have due regard to reliability and privacy."*
Protecting personal data and privacy	*"To protect personal data and privacy in digital environments. To understand how to use and share personally identifiable information while being able to protect oneself and others from damages. To understand that digital services use a 'Privacy policy' to inform how personal data is used."*
Protecting health and well-being	*"To be able to avoid health-risks and threats to physical and psychological well-being while using digital technologies. To be able to protect oneself and others from possible dangers in digital environments (e.g., cyberbullying). To be aware of digital technologies for social wellbeing and social inclusion."*
Protecting the environment	*"To be aware of the environmental impact of digital technologies and their use."*

Closer examination of these competences demonstrates that the competence 'safety' includes both aspects of what we call cyber security in this report (e.g., protecting devices and personal data) and aspects of what we call online safety (e.g., protection against cyber bullying, demonstrating the closeness of both aspects.

In addition, there appear to be a number of European wide initiatives, including: ***ECSC*** (***European Cyber Security Challenge***) (ENISA, nd-b), ***EU Cyber Security Month*** (ENISA, nd-c) and the ***Youth4Cyber programme*** of **ECSO** (**European Cyber Security Organisation**) (ECSO, nd), each engaging children and young people to differing degrees. The EU Cyber Security Month appears to target the general population, whereas the ECSC has five juniors (aged 14-20) per team (along with five seniors, aged 15-21 to make one team), with EU member states opting into the ECSC as a whole. Organisations and universities can opt to send a team to the ECSC. ECSO's Youth4Cyber specifically targets children and young people aged 6-26 years. These activities appear to be 'opt in' in nature, with participation in Youth4Cyber and the ECSC are individually initiated in terms of signing up for participation (i.e., they decide to take part of their own accord, it does not require schools to enrol them). However, at country level, each member state organises their own national teams via a national competition in regards to the ECSC.

3.3. GFCE

The **GFCE** is a global forum and community which supports cyber capacity building at a global level, where best practice can be shared and initiatives be developed to enhance cyber capacity (GFCE, 2017). There are 93 members [3] globally (including countries, intergovernmental organisations, international organisations and companies (GFCE, 2021). The *Delhi Communiqué* (GFCE, 2017) (the Global Agenda for the GFCE on cyber capacity building) named one of the themes for capacity building as '*Cyber Security Culture and Skills'*, including promoting awareness of cyber threats and vulnerabilities, and increasing the knowledge and skills for safe online practice along with 'creating a workforce **with a set of cyber security skills and knowledge employers require'** (emphasis added by authors). Capacity building in this sense appears to be broader than solely targeting pre university children and young people. Working groups were set up in 2018 following the themes from the *Delhi Communiqué*, with working group D being focused on cyber security capacity building (GFCE, 2020a). The *Global Cyber Capacity Building Research Agenda 2021* (2020b) is a recent tool developed by the GFCE to inform which projects and initiatives should be worked on, and exploring knowledge gaps within research. This agenda sets a priority list of topics for research. Working Groups A-D have with Working Group D 'Cyber Security Culture and Skills' notably having one topic as 'cyber skills amongst young people'. Cyber skills amongst young people as number one on their prioritised list within the research agenda, demonstrating a focus on the education of children and young people, and sharing of best practice in this domain.

3.4. UNICEF

The **UNICEF** is a UN agency providing humanitarian aid, working in 190 countries (UNICEF, nd-a). In regards to cyber security education at a pre-university level, most of the work that UNICEF undertake falls under the online safety aspect. Their work includes promoting the use of

[3] A full list of members can be found here: https://thegfce.org/member-overview/

acceptable safety measures on online platforms, and partnering with governments to lobby for regulations (UNICEF, nd-b). UNICEF also runs ***Global Kids Online*** and ***Disrupting Harm*** projects, which specifically seek to collect evidence on how children and young people use the internet, and the risks and opportunities that they face (UNICEF, nd-b, nd-c, nd-d).

3.5. OCED

The **OECD** supports digital security (their preferred term for cyber security, as digital security also includes 'economic and social aspects of cyber security' (OECD, nd)). The OECD's digital security work mainly has a business focus, with current projects including: enhancing the digital security of products, treating the vulnerabilities of devices and systems, and clarifying how businesses should respond to cyber attacks (OCED, 2021). Their recommendations also take a more technical approach to securing devices and data, rather than educating in a pre-university context (OECD, nd).

3.6. Informatics for All

The **Informatics for All** coalition (Informatics for All, nd) was formed in 2018, co-founded by the **ACM (Association for Computing Machinery) Europe Council** (ACM, nd) and the **Informatics Europe** (Informatics Europe, nd). Subsequently, the coalition was joined by the **CEPIS** (**Council of European Professional Informatics Societies**) (CEPIS, nd) and the **IFIP** (**International Federation for Information Processing**) (IFIP, nd). The '***Informatics Curriculum Framework for School***' document, made by Informatics for All, has a core topic area on *'Privacy, safety and security'*. This has a planned release date in 2022.

3.7. Summary

Within international and multi-national contexts, there is provision of cyber security education (through programmes, guidelines and initiatives) within a pre-university context, notably within a European and European Union context. Although pre-university education is a priority (in the case of the ITU), the education available seems to have more of an online safety education focus, therefore being less complete for covering the wider range of cyber security topics. Much of the provision from the ITU and other international/multi-national bodies covered in this Section appears to be extra-curricular in nature, supplementing to what countries may have already been providing, and require countries to 'opt in'. There also appears to be not a single **global** framework or a standardised set of guidelines for countries to follow. The **Informatics for All** and the '***Informatics Curriculum Framework for School***' it plans to release in 2022 are good examples of how different stakeholders in multiple countries can work together to produce more standardised and widely adopted curricula and guidelines. Although **Informatics for All**'s efforts have a clear focus on Europe, the participation of several international bodies (ACM and IFIP) can potentially help stimulate similar initiatives worldwide, although we envisage that creating a global framework may have various challenges, including diverse cultures, education systems and geopolitics.

4. UK

This section will explore cyber security education in the UK, considering each of its four constituent nations – **England**, **Northern Ireland**, **Scotland** and **Wales**. This report has a distinct focus on the UK for a number of reasons: 1) the project team is based in the UK and has more knowledge and connections with relevant stakeholders in the UK; 2) the UK is considered to be at the forefront of cyber security worldwide with a Global Cybersecurity Index (GCI) score of 99.54 (ranked 2/182 worldwide) (ITU, 2021a); 3) the UK is an active member of the GFCE Working Group D; 4) the UK's four constituent nations have their own developed governments, making the UK a complicated country to cover.

The content of this section will be explored through five perspectives or landscapes: stakeholder landscape, educational landscape, policy landscape, implementation landscape, and socio-cultural landscape. Each landscape examines different aspects of pre-university cyber security education: the stakeholder landscape explores parties with relevant interests and activities; the policy landscape examines relevant policies; the educational landscape explores the education systems in each country; the implementation landscape examines initiatives, programmes and actions; and the socio-cultural landscape examines influencing social, economic and cultural factors. The same structure will be followed in Sections 5 and 6 when for other countries covered in this report.

Note that we did not manage to arrange an interview with a relevant stakeholder in **Wales**, so the information about Wales is based on our desk research in Stage 2 only.

4.1. Stakeholder landscape

There are a variety of key stakeholders involved in pre-university cyber security education in the UK context. This section outlines major stakeholders in the UK, and briefly describes how they interact with each other. More details about their activities will be explained in later sections.

One key stakeholder is the **Government of the UK** (often called the **HM (Her Majesty) Government** domestically in the UK, but we will use the simpler and clearer term 'the **UK Government**', hereinafter in this report [4]), with various departments and public bodies responsible for different aspects related to cyber security and/or online safety. The **National Cyber Security Centre (NCSC**[5]), part of the **General Communications Headquarters** (**GCHQ**), is the UK-wide public body providing a single point of contact for organisations and the general public for cyber security matters. There is a similar body in Northern Ireland: the **NI Cyber Security Centre**. The **Department for Digital, Media, Culture and Sport** (**DCMS**) is the governmental department in charge of policies related to the digital sector covering several related areas, including data protection, internet safety, and cyber skills (DCMS, 2017). The **Department for Education** is responsible for setting the national curriculum guidance for schools and colleges in England to follow, and the **devolved governments of the three non-**

[4] When referring to a particular interviewee who is from a department of the UK Government, we will use the term 'HM Government' because this is preferred by the interviewee.

[5] In this section we will use the acronym NCSC, which is how this public body is known for domestically in the UK. It will be referred to as **NCSC-UK** from Section 5 to differentiate it from similar bodies in two other countries (NCSC-NZ of New Zealand, covered in Section 5, and NCSC-NL of the Netherlands, covered in Section 6).

English nations do the same for Northern Ireland, Scotland and Wales, respectively. The **Home Office** and **law enforcement agencies**, notably **National Crime Agency** (**NCA**), play a key role on extra-curricular educational activities on reducing cyber crime and online victimisation. The **UK Council for Internet Safety** (**UKCIS**), part of three UK Government departments – DCMS, Department for Education and Home Office, oversees online safety matters including online safety education (UKCIS, nd). The UKCIS evolved from the former **UK Council for Child Internet Safety** (**UKCCIS**) – a group of over 200 organisations from different sectors, by expanding its scope from protecting children online to the whole population (UK Government, nd-b). Other public bodies with relevant responsibilities and/or activities include **Office for Standards in Education, Children's Services and Skills** (**Ofsted**); **Children's Commissioners** in all the four constituent nations of the UK; and **Office for Communications** (**Ofcom**). The wide range of governmental departments and public bodies in the UK and the four constituent nations means that there are many interactions between the different bodies, and overall co-ordination can be complicated and challenging. The **Scottish Government** also provide **Glow**, an intranet system specific to schools in Scotland, in addition to the above.

At ISCED levels 3 and 4, **exam boards** play a key role in pre-university cyber security education since they dictate the outcomes of teaching and learning that occurs. Some exam boards are public bodies, but others are private bodies. More about such exam bodies are explained in greater detail in Section 4.3.3.2.

Communities of practice, **not-for-profit organisations** and **other public bodies** support both the guidance and curricula released by the Department for Education and devolved governments, and other more global efforts in regards to pre-university cyber security education. Examples of these communities of practice which are specific to computing-related subjects include: **Barefoot Computing** (Barefoot Computing, nd-a); **CAS** (**Computing at School**) (CAS, nd-a); and computing hubs run by the **NCCE** (**National Centre for Computing Education**) (NCCE, nd-a). However, the siloed nature is mirrored among these groups too, with some bodies repeating efforts by others or producing similar content (see Section 0) with co-ordination between the bodies being unclear. The **PSHE Association** (PSHE Association, nd-a) also provides guidance and curricula which are not computing related in each of the four constituent nations.

At the core of communities of practice are **teachers** who are an important group of stakeholders. Their knowledge and understanding of cyber security and of curriculum content can have a big impact on cyber security education at pre-university level. Not all teachers who teach cyber security related subjects are specialists in cyber security or even the wider subjects, e.g., at ISCED level 1 classes may be taken by a general primary class teacher. Therefore, support for teachers, in particular during their initial teacher training (ITT) and continuing professional development (CPD), seems to be key. Access to the communities of practice mentioned in Section 4.3.2 seems to be common cultural knowledge amongst teachers.

> *"We're in the early days of embedding digital literacy in initial teacher education. I think it's fair to say the task is largely around CPD." – Cyber Resilience Learning and Skills Coordinator, Scotland*

> *"We have a danger, and I think it's computer science generally, not just cyber, is just the lack of, …, specialists." – Assistant Head Teacher, England*

Parents (including legal guardians and carers) are another important group of stakeholders, especially for online safety education. A unique not-for-profit organisation in the UK, **Parent Zone**, plays a key role in supporting parents and connecting them with other relevant stakeholders for online safety and cyber security education:

> *"Parents are the largest untapped resource in supporting children – we do a lot of work to help parents and families in this area – directly or through schools. We also advocate for the inclusion of parents and families and make people realise there is this capacity for support available." – Research and Development Director, Parent Zone, England*

It appears that the **cyber security industry** in the UK has played a role in pre-university cyber security education, notably in regards to the *CyberFirst* programme, although different cultures and workplace demands between the cyber security industry and educational establishments do appear to cause some challenges (e.g., timetabling constraints, expectations of working with children and young people). Industry has also had input into standards for apprenticeships in regards to relationships between education and industrial partners:

> *"So these standards exist and they are written by industry. So the way a standard is written is an industry kind of 'get together' as they form – what's called a trailblazer group. And then they decide what they think should be in. What an apprentice should learn and have experienced throughout the course of that apprenticeship, and what they should be exposed to. And industry decides that [because] this is ultimately the people who employ these people, our industry." – Head of Department, HM Government*

Some organisations and charities support and collaborate with other stakeholders already mentioned, for example **SWGfL** (**South West Grid for Learning**) (SWGfL, nd-a), NSPCC (**National Society for the Prevention of Cruelty to Children**) and **ThinkUKnow**. Other charities and organisations are highlighted and signposted by the UK Government and its subdivisions in some released policy, e.g., Childnet International; whilst others independently provide information for children, young people and their parents, legal guardians or carers to access online (e.g., **Barnardo's**, **MoodSpark**, **Safe4Me**), adding to the variety of resources which can be accessed independently. **Cyber Security Challenge UK** runs CTF-style events to give pupils a flavour of cyber security activities and thinking (Cyber Security Challenge UK, nd-a).

4.2. Policy landscape

The policy landscape varies across the four constituent nations of the UK, with Wales, Scotland and Northern Ireland having policy input from each of their own devolved governments as well as the UK government. A variety of governmental departments have had input on policy related to cyber security of pre-university pupils.

4.2.1. UK-wide policy

The UK-wide ***National Cyber Security Strategy (2016-2021)*** (UK Government, 2016b) is a continuation of the UK's first strategy in this area, the *National Cyber Security Strategy (2011-2016)* (UK Government, 2011, 2016a). The 2016-2021 strategy includes developing cyber security skills across the general population (p55), improving the teaching of Computing and other related subjects, and embedding cyber security into the National Curriculum (p56), and addressing the lack of diversity in cyber security (p56). The development of a school's programme, ***CyberDiscovery***, and expanding another, ***CyberFirst*** (p56-57), were explicitly mentioned in regards to the education at pre-university level. On 15th December 2021, the UK Government also released its new ***National Cyber Security Strategy 2022*** (Cabinet Office (UK), 2021). Objective 2 of the implementation part of the new strategy is defined as: "*Enhance and expand the nation's cyber skills at every level, including through a world class and diverse cyber security profession that inspires and equips future talent*" (p54). One of the five

outcomes by 2025 under this objective is a "*steady and diverse flow of highly-skilled people coming through our education system*", which mentions cyber security education in the pre-university setting and upskilling of school teachers (p55).

In May 2021, on behalf of the UK Government, the **DCMS** proposed a '***Draft Online Safety Bill***' (DCMS, 2021b) to the UK Parliament for consideration, which has a few elements related to cyber security. Rather than addressing cyber security education, this bill provides safeguards and protections that will protect children and young people in the digital world. The bill does not have a focus on children and young people, rather covers the whole population. Notably, the bill aims to protect people from financial and romance fraud online and protect young people from racist abuse online (UK Government, 2021a). Technology companies are also required to report child abuse on their platforms. This follows on from '***Online Harms White Paper***' (DCMS, 2019). In this white paper, no mention has been found of cyber security education for young people, in spite of education and innovation being one of the aspects of the framework. The education appears to be for companies (technology companies in particular).

A list of online media literacy resources has also been provided by the DCMS (2021c), which includes resources on managing privacy, preventing online harassment and reporting inappropriate content. The UK Government (2021b) more broadly also have a list of online media literacy resources freely available, including the topics of managing privacy, online safety, preventing cyber bullying and recognising misinformation and disinformation.

The new ***Online Media Literacy Strategy*** was launched by the DCMS in July 2021 (with updates in August 2021), with the main aim of the strategy to '*support organisations to undertake media literacy activity in a more coordinated, wide-reaching, and high quality way*' (DCMS, 2021d, p4). The action points of this strategy which supports cyber security education at a pre-university level notably include (ibid, p5): '*ensuring a coordinated approach to media literacy activity*', '*addressing key gaps within the media literacy landscape*', and '*reducing barriers and creating opportunities for organisations undertaking media literacy activity*'. The ***Media Literacy Framework*** (ibid) constitutes one aspect of this strategy, and further supports cyber security education at a pre-university level. The five principles of the *Media Literacy Framework* include (ibid):

- '*the risks of sharing personal data online and how that data can be used by others, and be able to take action to protect their privacy online*'
- '*how the online environment operates and use this to inform decisions online*'
- '*how online content is generated, and be able to critically analyse the content they consume*'
- '*actions online have consequences offline, and use this understanding in their online interactions*'
- '*how to participate in online engagement and contribute to making the online environment positive, whilst understanding the risks of engaging with others*'

Furthermore, one of the key challenges of the *Media Literacy Framework* is '*building audience resilience to disinformation*' (ibid), which is key to cyber security education at a pre-university level. Although children and young people as a broader group are not targeted as a 'vulnerable group' in this strategy, informing parents is mentioned (ibid, p59), as parents can influence the amount of time that children and young people spend online and therefore impact their media literacy levels. In addition to the strategy as a policy document, DCMS also maintains a list of ***online media literacy resources and events*** for pupils, parents, families, teachers, foster carers and services, media, and other relevant stakeholders (DCMS, 2021d).

Department for Education's statutory guidelines '***Keeping children safe in education***' (Department for Education (UK), 2021) specifically examine safeguarding and have been updated since the COVID-19 pandemic with information on how to keep children and young people safe online. The guidelines suggest that online safety and safeguarding should be taught to pupils, particularly through remote, online teaching which has been commonplace for some pupils during the COVID-19 pandemic.

The '***Keeping children safe in education***' guidelines recommend numerous resources to help school staff. One important resource recommended is the guidance named '***Teaching Online Safety in Schools***' (Department for Education (UK), 2019), which can be used in all educational settings from early years to post 16 years old, with a main focus on primary and secondary schools. Teaching online safety is reported to complement teaching covered in Computing across all year groups in England. The content suggested includes:

- evaluating what you see online (is it valid/true/acceptable?)
- recognising persuasive techniques
- understanding acceptable and unacceptable online behaviour
- identifying online risks (e.g., what this might look like, digital footprint – live streaming)
- seeking support (e.g., fake profiles)

The '*Teaching Online Safety in Schools*' guidance also suggests that schools should consider the environment in which they are teaching content regarding online safety, e.g., schools should have a safe environment where pupils can say what they feel. A 'whole school approach' is recommended to further embed this in teaching, as is involving parents and carers and modelling online safety principles consistently. This guidance appears to be a non-statutory document; therefore, schools have the freedom to implement this in a way that suits them. They do, however, have to cover these topics in Relationships Education (primary schools) and Relationship and Sex Education (secondary schools).

The **Department for Education** also disseminates online teaching-specific advice related to cyber security and online safety, in the form of non-statutory guidance. For example, the guidance '***Safeguarding and remote education during coronavirus (COVID-19)***' (Department for Education (UK), 2021b) includes a range of advice, e.g., the use of institutional email accounts for work/school communications, schools advising pupils not to share personal information, and security tips surrounding logins and passwords for accessing online virtual learning environments and VoIPs.

Cyber bullying is mentioned in the **Department for Education**'s guidance '***Preventing and Tackling Bullying***' (Department for Education (UK), 2017). It permits school staff to delete and examine files on an electronic mobile device seized by a teacher, without the need to secure parental consent. There is no mention of any kind of educational measures or online safety in regards to prevention of cyber bullying, or interventions. Specific advice is also given regarding cyber bullying, including for staff (Department for Education (UK), 2014b). The importance of the 'whole school community' in preventing cyber bullying is emphasised, repeating similar advice from the '*Teaching Online Safety in Schools*' guidance (Department for Education (UK), 2019). Other sources have also shared guidance and tips in regards to cyber bullying, however the information given is usually information for those who have, or are being, cyberbullied rather than practical teaching resources or suggesting education (e.g., (UKCCIS, 2017)).

The **Home Office**, in partnership with other stakeholders, including the National Society for the Prevention of Cruelty to Children (NSPCC), Behavioural Insights Team, O2, National Union of Students, and Sussex Police, created guidance for professionals to teach young people (ideally aged 13-18) about abusive behaviour online that can lead to cyber bullying and other online

safety issues (Home Office (UK), 2015). The topics covered include: identifying unwanted/abusive behaviours, why are these behaviours unwanted, and personal values and online behaviour. Resources and examples to use within the teaching sessions are also given (e.g., examples of abusive behaviour online and consequences to actions).

The **UKCIS** provides '***Education for a Connected World – 2020 edition***' (UKCIS, 2020), a framework to assist teaching online safety education. This builds on a previous version of '*Education for a Connected World*', which was released in 2018 (UK Safer Internet Centre, 2018). The areas the framework covers are (more cyber security and online safety relevant ones highlighted in ***italic boldface***):

- Self-image and identity:
  - differences between ***online and offline identity***, including ***harvesting of online identity by AI*** (suggested for ISCED levels 3 and 4 (14-18-year-olds))
- Online relationships:
  - online relationships, harm and consent, including ***cyber bullying*** (suggested for ISCED level 2 (11-14-year-olds))
- Online reputation:
  - how others use online information to make judgements, including how information can be copied from online (suggested for ISCED level 1 (4-7-year-olds)), laws and behaviour governing online behaviour (suggested for ISCED levels 3 and 4 (14-18-year-olds))
- ***Online bullying***
- Managing online information:
  - how information is viewed, stored and interpreted
- Health, wellbeing and lifestyle
- ***Privacy and security***:
  - '***how personal online information can be used, stored, processed and shared***, including ***what passwords are*** (suggested for ISCED level 1 (4-7-year-olds)), explaining ***what a strong password is*** (suggested for ISCED level 1 (7-11-year-olds)), understanding the ***benefits of two-factor identification*** (suggested for ISCED level 2 (11-14-year-olds)), understanding law regarding data use, e.g., ***GDPR*** (***General Data Protection Regulation***) (suggested for ISCED levels 3 and 4 (14-18-year-olds))
- ***Copyright*** and ownership (ownership of online content)

Another relevant work is the ***Digital Resilience Framework*** developed by members of the **UKCIS Digital Resilience Working Group** (**DRWG**) (UKCIS Digital Resilience Working Group, nd). The framework (UKCIS, 2019a) was released with a policy paper (UKCIS, 2019b), with the two papers complimenting each other in the information given. The *Digital Resilience Framework* (UKCIS, 2019a) is designed as a document whose aim is '*to provide a shared focus for decision making, placing digital resilience at the centre of considerations for organisations, communities and groups*'. Both the *Digital Resilience Framework* and the accompanying policy paper provide a definition of digital resilence and a self-assessment tool. In both documents, digital resilence is described as a 'dynamic' entity, comprising of 4 key areas: 'understand' (e.g., when they are at risk); 'learn' (e.g., from previous experiences); 'know' (e.g., which resources to use to seek help from; and 'recover' (e.g., receiving support when things go wrong online). The policy paper provides further information on each element of the self assessment. The self-assessment tool can be used by anyone and can be used on behalf of a child or a young person to assess their digital resilience.

4.2.2. *Devolved governments' policies*

'***The Strategic Framework for a Cyber Resilient Scotland*** (Scottish Government, 2021a) is a framework specific to **Scotland** in regards to cyber resilience[6]. Outcome 1 of the framework is relevant to cyber security education; '*people recognise the cyber risks and are well prepared to manage them*'. This includes '*increasing people's cyber resilience by embedding it into relevant curricula and qualifications*'. Appendix C of the framework includes notable actions relevant to cyber security education in Scotland, in particular in the 'Learning and Skills' domain (Scottish Government, 2021b). Those actions are detailed in Table 6.

Table 6: An overview of the actions and sub-actions relevant to cyber security within the Strategic Framework for a Cyber Resilient Scotland (Scottish Government, 2021a)

Main Action	Sub-action
Increase people's cyber resilience through awareness raising and engagement	• Disseminate general and targeted cyber awareness messages to individuals, groups and communities, and ensure these are in accessible/alternative formats where possible
Explicitly embed cyber resilience throughout our education and lifelong learning system	• Build capacity across school education for teachers to embed cyber resilience learning across the curriculum, with the support of training, resources and tailored guidance/support • Work with key community learning and development (CLD) partners to further embed cyber resilience learning and skills development in non-formal learning • Embed cyber resilience within initial training for education professionals • Work with colleges, universities and training providers to embed cyber resilience across their delivery • Support parents and carers to help with their children's cyber resilience
Support the development of accessible cyber security skills training pathways and effective careers guidance to help ensure that skills supply meets demand	• Grow numbers of people studying cyber security in Scotland at all levels • Increase the uptake of cyber security apprenticeship training and provision • Ensure education professionals have access to support and materials to enable them to deliver cyber-related qualifications, recognising the wider digital learning landscape • Ensure cyber security skills development opportunities are inclusive, particularly of women and girls, people from disadvantaged backgrounds, people from BAME backgrounds, and neurodivergent people, including championing skills development opportunities for under-represented groups • Co-ordinate and shape added-value/extra-curricular programmes in cyber security for effective rollout in Scotland so that they are part of a coherent offer • Support both individuals and employers navigate a complex cyber security profession, to help talent enter and develop a career in cyber security, working alongside the new UK Cyber Security Council

[6] The title of the framework shown on the web page (Scottish Government, 2021a) was '*Cyber Resilient Scotland: strategic framework*', but we were advised by our Scottish contact that the correct title should be '*The Strategic Framework for a Cyber Resilient Scotland*', which is what we use in this report.

	to develop a career pathways framework built on the Cyber Security Body of Knowledge • Work with partners at UK level to ensure appropriate alignment of cyber skills development plans • Strengthen interaction between all parts of our education and lifelong learning system around cyber security skills development to grow new pathways and opportunities • Co-ordinate, prioritise and target industry/employer engagement in education in order to promote cyber security careers and add value to cyber security skills development for young people

An interview with a colleague in Northern Ireland confirmed no similar framework in **Northern Ireland**. There is, however, a Northern Ireland specific policy titled '***Keeping children and young people safe: an Online Safety Strategy for Northern Ireland 2020-2025***' (Northern Ireland Government, 2021), with focuses uniquely on online safety. This policy mentions online safety education, specifically in regards to managing online experiences and reporting content, accessing support when required, and educating children and young people on the risks of using digital technologies.

For **Wales**, we did not find any specific framework that we could consider relevant. Cyber security is highlighted in Welsh Government's ***International Strategy for Wales*** (Welsh Government, 2020c) as one of three distinct and growing sectors "*in which Wales excels and which demonstrate how Wales is a nation committed to creativity, technology and sustainability*". This strategy has some mentions of pre-university education, but not in the context of cyber security or online safety.

4.3. Educational landscape of the UK

Education in the UK is a devolved matter. This means that education (including the curriculum, examinations and the structure of education) is managed by governments in each of the four constituent nations with no centralised mandate on how each nation should run their respective education system. In spite of the devolution of education, the length of time which pupils spend in school appears to be similar across all four constituent nations.

4.3.1. Types and length of education

Within the UK, different types of school have differing obligations in regards to the curriculum they are required to follow. Non-independent schools in England have differing levels of adherence to the English ***National Curriculum***. Maintained schools in England (i.e., schools which are funded and controlled by the local education authority (county)) have to follow the English *National Curriculum* (Department for Education (UK), 2014a). The English *National Curriculum* guides what those types of schools should cover (UK Government, nd-a). Since the Academies Act 2010 (UK Parliament, 2010), maintained schools have been able to convert to academies, one type of schools that sit outside local education authority's control) were introduced with the Learning and Skills Act 2000 (UK Parliament, 2000). Academies are funded directly by the Department for Education and partly by academy trusts, which may gain extra funding or sponsorship from other sources (for example, charities), and do not have to follow the *English National Curriculum*, but must follow a broad and balanced curriculum (UK Government, nd-a). Independent schools also do not have to follow the English *National*

Curriculum. Table 7 summarises the different types of school in England along with whether they have to follow the English *National Curriculum*.

Table 7: Types of school in England and whether they have to follow the English National Curriculum.

Type of school	Mandatory to follow the English *National Curriculum*?
Maintained schools	Yes
Academies	No
Independent schools	No

In the semi-structured interviews, the complex landscape of the different types of school in England was touched upon in regards to mandatory content to be taught:

> *"… that's why you very carefully use the word 'statutory'. So schools that are not academies, i.e., state-maintained schools, will be required to teach the National Curriculum programme of study. But as you may appreciate, most schools are no longer state-maintained. So schools need to meet the broad and balanced aims of the overall curriculum rather than being required to teach the programme of study specifically. They are required to explain and show why they may have chosen to teach something else, and why that's better for the students in their school." – Director of Education, BCS*

> *"So whereas in the past, all schools are expected to follow the national curriculum. There isn't that now because a lot of that, a lot of the high level guidance for schools, has been replaced by the autonomy that you find within things like academies. So academies can set their own curriculum, that [is how] large groups of schools essentially operate." – Online Safety Director and SMT member, South West Grid for Learning (SWGfL), England*

Academies do not exist in **Wales**, where local authorities remain responsible for funding non independent schools and the ***Curriculum for Wales*** must be followed in local authority schools.

There are schools that are nominally called academies in **Scotland**; however, these are not the same 'academies' as in England. Schools in Scotland are, in the main, state-funded, coming under the control of the local authority. Schools have the same responsibility in regards to the curriculum, where the ***Curriculum for Excellence*** is used as guidance.

In **Northern Ireland**, there are a variety of different types of school (controlled school, maintained school, voluntary schools, integrated schools) and these all hold the same responsibility in regards to following the ***Northern Ireland National Curriculum***.

The other main consideration to account for in regards to curriculum provision and differences between the four nations in the UK are the school leaving ages and the length of mandatory education. In Wales, Scotland and Northern Ireland, pupils can leave school at 16 years of age. However, in England pupils need to stay in some sort of education until they are 18, e.g., between 16 and 18 this can take the form of an apprenticeship, full-time or part-time education, training with part-time working or volunteering (up to 20 hours a week) (UK Government, nd-c). This is key to consider in terms of ISCED level 4 (age 16-18) provision.

In England and Wales, post-school (further education) colleges can be independent (fee paying) or non-fee paying (i.e., academies or maintained), and may be attached to a school (named a sixth form) or separate from a school. In Northern Ireland, there are six further education colleges, all of which are financially supported following the Funded Learning Unit (FLU) model, a distributive funding mechanism (Department for Employment and Learning (Northern Ireland, UK), 2016). In Scotland, there are currently 27 further education colleges

(Colleges Scotland, nd; CDN, nd), which are largely funded by governmental sources especially the **Scottish Funding Council** (**SFC**) and grants from **Regional Strategic Bodies** (**RSBs**) (SFC, 2020a, 2020b). Colleges in all the four UK nations do not have to follow the respective curricula, due to pupil choice of subjects at this level of education. A wide variety of qualifications can be achieved at colleges, including ***A-levels*** (Advanced levels; an academic qualification), ***BTECs*** (Business and Technology Education Council; a vocational or career-focused qualification), ***T-levels*** (a technical qualification with theory and practice combined; starting September 2020 in England), and a range of vocational qualifications.

4.3.2. Nature of cyber security education within the curricula

Cyber security education within each of the four constituent nations of the UK takes a different approach. However, they all embed it under a computing-related subject. Table 8 outlines where cyber security falls in each of the constituent nations:

Table 8: Computing-related subjects within which cyber security may be taught, across all the four UK nations

Country	Computing-related curriculum subject
England	Computer science (General Certificate of Secondary Education (GCSE)) (ICT phased out since 2019, however ICT lessons still taught)
Wales	ICT
Scotland	Computer science and technologies
Northern Ireland	ICT and digital technology

The differences in provision of cyber security education can be further observed when comparing whether computing-related subjects are mandatory or not. The move towards computer science in England is discussed in the quotation below:

> *"We saw a massive move at that time towards funding the National Centre for Computing Education, the drive for coding and … the swing away from ICT into a computing curriculum. So developing computational thinking and the ability to code … to a certain degree, we lost a lot of drivers around the broader aspects of cyber security. And now we've seen a little bit of the pendulum swinging back so that, …, we work with a really broad pallets of different skills which, …, knowledge and skills based services of which cyber is just one." – Online Safety Director and SMT member, South West Grid for Learning (SWGfL), England*

Table 9 provides an overall comparison between the four constituent nations within the UK. It is important to note that cyber security education coverage is optional in all nations in ISCED level 4 (ages 16-18). Therefore the majority of focus is on ISCED levels 0-3 with an examination of options available at ISCED level 4.

Table 9: Cyber security teaching provision within computing-related subjects in national curricula in the UK

	Age reached at school														
Nation	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
England	x	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	o	o	o	o
Wales	x	x	x	x	✓	✓	✓	✓	✓	✓	✓	o	o	x	x
Scotland	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	o	o	o	o
Northern Ireland	✓	✓	✓	✓	✓	✓	✓	✓	o	o	o	o	o	o	o

Legend: ✓ compulsory x not covered o optional

For schools in England who do have to follow the English *National Curriculum,* Computing is compulsory across ISCED levels 1-3 (ages 5-16) and has a main driver of 'digital literacy' (Department for Education (UK), 2013). There is an element of cyber security across ISCED levels 1-3 (ages 5-16) of the Computing curriculum in England, notably including keeping information safe and identifying where to go for help. This also gradually increases over key stages incrementally, but not discretely (e.g., qualitative adjectives are added; respectfully, responsibly, securely) (Department for Education (UK), 2013). Students do not have to take computing in ISCED level 3 (ages 14-16) in England, yet schools do have to offer the opportunity to study computer science during ISCED level 3 (ages 14-16) (Department for Education (UK), 2014a). There is a notable use of 'should' in guidance (Department for Education (UK), 2013, 2014a), echoing school-led decisions on what is covered. An overview of the competencies in regards to cyber security education in England is given in Table 10.

Table 10: An overview of competencies linking to cyber security education in the English National Curriculum

ISCED level (Age)	Competencies
ISCED level 1 (4-7 years)	"*Use technology safely and respectfully, including keeping personal information safe and knowing where to go for help … e.g., not sharing personal information online, respecting others privacy, awareness of the school's acceptable use policy.*" "*Pupils should know how to report concerns*" (Department for Education (UK), 2014a)
ISCED level 1 (7-11 years)	"*Use technology safely, respectfully and responsibly, be able to recognise acceptable and unacceptable behaviour and be able to report concerns about content … e.g. responsible, a focus on the impact of behaviour on others, including copyright, age restrictions on websites and keeping passwords and personal information secure.* *Pupils should be aware of their digital footprint and of school acceptable use policies and terms of conditions that they sign.*" (Department for Education (UK), 2014a)
ISCED level 2 (11-14 years)	"*Online identity and privacy are explicitly mentioned for the first time, along with recognising inappropriate content*" (Department for Education (UK), 2013, 2014a)
ISCED level 3 (14-16 years old)	General Certificate of Secondary Education (GCSE) Computer Science is available as an option for pupils to study. See Section 4.3.3.2 for a comparison of content covered, as content covered is guided by examination boards.

At ISCED level 4 (ages 16-18) in England, A-level Computer Science is available as an academic qualification. The content covered is guided by examination boards. A list of available examination boards and corresponding content will be covered in depth in Section 4.3.3.2, alongside a comparison of other examination boards.

There is a national curriculum for ISCED levels 1-3 (ages 7-16) and a framework for the ISCED levels 0-1 (ages 3-7) in Wales (Welsh Government, 2015, p2) for ICT. At ISCED level 1 (ages 4-7), pupils should get the opportunity to experience ICT (Welsh Government, 2015, p10), however it does not say which aspects of ICT, or if anything includes cyber security. At ISCED level 1, ICT remains a key part of the curriculum, however, none appears to be in the realm of cyber security education, with communicating information from a range of 'given safe and suitable sources', communicating ideas in an appropriate way, and considering how to acquire information (Welsh Assembly Government, 2008, p10). Although no direct mention of cyber security remains at ISCED level 2 (ages 11-14), an awareness of computers and information technology along with the impact it can have socially, ethically, morally and economically is mentioned for the first time (Welsh Assembly Government, 2008, p10). It is however unclear what this looks like, or if it is directly related to cyber security education. For ISCED level 3, it

has been recommended that all schools provide some sort of ICT education, with opportunity for a formal qualification (Welsh Assembly Government, 2009, p3). The ***Welsh Baccalaureate*** has a requirement for ICT, however, again it remains unclear how much is digital literacy or cyber security education focused (Welsh Assembly Government, 2009, p5). At ISCED level 4 (ages 16-18), A-level ICT is available. The content covered is guided by the examination board in Wales, the Welsh Joint Education Committee [WJEC]. Its content will be covered in depth in Section 4.3.3.2, alongside a comparison of other examination boards.

Wales also has a ***Digital Competence Framework*** (Education Wales, 2018) to assist pupils aged 3-19 to be confident users of digital technologies and systems. As part of this, there is a strand on citizenship which directly covers aspects of cyber security education (Education Wales, 2018), including:

- identity, image and reputation
- digital rights licensing and ownership
- online behaviour and cyber bullying

The curriculum in Scotland is called ***Curriculum for Excellence*** (Education Scotland, nd-a) and computing as a subject fits into the curriculum area 'Technologies' (Education Scotland, 2015). Education Scotland emphasises that '*digital literacy should be placed at the heart of all learning*', meaning that aspects of digital literacy may be covered in other subjects, however, how this occurs appears to be down to the teacher's discretion (Education Scotland, 2018).

> *"Scotland has a devolved education system and policy and we do not have a mandated curriculum. We have guidelines and benchmarks that young people can expect to reach through their education. It's a flexible curriculum and you can have in theory, learners in classrooms learning at different levels." – Cyber Resilience Coordinator for Learning and Skills, Scotland*

Digital literacy is a compulsory component of '*broad general education*' (Education Scotland nd-a). Experiences and Outcomes (Education Scotland, 2018) provide a framework for what is to be covered. The relevant benchmarks for cyber security education sit under the '*cyber resilience and internet safety*' aspect of the technologies framework (Education Scotland, 2017), under the header '*digital literacy*'. Table 11 gives a detailed overview of the benchmarks set by the Education Scotland on the technologies framework.

Table 11: A detailed overview of cyber security education included in the Scottish Technologies framework

ISCED level (Age)	Competencies
ISCED level 0 (3-5 years)	*"I can explore, play and communicate using digital technologies safely and securely."* (Education Scotland, 2017) Includes appropriate behaviour and the importance of keeping passwords safe
ISCED level 1 (5-8 years)	*"I can extend my knowledge of how to use digital technology to communicate with others and I am aware of ways to keep safe and secure."* (Education Scotland, 2017) Includes: rights and responsibilities as a digital citizen (however no further explanation of this), understanding of dangers and who to report concerns to, why strong passwords are needed and consent regarding photographs
ISCED level 1 (8-11 years)	*"I can explore online communities demonstrating an understanding of responsible digital behaviour and I'm aware of how to keep myself safe and secure."* (Education Scotland, 2017) Includes: content that should go on an online profile, importance of being a responsible digital citizen, know how to report concerns, uses strong passwords and understands legislation in regards to inappropriate internet use.

ISCED level 2 (12-15 years)	*"I can keep myself safe and secure in online environments and I am aware of the importance and consequences of doing this for myself and others."* (Education Scotland, 2017) Includes: legal implications of protecting one's own and others' identities online, applying relevant online safety features, understands cyberthreats e.g., theft, phishing; understands device security; evaluates own online presence; understands device safety. *"I can explore the impact of cyber-crime for business and industry and the consequences this can have on me."* (Education Scotland, 2017) Includes: understands how industry collects data ethically; understand how cyber-security breaches impact individuals; evaluate digital footprints and identify good practice; identify main causes of data security breaches; understands how to safely dispose of devices
ISCED levels 3 and 4 (15-18 years)	Students can take computing at N5 (GCSE equivalent), Higher or Advanced Higher. National 5: The course does not have a component covering aspects of cyber security or similar, other than why machines may be encrypted and firewalls as part of security precautions in computer systems (SQA, 2021a). Higher: The course does not specify cyber security as a component of the course, however, some relevant topics are included such as security risks and precautions including legislation (Computer Misuse Act 1990), security risks of tracking cookies and encryption in transmission of data (SQA, 2021b). Advanced Higher: The course does not specify cyber security as a component of the course, however security risks and precautions including the security risks of SQL code injections are covered (SQA, 2019).

In addition to Nationals, Highers and Advanced Highers in Scotland, cyber security specific qualifications are also available through the SQA, notably in the case of pre-university education. The two relevant qualifications to pre-university pupils are ***Award in Cyber Security Fundamentals*** and ***National Progression Award (NPA) in Cyber Security***. Table 12 shows an overview of these qualifications.

Table 12: An overview of cyber security specific qualifications in Scotland

Qualification	ISCED level	Pre-university pupils ages	Course description	Outcomes covered
Award in Cyber Security Fundamentals	2	14-18	One unit introduces basic knowledge and skills relevant to cyber security.	*"State common cyber security threats to individuals, businesses and nations."* *"Describe routine defensive measures to minimise the risks posed by these threats."* *"Secure a digital device for personal use."* (SQA, 2015a)
NPA in Cyber Security	2-3	14-18	Three national units comprising of: Data Security, Digital Forensics, Ethical Hacking (SQA, 2015b). This course can be taught at SQF levels 4, 5 and 6. The units remain the same, with the amount and complexity of content changing per level (SQA, 2015b).	See Table 14 for a detailed overview of outcomes for each unit at each SCQF level.

Each module on the NPA in Cyber Security can be taken at Scottish Credit and Qualifications Framework (SCQF) levels 4, 5 and 6 (SQA, 2015b). SQCF levels are specific to Scotland. A short overview of SCQF levels 4, 5 and 6, and how these map across to ISCED levels are given in Table 13. This overview is given to aid clarity of the different achievement levels, as the same qualification is available at 3 different SCQF levels.

Table 13: SCQF levels 4-6 mapped against ISCED levels

SCQF level	ISCED level
4	2
5	2
6	3

The NPA in Cyber Security contains 3 main units, whose outcomes at each of the three SCQF levels are shown in Table 14.

Table 14: Outcomes of the NPA in Cyber Security in Scotland, differentiated by SQE level

Unit Name	SCQF level 4	SCQF level 5	SCQF level 6
Data security	*"Describe how personal data can be stored, used and shared by social media."* *"Identify the risks associated with storing and sharing personal data."* *"Apply basic practical methods of protecting personal data."* (SQA, 2015c)	*"Describe the legal and ethical obligations around storing and sharing personal and business data."* *"Explain the causes and effects of data security breaches."* *"Protect data against security breaches."* (SQA, 2015f)	*"Analyse the approach to data security made by organisations."* *"Investigate technologies and strategies used by businesses to protect customer data."* *"Create a security strategy for a small business."* (SQA, 2015i)
Digital Forensics	*"Describe the steps in the digital forensics process."* *"Apply basic techniques of data acquisition."* *"Examine digital evidence."* (SQA, 2015d)	*"Explain the digital forensics process."* *"Apply relevant techniques in acquiring data."* *"Examine digital evidence."* (SQA, 2015g)	*"Explain the digital forensics process and job roles."* *"Apply complex techniques in acquiring data."* *"Evaluate digital evidence."* (SQA, 2015j)
Ethical Hacking	*"Identify current legislation relating to computer crime."* *"Describe the basic methods that ethical and malicious hackers use to compromise computer systems."* *"Apply basic hacking methods to compromise computer systems in a controlled environment."* (SQA, 2015e)	*"Describe current tools and techniques used by ethical and malicious hackers to compromise computer systems."* *"Explain current legislation relating to computer crime and hacking."* *"Perform a routine penetration test on a computer system within a controlled environment."* (SQA, 2015h)	*"Analyse current trends in cybercrime."* *"Evaluate contemporary legislation relating to cybercrime."* *"Perform a complex penetration test on a computer system in a controlled environment."* (SQA, 2015k)

In the NPA in Cyber Security, pupils have the opportunity to mix and match SCQF levels across units whilst undertaking the qualification, earning a group award at the level of the lowest-levelled unit taken (SQA, 2015b).

Using ICT is a key component of the **Northern Irish Curriculum** in primary schools (ISCED level 1; ages 5-11) (CCEA, 2007, p5), however it appears integrated into other parts of the curriculum and not taught as a 'standalone subject'. Northern Ireland introduced online safety as part of their curriculum in 2009 (CCEA, nd-a). The main element is understanding how to stay safe online and understanding acceptable behaviour online (CCEA, 2007, p7). For pupils in ISCED level 2 (aged 11-14), each school makes their own decision about how best to interpret and combine minimum requirements so as to provide a broad and balanced curriculum (CCEA, nd-b). Online safety is also a key element of ICT lessons, with online safety and acceptable behaviour online as key components of the ICT curriculum at ISCED level 2 (CCEA, 2019a, p27). No further information on cyber security or online safety education is stipulated. For pupils at ISCED level 3 (aged 14-16), ICT is a key part of the curriculum (CCEA, 2019b, p20), however, online safety and cyber security do not appear to be a part of the curriculum. At ISCED level 4 (ages 16-18), A-level Digital Technologies is available. The content covered is guided by the **Council for the Curriculum, Examinations & Assessments (CCEA)**, the examination board in Northern Ireland. Its content will be covered in depth in Section 4.3.3.2, alongside a comparison of other examination boards.

4.3.2.1 Vocational subjects

T-levels are a new qualification being rolled out in **England** from September 2020, combining both academic and practical content and skills. These are different to A-levels, which will be covered in Section 4.3.3.2, and provide a mixture of academic study and work experience throughout the course. Two T-levels qualifications contain information technology content and aspects of cyber security in a broad manner:

- **T-level in Digital Production, Design and Development** (UK Government, nd-d)**: '***the ethical and moral implications of digital technology*', '*legal and regulatory obligations relating to digital technologies*', '*the privacy and confidentiality of personal data*', and '*the technical, physical and human aspects of internet security*'.
- **T-level in Digital Support Services** (UK Government, nd-e)**:** the above four points, '*using digital technologies to analyse and solve problems*', and '*digital environments, including physical, virtual and cloud environments*'.

There are over 2,000 ***Business and Technology Education Councils (BTECs)*** across 16 sectors at three levels, of which two are at pre-university level: ***BTEC Firsts*** (at ISCED level 3 equivalent), ***BTEC Nationals*** (at ISCED level 4 equivalent) (UCAS.com, 2021). *BTECs* are studied across all nations in the UK. *BTEC Nationals* are well regarded by many universities, with some pupils using them to gain entry to courses instead of Advanced (A-)levels (UCAS.com, nd). *BTEC* courses are vocational courses, often with a large practical element, with assignments based on real life scenarios (Pearson Edexcel, 2018). Table 15 lists BTECs pre-university education with a cyber security component.

Table 15: An overview and comparison of BTECs with cyber security components.

BTEC course name	Contents and units relevant to cyber security
Digital Information Technology (BTEC First)	Threats to individuals, e.g.: invasion of privacy, targeting vulnerable groups of people, inaccurate data could be stored. (Pearson Edexcel, 2019) Data security on cloud technologies (Pearson Edexcel, 2019) Cyber security – Why systems are attacked; External threat; Internal threats; Impact of security breaches (Pearson Edexcel, 2019) Management of data threats – User access restriction; Data level protection; Finding weaknesses and improving system security (Pearson Edexcel, 2019)

Information Technology (BTEC First)	Understand the impact of IT on individuals, communities and society (Pearson Edexcel, 2010)
Computing (BTEC National)	Unit 7: IT Systems Security and Encryption (Pearson Edexcel, 2020a)

4.3.2.2 Non-computing subjects

All schools have to make provision for ***Personal Social and Health Education*** (***PSHE***) in **England** (Department for Education (UK), 2014a), of which ***Relationships Education*** and ***Relationships and Sex Education*** is a part of. Online safety is to be covered within *Relationships Education* (ISCED level 1) and *Relationships and Sex Education* (ISCED levels 2 and 3). Within ***Citizenship Education***, media literacy is covered, which is linked with the area of cyber security education (e.g., online mis- and disinformation).

Wales released guidelines for the Health and Wellbeing aspect of the ***Curriculum for Wales*** in 2020 (Welsh Government, 2020a), however in the Description of Learning statements that guide this documentation, there appears to be no mention of online safety (Welsh Government, 2020b). No mention was found of online safety in the accessible information, however it is possible that the **PHSE Association** provides resources on online safety for Welsh schools (PSHE Association, nd-b).

In **Scotland**, the equivalent subject to PSHE is Health and Wellbeing education. The six areas of Health and Wellbeing education are (Scottish Government, nd):

- mental, emotional, social and physical wellbeing;
- planning for choices and changes;
- physical education, physical activity and sport;
- food and health;
- substance misuse;
- relationships, sexual health and parenthood.

No explicit mention of online safety is made in the curriculum guidance, but Education Scotland has undertaken an exercise to map elements of the Health and Wellbeing curriculum to the cyber resilience and internet safety Experiences and Outcomes.

Northern Ireland's subject ***Personal Development and Mutual Understanding*** (***PD&MU***) is the equivalent of PSHE and Health and Wellbeing in England, Wales and Scotland (CCEA, nd-c). There are resources available for teachers to use, however there are no units pertaining to online safety.

4.3.3. Assessment methods

Computing-related subjects undergo a variety of internal (by teachers) and external (by exam boards) assessment methods which differ across all the constituent nations in the UK.

4.3.3.1 Internal Methods

In terms of internal assessment, levels no longer exist in the English ***National Curriculum*** in **England**, and it is down to individual teachers to mark assessment and mastery (Department for Education, 2014a). **Computing at School** (a community of practice for teachers of computing related subjects in the UK) has recommended teachers to use a criteria-based approach to assessment. However, there is no obligation for this and schools have complete liberty in how they assess competencies (e.g., has the child mastered this?) as guidance only stipulates that pupils should reach set targets (Department for Education, 2014a). Previously,

levels 1-7 were used to assess pupils' knowledge (EdPlace.com, nd; TheSchoolRun.com, nd-b), however, cyber security and digital literacy were not allocated to these levels given the changes in curriculum.

Wales uses a system similar to the previous system that England used, with assessment levels (1-8) to denote progress (Welsh Assembly Government, 2008, p10). These levels are different to ISCED levels, and demonstrate if a pupil has met required competencies at each ISCED level. It has been recommended that all schools provide some sort of ICT education and qualification, however, it is at the school's discretion whether this occurs (Welsh Assembly Government, 2009, p3). In Northern Ireland, teachers are not obligated to use Levels of Progression at ISCED level 3 (ages 14-16) (CCEA, 2019b, p20).

Teachers in **Scotland** use a variety of assessment approaches, formative and summative, to explore children and young people's skills, knowledge and understanding within the appropriate level taking account of learning that will have taken place throughout the session (Education Scotland, 2021). Due to context and experiences this will vary across sectors and establishments. As such, there are no general assessments for digital literacy (and for the '*cyber resilience and internet safety*' aspect) but teachers will assess learners' progress against the Technologies' Experiences and Outcomes at the appropriate level (ibid).

4.3.3.2 External methods

The four constituent nations have a varying number of exam boards and qualifications. **England** has various exam boards for ***General Certificate of Secondary Education*** (***GCSE***) and ***Advanced (A-) levels*** including **Eduqas**; **Assessment and Qualifications Alliance** (**AQA**); and **Oxford, Cambridge and RSA Examinations** (**OCR**). Each has their own syllabus for pupils to cover which differs slightly. In the other three constituent nations, there is just one main exam board – **Welsh Joint Education Committee** (**WJEC**) in **Wales**, **Council for the Curriculum, Examinations & Assessments** (**CCEA**) in **Northern Ireland**, and **Scottish Qualifications Authority** (**SQA**) in **Scotland**. WJEC also offers the same qualifications in England, under a different brand name, **Eduqas**. England, Wales and Northern Ireland have GCSEs and A-levels, whereas Scotland has its own qualification system of ***National 4*** and ***5***s, ***Highers*** and ***Advanced Highers***.

Due to the variety of exam boards across the UK in spite of similar qualifications, Table 16 shows a comparison of cyber security related topics covered in each qualification at GCSE, Advanced Subsidiary (AS-) and A-levels in England, Wales and Northern Ireland.

Table 16: A comparison of cyber security related topics covered by different exam boards in the UK

	AQA	CCEA*	OCR	Pearson Edexcel	WJEC/Eduqas
GCSE	Fundamentals of cyber security; Ethical, legal and environmental impacts of digital technology on wider society, including issues of privacy (AQA, 2020)	Cyberspace, network security and data transfer; Ethical, legal and environmental impact of digital technology on wider society (CCEA, 2019c)	Network Safety; Ethical, legal, cultural and environmental impacts of digital technology (OCR, 2021a)	Network security; Ethical and legal; Cybersecurity (Pearson Edexcel, 2020b)	Data security; Network security; Cyber security; Ethical, legal and environmental impacts of digital technology on wider society (WJEC, 2019a)

AS level	Consequences of uses of computing; Encryption (AQA, 2019)	No content covered (CCEA, 2019d)	Exchanging data; Legal, moral, cultural and ethical issues (OCR, 2021b)	NA	Data security and integrity processes; Economic, moral, legal, ethical and cultural issues relating to computer science (WJEC, 2019b)
A level	Consequences of uses of computing; Encryption; Internet security (AQA, 2019)	Describe the threats to the privacy of the individual from the use of data mining; Individual, social and legal considerations (CCEA, 2019d)	Exchanging data; Legal, moral, cultural and ethical issues (OCR, 2021c)	NA	Data security and integrity processes; Economic, moral, legal, ethical and cultural issues relating to computer science; Data transmission (WJEC, 2019b)

* CCEA does not offer a computer science GCSE or A-level, however it offers 'Digital technologies' which appears to cover much of the same content.

4.4. Implementation landscape

How educational initiatives and policy are implemented across the UK appears to be idiosyncratic and dependent on many factors, including access, awareness and funding. In this section, initiatives and how policy is implemented will be examined under three domains: government and national agency action and initiatives, communities of practice, and charities and NGOs. One aspect which is fundamental to understanding provision amongst the implementation landscape is the **fragmentation** and **disconnected nature** of many initiatives:

> *"I think the feedback that we get that was that, within government there is a very confusing and very busy picture. So there are lots of many different disparate activities, but they're not all brought together to create that clear strategy and that clear vision." – CyberFirst employee, HM Government*

The differences between different types of school in regards to difficulties in disseminating initiatives and programmes were also noted, with this example coming from a Northern Irish context in regards to schools:

> *"We also have other bodies such as Catholic schools and other faith schools, those sorts of things, which would have their own governance structures." – Head of NI Cyber Security Centre, Northern Ireland*

This fragmentation at both the school side and the implementation side demonstrates how disconnected the picture in regards to cyber security education is, and how this impacts the number of initiatives and programmes related to cyber security, and who they are reaching.

4.4.1. Government and national agency actions and initiatives

Children's commissioners can be an important source of information for online safety, and for promoting the importance of online safety and cyber security for children and young people. Table 17 summarises whether the four constituent nations have a children's commissioner and any relevant work they have done on cyber security and online safety.

Table 17: Existence of a children's commissioner in the four constituent nations in the UK

Country	Children's Commissioner?	Any relevant work to cyber security and online safety
England	Yes, named Children's Commissioner for England	Online safety and wellbeing kit for parents and safety guide for children (Children's Commissioner for England, nd).
Wales	Yes	Report in 2019 on children's experiences of cyber bullying (Children's Commissioner for Wales, 2019).
Scotland	Yes, named Children's and Young People's Commissioner Scotland (CYPCS)	Information available on online safety (CYPCS, nd-a) Signposts to ThinkUKnow and CEOP (CYPCS, nd-b).
Northern Ireland	Yes, named Northern Ireland Commissioner for Children & Young People (NICCY)	Information for parents and carers on online safety (NICCY, nd)

We will examine UK-wide government and national agency actions and initiatives regards to other governmental and national agency action initiatives. All initiatives and actions in this section lie at a UK-wide level.

The **Ofsted** inspectors have assessed how well online safety is taught in primary schools in all parts of the UK since the ***Cyber Crime Strategy*** release (Home Office (UK), 2010), this includes in reference to the PSHE curriculum (Ofsted, 2021). Inspectors also comment on the safeguarding policies of the school being inspected and the culture surrounding safeguarding (Ofsted, 2021). However, some schools do not appear to have sufficiently comprehensive online safety policies (NFER, 2014).

The **NCSC** runs the ***CyberFirst*** programme, which offers extra-curricular educational opportunities to 11-17 year-olds (at ISCED levels 2-4) who are interested in cyber security and technology (NCSC-UK, nd-a). The aim of *CyberFirst* is to *'identify and nurture the future generation of cyber security experts to keep the UK safe in the future'* (NCSC-UK, 2021b). A Cyberskills hub has been piloted in Gloucestershire since 2018 (NCSC-UK, nd-b) and currently the pilot has been widened to include both Gloucestershire and Wales (NCSC-UK, nd-b). Schools that take part can be awarded with a gold, silver or bronze award (NCSC-UK, 2021b):

- Gold: awarded for three years; delivering excellence
- Silver: awarded for two years; delivering good standard
- Bronze: awarded for one year; aspiring to deliver excellence

> *"It felt to be an appropriate way to gauge where we were. So it was a really good opportunity to figure out what we do well and then what we need to do to up our game, because we're very reflective, very inward looking, and I'm not afraid to make changes based on what comes out of that. … The one thing that has changed dramatically is the fact we've got more and more companies doing digital talks on lunchtimes, … obviously kind of being the key thing in that. But we've got upwards of 20 talks over the year." – Assistant Head Teacher, England*

The awards take into consideration teaching on specific aspects of cyber security, CPD of staff, numbers of pupils taking Computing/ICT, and wider school strategy (NCSC-UK, nd-b; NCSC-UK, 2021b). There does not appear to be a given list of concepts to teach, and the assessment for these awards is holistic, e.g., it looks at current school teaching plans. This is in addition to the curricula of the four constituent nations and is a UK-wide initiative, based in existing schools. Gold-awarded schools provide cyber security education for all year groups and teaching CPD

opportunities for teachers (NCSC-UK, 2021b), ***CyberFirst*** enrichment activities and 1.5 hours per week of computing/ICT teaching at ISCED level 2 (ages 11-14).

> *"But as a CyberFirst school, three standards, Bronze, Silver and Gold. So for the Gold and Silver, they do have to be offering computer science at GCSE level or equivalent, and at Bronze, they should be trying to aspire. That's about the only qualification per say that we look at." – CyberFirst employee, HM Government*

CyberFirst also supplements Ofsted's framework (NCSC-UK, 2021b), including: quality of education, behaviour and attitudes, personal development and leadership and management (NCSC-UK, 2021b). Schools apply to and opt into *CyberFirst*. In regards to how this is recorded on any student record of achievement, Scotland have taken the step to record attendance on a CyberFirst programme as part of a pupil's record of achievement.

> *"The Scottish Qualifications Authority, our awarding body, accepts as evidence attendance or completion of one of the CyberFirst residential summer courses as evidence of learning towards the National Progression Awards in Cyber Security at three different levels." – Cyber Resilience Learning and Skills Coordinator, Scotland*

CyberAware (a campaign from the NCSC) has a collection of advice from the government regarding cyber security, but no focus on under 18s, rather a general population focus (NCSC-UK, nd-a). Six actions are recommended to improve your cyber security, including: using a strong and separate password for your email; creating strong passwords with three random words; saving your passwords in your browser; turning on two-factor authentication; updating your devices; backing up your data (NCSC-UK, nd-a).

The NCSC has also provided information for schools in assisting them become more 'cyber secure', however this appears to be targeted at adults and staff (e.g., teachers, administrators) rather than pupils under the age of 18 (NCSC-UK, 2019). This includes:

- why cyber security is important for schools
- why schools may be targeted
- why people undertake cyber crime
- the importance of strong passwords, two-factor authentication and locking your computer when you step away from it
- suggestions on how to make a strong password
- guidance on managing phishing emails and how to spot phishing emails
- using USBs safely
- safety working from home

CyberDiscovery was the UK Government's free online extracurricular programme with a focus on cyber security and online safety, funded by the **DCMS** as part of the *National Cyber Security Strategy* (CyberDiscovery, nd). The programme worked through an online game and was designed for 13-18-year-olds with the aim of training them to be the next leaders in cyber security. The programme was in three stages: ***Cyberstart Assess***, ***Cyberstart Game***, and ***Cyberstart Essentials***.

Each stage had to be completed before moving onto the next, and stages were not permanently open. *Cyberstart Game* and *Cyberstart Essentials* provided training materials and tools used in the cyber security industry. Within Cyberstart Essentials, the final exam was provided by GIAC (Global Information Assurance Certification) (CyberDiscovery, 2021). The *CyberDiscovery* programme closed on 30th June 2021, with another programme under development. ***Cyberstart Compete*** and ***Cyberstart Elite*** are mentioned as part of the

programme with further training with real life professionals, however no information on these were found at the time of writing this report.

The **NCA** run the ***Cyber Choices*** programme (NCA, nd), an initiative *'created to help people make informed choices and to use their cyber skills in a legal way'*, i.e., to help enhance awareness of cyber crimes with children and young people as a preventative measure. It provides resources (including professionally made videos) for children and young people, but also has dedicated resources for parents/guardians/carers (NCA, 2021a) and teachers (NCA, 2021b). The NCA also work with educational partners such as **PSHE Association** and **Barefoot Computing** (Barefoot Computing, nd-a) to develop lesson plans covering cyber security related topics such as cyber crime, decision making and victim awareness (PSHE Association, 2019; Barefoot Computing, nd-b).

The NCA's **Child Exploitation and Online Protection Command** (**CEOP**) have several initiatives that support the implementation of online safety education of children and young people, parents/carers, professionals and private sector organisations (CEOP, nd). Such initiatives are delivered mainly via the public-facing website **ThinkUKnow** (nd-a), maintained by the CEOP. The resources for 4-7 year-olds are based on a dedicated animation series of ***'Jessie & Friends'*** (ThinkUKnow, nd-b), and those for 8-11 year-olds are based on both the ***'Play Like Share'*** animations and the ***Band Runner*** game (ThinkUKnow, nd-c). For both age groups, there is separate guidance for parents and carers (ThinkUKnow, nd-d; nd-e), and for children's workforce (ThinkUKnow, nd-f; nd-g). Components found in the resources for 4-7 year-olds and 8-10 year-olds include: distinguishing between safe and unsafe behaviours, knowing when to seek help and how to stay safe online. Resources for older children (11-13 year-olds and 14-plus) (ThinkUKnow, nd-h; nd-i) appear to be more self-facilitating (learners access the resources of their own accord and work through the resources at their own pace).

In addition to its policy work, the **UKCIS** also created the ***UKCIS Digital Passport*** as a communication tool to 'support children and young people with care experience to talk with their carers about their online lives' (Internet Matters, 2021). There are resources for both children and young people, and also for adults and carers.

National Cyber Resilience Centres (CRCs) in England and Wales provide advice and educational resources (National Cyber Resilience Centre Group (UK), nd). Table 18 shows the current national CRCs and their provision in regards to cyber security education.

Table 18: National CRCs in the UK as of Febaury 2022, and if they had any cyber security educational activities (National Cyber Resilience Centre Group (UK), nd)

Cyber Resilience Centre	Cyber security education?
Business Resilience Centre for the North East	Business focus. No education (Business Resilience Centre for the North East, nd)
Cyber Resilience Centre for the North West	Business focus, no education (Cyber Resilience Centre for the North West, nd)
Cyber Resilience Centre for the East Midlands	Business focus, no education (Cyber Resilience Centre for the East Midlands, nd)
Cyber Resilience Centre for the West Midlands	Business focus, no education (Cyber Resilience Centre for the West Midlands, nd)
Cyber Resilience Centre for the South East	Business focus, no education (Cyber Resilience Centre for the South East, nd)
Cyber Resilience Centre for the South West	Business and charity focus, no education (Cyber Resilience Centre for the South West, nd)

Cyber Resilience Centre for Wales	Business focus, no education (Cyber Resilience Centre for Wales, nd)
Eastern Cyber Resilience Centre	Education resources and information mainly focus on resilience in the education sector and training for schools and staff, rather than education for children and young people (Eastern Cyber Resilience Centre, nd)
Cyber Resilience Centre for London	Under development

4.4.2. Communities of Practice and Resources

As mentioned in Section 4.1, various communities of practice and teaching resources exist in the UK to help assist teachers and their teaching of computing and computing related subjects, and the most relevant ones are **Barefoot Computing**, **CAS** (**Computing at School**) and **NCCE** (**National Centre for Computing Education**). Scotland hosts communities of practice on its national schools intranet, ***Glow***, where learning and teaching resources are hosted.

Communities of practice for teachers have been focused upon, as teachers' own knowledge and understanding of topics impacts pupil learning experiences. Furthermore, a lack of specialist teachers was gleaned from the semi-structured interview stage of the research project, therefore understanding what is available to support teachers is of vital importance.

> *"Because if you don't have the technical team and we're quite lucky, we've got five specialists in our team. …, I have to plan this as if I could get run over by a bus. Yeah. Because selfishly, I would do the infrastructure one if I leave and I say if I get over by bus, then there's a gap. So I think we'll end up doing the support and then customising it a little bit." – Assistant Headteacher, England*

Barefoot Computing provides resources for, and supports teachers who teach computing and computing related subjects at ISCED level 1 (ages 4-11) computing (Barefoot Computing, nd-b). Lesson plans (Barefoot Computing, nd-c) and online guides for teachers (Barefoot Computing, nd-d) are available to help guide teachers plan lessons and also understand the content which they will be teaching. Barefoot Computing is part of CAS, and partnered with the NCCE (Barefoot Computing, nd-d).

The **CAS** is a community for teachers to share lesson plans, knowledge about computing and computing related topics and to further their own knowledge of computing and computing related subjects. There is a community forum (CAS, nd-b) where teachers can ask questions and gain answers and ideas to try in the classroom from other teachers who teach computing at ISCED levels 1-4 (ages 5-18).

The **NCCE** supports teachers of computing and computing related subjects at ISCED levels 1-4 (ages 5-18), including lesson plans, teacher continuing and professional development (CPD) and access to 34 computing hubs which are located around England (NCCE, nd-b).

> *"And then there is the National Centre for Computing Education, and the Teach Computing Curriculum – a complete curriculum which includes every single lesson for the computing programme of study. From year 1 through to year 11, there's a curriculum route through GCSE Computer Science, as well as a non-GCSE route. There is a specific cyber security unit features in year 9. And there's also a unit which is focused on understanding your data and understanding." – Director of Education, BCS*

Glow is a Scotland-specific initiative (Glow, nd), which is an intranet for all Scottish schools (teachers and pupils). This is mentioned as part of the Home Office *Cyber Crime Strategy* regarding education for young people against cyber crime.

The **Association for Citizenship Teaching** (ACT) also has resources for teachers publicly available on the teaching of media literacy for pupils at ISCED levels 2 and 3 (ACT, nd). The resources include a PowerPoint, worksheets and source sheets. The focus of these teaching resources is the COVID-19 pandemic.

As mentioned in Section 4.4.1, some educational organisations such as **PSHE Association** and **Barefoot Computing** have been collaborating with the **NCA** to develop cyber security related lesson plans (PSHE Association, 2019; Barefoot Computing, nd-b).

4.4.3. Companies, charities and non-government organisations (NGOs)

Another manner in which cyber security education can be provided is through information from companies, charities and NGOs, such as **SWGfL**, **NSPCC** and **Cyber Security Challenge UK** mentioned in Section 4.1. This educational provision is a mixture of both cyber security focused provision (e.g., Cyber Security Challenge UK) and online safety (e.g., NSPCC).

360safe is a self-review tool which schools and academy trusts can use to assess their online safety policies and develop good practice in regards to cyber safety (SWGfL, nd-b, nd-c). It remains unclear whether cyber security teaching is a core part of the self-assessment, however, case studies of the 360safe tool include schools increasing their digital skills and cyber security teaching. For ISCED level 0, a pre-school version of 360safe called ***360 Early Years*** has also been developed (SWGfL, nd-d). Another initiative from SWGfL is ***ProjectEVOLVE*** (SWGfL, nd-d), which is a content library based on the **UKCIS** *'Education for a Connected World'* document (UKCIS, 2020), with teacher CPD, lesson plans and activities, and research connected to each of the 330 statements in the *'Education for a Connected World'*. The content is written by the **UK Safer Internet Centre** (UK Safer Internet Centre, nd-d), a partnership of three organisations in the UK: **Childnet International**, **IWF** (**Internet Watch Foundation**) and **SWGfL**.

Childnet International, which is recommended in government policy as a useful resource and tool, provides information and guidance on how teachers and professionals can talk to children and young people about online safety, including cyber security (Childnet International, nd-a). They recommend sharing enthusiasm about technology, integrating elements of online safety and cyber security beyond Computing and ICT lessons and safety advice being age appropriate. Childnet also provides a teachers and technology toolkit; with passwords, online reputation, modelling how to use technology and following school policies on online and computer behaviour (Childnet International, nd-b). This echoes recommendations given by other providers (e.g., UKCIS) and appears to focus more on staff behaviour rather than what to teach pupils, despite the apparent overlap.

Childnet International also have a variety of resources to support cyber security education for children and young people. For instance, ***Digiduck*** is a collection of activities designed for children aged 3-7 (ISCED level 0-1) as a resource for parents, carers and teachers to use (Childnet International, nd-c). The resources include ebooks, PDFs, a poster and an interactive app, and cover elements of cyber security, including internet safety rules, writing emails and using online chat forums and messengers. Another useful resource is the ***STAR SEND Toolkit*** (Childnet International, nd-d), a toolkit for children and young people aged 11-16 who are disabled or have additional learning needs (e.g., are autistic, have a learning disability). The toolkit includes videos and lesson plans, and is configured around: safe, trust, action and respect. Another example is the ***Childnet Digital Leaders Programme*** (Childnet International, nd-e), which provides children and young people with a peer-to-peer online training programme

assisting online safety education in schools. The programme uses an online platform working through modules, using games as the main teaching tool.

The **NSPCC**, along with Childnet International, have ***online safety courses*** for those who work with children (NSPCC, nd-a), however, these are not for children or young people. The main focus of the course is exploring the dangers children and young people face online, and children and young people's behaviour online (NSPCC, nd-a). The NSPCC also has advice for parents teaching children about internet and online safety (NSPCC, nd-b). Although cyber security is not explicitly mentioned, open conversation and a keen interest in the child's activity is recommended, with a focus on games and apps and asking children how they know their friends online. No mention is given regarding passwords or sharing of content (other than livestreaming and risky content). **Barnardo's** (2021) offer similar information and resources. No resources are linked. The NSPCC's Online Safety Resources (NSPCC, nd-c) recommend resources from **ChildLine** (ChildLine, nd), which is mainly focused on online safety in regards to content sharing and reporting abuse.

The **Cyber Security Challenge UK** is a provider of cyber security competitions and learning programmes within UK. ***CyberCenturion***, open to UK residents and residents of British Overseas Territories who are between 12 and 18 years old (Cyber Security Challenge UK, nd-b), is one of Cyber Security Challenge UK's offer for children and young people. The competition is free to enter and currently not yet open for registration, however, interest for the next competition can be registered. The Cyber Security Challenge UK also provide a schools programme, including ***Cyber Challenge in a Box*** (Cyber Security Challenge UK, nd-c) for pupils at ISCED levels 1-2 (age 10-14).

Stop Online Abuse also provides a comprehensive list of resources in regards to online safety and cyber security (Stop Online Abuse, nd) with a large focus on identifying and getting support with online abuse. Other aspects of cyber security are not covered.

Safe4Me (Safe4Me, nd) has resources on online safety, which include lesson plans to be used by teachers and other group facilitators focused on cyber bullying, sexting and reporting inappropriate content online. Another similar NGO providing online safety information for children is **MoodSpark** (MoodSpark, nd), which focuses on 10-16 year-olds.

4.4.4. Non-school contexts supporting extra-curricular learning

In regards to where these initiatives are implemented, it appears not all occur within a curricular or extra-curricular school framework. Both Scotland and Northern Ireland reported in interviews working alongside young people in an educational context outside of school, for example, with youth workers, or uniformed groups (e.g., Scouts, Guides, Boys' and Girls' Brigade).

> *"We are doing significant work with these organisations to build capacity amongst youth workers to deliver sessions 'off the shelf' – in the way a youth worker might deliver learning about drugs or sexual health or that sort of thing. So – not a formalised curriculum, but for example, this is how to run a session on good passwords; this is how to run a session on what you put online, how to stay safe online, and your digital rights." – Cyber Resilience Learning and Skills Coordinator, Scotland*

> *"We're doing things outside of the traditional old sort of school environment. We're working quite closely with the non-uniformed and uniformed groups of Girl Guides, Scouts, Boy's Brigade, cadets, that sort of thing." – Head of the Northern Ireland Cyber Security Centre, Northern Ireland*

This shows different approaches to settings for cyber security education, and how non-school contexts can support cyber security education, particularly in the case of online safety.

4.5. Socio-cultural landscape

Digital skills are perceived as inherently **important in the job market** in the UK, a finding which was supported by interviewees who took part in the semi-structured interview stage of the research project. This is in spite of a lack of awareness of what a career in cyber security may look like more broadly:

> *"…. kind of the relevance of computing as a subject and on all career pathways, not just a cyber pathway, not just a tech pathway, but to be a nurse, to be a doctor, to be a teacher, you've got to have great digital skills." – Director of Education, BCS*

> *"I guess to kind of summarise the where digital and coding sit is like a right, like maths and English, you're going to need to use it for just about every job. And that's not the paradigm shift that the education has taken yet is it's a fundamental right to be employable. You probably need to have the basics of Excel in just about every job, let alone word processing capability and being able to use technology to express, …, electronic stuff." – CyberFirst employee, HM Government*

> *"A lot of that has been stripped out over the last 10 years to focus purely on the computation on the coding, and we're beginning to see the results of those gaps. It is very interesting that when after not having 10 years of good broad information and communication technology curriculum, and as being swapped out for computing knowledge, we've seen a large number of children not taking computing as a specialism, whereas they would be before. But over the pandemic, when young people are asked to work from home, many struggle because they didn't have the broader business-based IT skills to operate the sorts of things we're using now, even simple things like work [with] Word … [and] … PDF [files], those sorts of things or well, …, copy a table from a PDF into a spreadsheet or vice versa." – Online Safety Director and SMT member, South West Grid for Learning (SWGfL), England*

Another vital aspect of the socio-cultural landscape within the UK was who cyber security was perceived to be for, and the **stereotypes** that appear to be associated with those who work in cyber security. These stereotypes appeared to be one of the aspects fuelling under participation in cyber security initiatives, such as *CyberFirst* and *CyberDiscovery*.

> *"From a diversity point of view, we don't necessarily end up with reaching all the audiences we want because the kinds of people who take part are the ones who are already kind of sold on the idea of cyber security as an important or worthwhile thing." – Head of Department, HM Government*

> *"I think there's an awareness deficit. I think people don't know what cyber security is about. But I also think that there is a sort of in-built bias that it is for particular people: eggheads and techies, and boys, or that the jobs might be boring. So I think there are a lot of stereotypes." – Learning and Skills Co-ordinator, Scotland*

Some groups are now being targeted, particularly girls and women in a UK context, however success in targeting girls (particularly through the ***CyberFirst Girls Competition***) appears quite mixed and dependent on the area and school, including socioeconomic status:

"We don't see such a big uptake of the CyberFirst Girls Competition. I think partly we don't have a lot of girls-only schools – I think down in England there are probably a lot more girls-only schools, including independent girls schools." – Learning and Skills Co-ordinator, Scotland

"Traditionally we tend to find that independent schools may take up opportunities quite readily. We target the schools where there is socio-economic disadvantage." – Director of Education, BCS

Therefore, any changes or improvements that may be taken up in regards to cyber security education, should be sensitive to the many factors that can affect the current landscape.

"It's the answer to establish a cyber security pipeline … would require a whole series of new things because it's really, really complicated." – CyberFirst employee, HM Government

4.6. Summary

The UK offers a wide variety in regards to a pre-university cyber security education, however each country within the UK has a slightly different approach, and England, Scotland and Northern Ireland appear stronger than Wales in terms of pre-university cyber security education. Despite these differences, cyber security appears to be important in terms of government priorities and actions at a UK-wide level. The fragmented nature of pre-university cyber security education provision can be seen in the education systems and provision in particular. Information and access to initiatives and programmes appears to be impacted by awareness of cyber security and initiatives, socioeconomic background, and having a flexible curriculum and timetable to accommodate pre-university cyber security activities. There is also the tension between different approaches of computing-related subjects, including notably the tension between computational thinking demanded from Computing, and a more vocational approach of ICT, with all four constituent nations taking a slightly different approach. There is also a wide variety of initiatives targeting both cyber security and online safety aspects of cyber security education, however those who are not aware of the cyber security aspects (e.g., CTF-style competitions and CyberFirst programme) may only receive the online safety aspects of cyber security education, therefore reducing the diversity of the beneficiaries of such educational activities.

5. Australia, Canada, New Zealand, Singapore and US

This section will explore pre-university cyber security and online safety education in the rest of the countries within our group 1: **Australia**, **Canada**, **New Zealand**, **Singapore** and the **US**. As described in Section 2.2.4, these countries were put in group 1 because English is the official language (therefore, relevant documents would be accessible to the research team in English) and a cyber security educational program for schools is likely to be more established. Many of these countries are also at the forefront of cyber security education worldwide, with a Global Cybersecurity Index (GCI) score within the top 10, in particular the US (100; ranked 1/182), Singapore (98.52; ranked 4/182) and Canada (97.67; ranked 8/182) (ITU, 2021a).

Each country will be explored through the five landscapes presented in Section 4: stakeholder landscape, educational landscape, policy landscape, implementation landscape and socio-cultural landscape. Each subsection will be supported by excerpts from interviews undertaken with stakeholders from three of the four countries covered (Australia, New Zealand and Singapore).

5.1. Stakeholder landscape

Each of the five countries covered in this section has a variety of stakeholders involved in pre-university cyber security education, in much the same way the UK does (see Section 4.1). Cyber security strategies, which call for upskilling of the workforce and nurturing the talent pipeline to various degrees in each of the five countries comes from central government, and from a variety of different departments, for example defence departments (e.g., **Department of Defense** in the US), domestic affairs departments (e.g., **Department for Home Affairs** in Australia**; Department of Homeland Security** in the US), cyber security agencies (e.g., **Cyber Security Agency of Singapore** in Singapore), public safety departments (e.g., **Public Safety Canada** in Canada) and cabinet offices (e.g., **Department of the Prime Minister and Cabinet** in New Zealand).

Even if cyber security policy does not come from central government, each country has a dedicated cyber security centre or a body with a cyber security focus. These centres are as follows:

- Australia: **Australian Cyber Security Centre** (**ACSC**)
- Canada: **Canadian Centre for Cyber Security**
- New Zealand: **National Cyber Security Centre** (**NCSC-NZ**)
- Singapore: **Cyber Security Agency of Singapore** (**CSA Singapore**)
- US: **Cybersecurity and Infrastructure Security Agency** (**CISA**)

For all countries covered in this section except the US, schools and colleges, with the corresponding national curriculum (if there is one), are regulated by the **relevant department or ministry of education within the central or federal government**, e.g., **Department of Education, Skills and Employment** (**DESE**) in **Australia**; **Ministry of Education** in **New Zealand** and **Singapore**. As a federal country, the **US** has a **Department of Education** at the federal level, however, education is a matter dealt with at the state level. Therefore, each state in the US governs its own education affairs (e.g., **California Department for Education; New York**

State Education Department; Texas Education Agency (TEA); Utah Education Network), including frameworks, benchmarks and curricula (including state-wide guidance).

Stakeholders involved in extra-curricular pre-university educational provision in Australia and Singapore appear to be government-led, e.g., Australia's Grok Academy (part of ACSC, see Section 5.4.1.1) and Singapore's *SG Cyber Youth Programme* and *SG Cyber Safe Students Programme* (led by CSA Singapore, see Section 5.4.1.4). In New Zealand, an independent not-for-profit organisation Netsafe plays an active role in supporting schools on online safety and digital citizenship education (see Section 5.4.3.3). Stakeholders in the US and Canada appear to have a mix of provision provided by public bodies, e.g., the National Institute of Standards and Technology (NIST, part of the U.S. Department of Commerce), and private sector organisations, e.g., the international coalition Anti-Phishing Working Group (APWG) and the US-based not-for-profit organisation Air Force Association (AFA) (see Sections 5.2 and 5.4 for more details). These approaches show a great deal of heterogeneity within this sample of countries.

Echoing the situation in the UK (see Section 4.1), parents are considered important stakeholders in pre-university cyber security education in terms of helping pupils to access opportunities to learn about cyber security, as well as in the lives of children and young people more broadly. A positive attitude from parents on the provision of pre-university cyber security education helps improve access to this education for children and young people.

> *"We received positive response from parents and educators on our efforts in providing students opportunities to learn about cybersecurity through the bootcamps that we held, as well as engaging the students through school talks and events." – Senior Assistant Director, Ecosystem Development, Cyber Security Agency of Singapore, Singapore*

Similar to the UK case, access to knowledge and resources for teaching cyber security appears to be important for teachers in countries covered in this section as well, with upskilling teachers' knowledge in Australia and New Zealand earmarked as a challenge to tackle in the future.

> *"I think the challenges for schools now is that we're offering this new type of teaching or this new theme on them of cyber security, and they themselves just don't have the understanding. So that's going to be our biggest challenge is really upskilling teachers, providing them with the resources." – A/Curriculum Specialist Technologies, Australian Curriculum, Assessment and Reporting Authority (ACARA), Australia*

> *"My take is that cyber security expertise may be a limiting factor in the workforce, … For example, in a previous life I taught computer science without formal training in the subject. I don't know exactly what the current situation is, but the introduction of digital technologies to the curriculum for all schools and kura will only have increased the need for more skilled, experienced computer science teachers." – Director of Research and Policy, Netsafe, New Zealand*

Industry was also found to be supporting content delivery in schools, was actively encouraged to network with schools and other educational institutions, and also to be aware of the content being taught in schools, as found in Australia:

> *"But we also work with external organisations to say, 'Hey, here's a new piece of content for teachers. What can you offer as far as support goes to them as well?' So industry is really excited about it and they're really keen to get involved. We do connect quite closely with industry here." – A/Curriculum Specialist Technologies, Australian Curriculum, Assessment and Reporting Authority (ACARA), Australia*

"So we meet with those bigger industry players and we talk to them about what curriculum looks like because they're not teachers generally. This is kind of what it looks like. And then we kind of really just encourage them to make connections with leaders in the states and territories and get conversations going. So, …, if they're holding conferences, webinars, doing podcasts, we really encourage to have that curriculum aspect …" – A/Curriculum Specialist Technologies, Australian Curriculum, Assessment and Reporting Authority (ACARA), Australia

The above echoes our findings from Section 0 regarding relevant stakeholders in the UK, demonstrating the importance of engagement from multiple stakeholders from different sectors in the pre-university cyber security education of children and young people.

5.2. Policy landscape

The policy landscape varies across each of the countries in this section, with the application of policy in regards to pre-university cyber security education impacted by the nature of the government in each country: in unitary countries, the government is centralised, and local governments only act on the powers given to them by central government (Oxford Reference, 2021), whereas in federal countries, power is divided between national and regional governments (Oxford Reference, 2021). The table below gives an overview of the types of government in each country covered in this section. The countries are covered in the same order as in Table 19 throughout the rest of the section.

Table 19: Government types of the countries covered in Section 5

Country	Federal or unitary country?
Australia	Federal
Canada	Federal
New Zealand	Unitary
Singapore	Unitary
US	Federal

5.2.1. Australian policy landscape

Australia's ***Cyber Security Strategy (2020),*** from its **Department for Home Affairs**, builds on the ***2016 Cyber Security Strategy*** (Department for Home Affairs (Australia), 2020, p6). The key points of this strategy include: 'Improved community awareness of cyber security threats'; '*greater collaboration to build Australia's cyber skills pipeline*' and '*24/7 cyber security advice hotline for SMEs (small and medium-sized enterprises) and families*' (Department for Home Affairs (Australia), 2020, p6). *The* ***Cyber Security National Workforce Growth Program*** aims to increase cyber skills in a variety of different groups (Department for Home Affairs (Australia), 2020, p32), including:

- apprenticeships, internships and work experience (although not marked out as for under 18-year-olds);
- training for teachers;
- increasing cyber skills education in primary and secondary, however, no goals or outline is given.

The **Department of Education, Skills and Employment** (**DESE**) has a '***National STEM School Education Strategy 2016–2026'***, which includes digital technology as a key part of STEM

(DESE, 2021a). STEM (science, technology, engineering, and mathematics) educational initiatives are a key part of this strategy (DESE, 2021b). However, there is no explicit mention of cyber security or online safety as part of these initiatives.

The ***Digital Literacy Skills Framework*** is a set of competencies for workplace digital literacy for use in vocational training settings (DESE, 2021d). It is not clear if this framework is intended for young people in the equivalent of further education. The domain 'digital identity and safety' particularly covers cyber security and online safety.

The ***Digital Skills Cadetship trial program*** aims to give digital skills training, including in the field of cyber security, as a cadetship (DESE, 2021c). It is unclear what age the cadetship is for, as it remains undisclosed in the information. However, given the fact that further education qualifications, e.g., VET (vocational education and training), will be gained through this cadetship, it is assumed that these cadetships will be open to 16-18-year-olds. Learning will be through on the job training and mentorship with experienced employers in the field, and starting in 2022.

5.2.2. Canadian policy landscape

The ***National Cyber Security Strategy*** (Public Safety Canada, 2018a) is the Canada-wide cyber security strategy. Education on cyber security is mentioned twice in the strategy document, including education at both a pre-university level and more generally (ibid):

- "*The Government of Canada will explore new ideas for making businesses and Canadians of all ages and backgrounds more cyber secure. The federal government has already committed investments to improve digital skills, such as coding education for kids.*"
- "*The Government of Canada is playing its part through long-term investments to help Canadians of all backgrounds to get the education and work experience they need to participate in an increasingly digital economy.*"

Cyber security education is not specifically mentioned in this strategy, and digital skills are referred to in quite a broad manner. Canada's ***National Cyber Security Action Plan (2019-2024)*** builds on the ***National Cyber Security Strategy,*** through outlining actions and initiatives for Canada. However, education and links with educational establishments focus on post-secondary institutions. The cyber education and awareness tool is an action not specific to children and young people, but rather small and medium size businesses (Public Safety Canada, 2018b).

There are relevant policies at the provincial level as well. For instance, the **Province of Ontario** has a ***Digital and Data Strategy*** (Ontario Treasury Board Secretariat, 2021), with one of the challenges being reskilling and retraining people in Ontario in digital skills. However, there is no mention of education, training or upskilling children or young people and appears to focus on working age adults, businesses and the public sector.

5.2.3. New Zealand's policy landscape

New Zealand's **Ministry of Education** provides guidance for school leadership and teaching staff on backing up emails, phishing scams and ensuring secure network connections (Ministry of Education (New Zealand), 2021b). This is general school safety targeting teachers and other school staff, and does not include pre-university cyber security education for children and young people.

The new update to the curriculum in 2017 (Ministry of Education (New Zealand), 2021c) provides guidance for parents and carers in supporting children and young people with digital skills in schools. The little information which is available for pupils appears to be focused on '*selling the (cyber security) subject*' rather than providing educational materials relevant to pre-university cyber security education (Ministry of Education (New Zealand), 2020).

The **Department of the Prime Minister and Cabinet** released the ***Cyber Security Strategy*** in 2019 (New Zealand Government, 2019, p11), which includes:

- *"practical, targeted and regular awareness campaigns to build awareness and resilience among different groups of people"*
- *"increasing the availability of educative tools so people can be secure and safe online"*
- *"increasing efforts to educate vulnerable users, such as the elderly and children, to prevent victimization"*
- *"sharing research so people can understand the threat and vulnerability landscape for their businesses, communities and families."*

There is no direct mention of children or young people in the 2019 strategy document. There were two previous *Cyber Security Strategies* (New Zealand Government, 2011, 2015). Their relevant policy is summarised in Table 20.

Table 20: Relevant policies in New Zealand's Cyber Security Strategy 2011 and 2015

Policy name and date	Relevant aspects of policy
New Zealand's Cyber Security Strategy 2011	Increasing awareness and Online security (New Zealand Government, 2011, p6) – awareness (ibid, p7) but none child or young person focused, more focused on businesses and infrastructure.
New Zealand's Cyber Security Strategy 2015	Cyber Capability (New Zealand Government, 2015, p5). Awareness and cyber security education more broadly (although not advertised as such).

The **National Cyber Policy Office** (**NCPO**) established in 2012 leads the development of advice on cyber security policies and provides such advice to the New Zealand government on investing in cyber security activities (Department of the Prime Minister and Cabinet (New Zealand), 2020). Its head holds the role of the **Prime Minister**'s **Special Representative on Cyber and Digital, and Cyber Coordinator**, and consults the Prime Minister, the **Minister for National Security and Intelligence**, and **other ministers** on relevant cyber security policy matters. Formally, the NCPO reports to the **Minister of Broadcasting, Communications and Digital Media**. The NCPO works with the **Ministry of Foreign Affairs and Trade** on New Zealand's international engagement on cyber security policy. It also has outreach activities with the private sectors, although not specifically on supporting schools, pupils or parents.

5.2.4. Singapore's policy landscape

The ***Singapore Cybersecurity Strategy*** was first defined in 2016 (CSA Singapore, 2016) and recently updated in 2021 (CSA Singapore, 2021a). The new ***Singapore Cybersecurity Strategy 2021*** explicitly covers cyber security education as part of its '***Foundational Enabler 2: Grow a Robust Cyber Talent Pipeline***' (ibid, Chapter 5). One major activity identified for this foundational enabler is "*Move **upstream** to engage talent: … reach out to **the young** to develop their interest and cyber skills, and encourage more **youths** to pursue a career in cybersecurity.*" This is further detailed as part of the activities to '*support **youths**, women, and mid-career professionals to pursue a cybersecurity career*', and ***SG Cyber Youth*** (to be detailed later in Section 5.4.1) is highlighted in the Strategy as '*a national programme that guides*

youths *in their cybersecurity journey, with support from the academia, community, and industry*' (ibid, p53). The Strategy also mentions the **National Police Cadet Corps** (**NPCC**) *Cybercrime Prevention Programme*, the **CSA Singapore**'s ***SG Cyber Safe Students Programme*** and the ***Go Safe Online portal*** for reaching out to the general public, including pre-university pupils for cyber security and cyber crime awareness (ibid, p27, p28).

Since the ***Singapore Cybersecurity Strategy 2021*** is very new, we also cover the ***Singapore Cybersecurity Strategy 2016*** (CSA Singapore, 2016) here. It includes aspects relevant to cyber security education for children and young people, such as ***cyber security scholarships for exceptional students***, however, no age is given in terms of who the recipient would be (ibid, p37). Curriculum changes and adjustments mentioned are for universities and polytechnics, rather than schools (ibid, p37). The 2016 Strategy also mentions the ***Collaborative Social Programme*** (***CoSP***), as part of the ***National Cybercrime Action Plan*** (***NCAP***), which involves ***working with schools and school-aged children and young people*** (ibid, p26; Ministry of Home Affairs (Singapore), 2016).

5.2.5. The US' policy landscape

The ***National Cyber Strategy*** (The White House, 2018) seeks to target children and young people as part of promoting American prosperity, by developing a superior cyber security workforce. One priority action notably includes investment in the talent pipeline at ISCED levels 1 and above (described as primary to post-secondary in the documentation).

The **National Institute of Standards and Technology** (**NIST**, part of the **U.S. Department of Commerce**) manages the ***National Initiative for Cybersecurity Education*** (***NICE***), which is '*a partnership among government, academia, and the private sector focused on education, training, and workforce development that will strengthen the cybersecurity posture of organizations*' (NIST, 2020a). While being led from a single public body (NIST), the operation of NICE heavily relies on a wide range of **NICE partners**, and its implementation plans and metrics are developed through a consultative process that includes two key bodies: the **NICE Interagency Coordinating Council** (**ICC**) engaging employees and representatives from 15+ federal governmental bodies (NIST, 2020a, 2020c), and the **NICE Community Coordinating Council** (**NICE Community**) engaging both public and private sector participants (NIST, 2020a, 2021f). The NICE also maintains a **K12 Cybersecurity Education Community of Interest** as a forum for engaging even wider stakeholders including K-12 teachers, school administrators, local and state education agencies (NIST, 2021g). The NIST has defined three continuous ***strategic plans*** for NICE since 2012 (NIST, 2012, 2016, 2020a), and its ***current NICE strategic plan for 2021-25*** (NIST, 2020a) also has a specific ***implementation plan*** (NIST, 2021c). The 2021-25 strategic plan has five goals with multiple objectives under each goal, among which the following are of high relevancy to the pre-university education setting (important keywords and phrases highlighted in ***bold face***):

- Goal 1: "*Promote the Discovery of Cybersecurity Careers and* ***Multiple Pathways***"
  - Objective 1.1: "*Identify and share effective practices for promoting* ***cybersecurity career awareness*** *and discovery to diverse stakeholders*"
  - Objective 1.2: "*Increase understanding of* ***multiple learning pathways*** *and* ***credentials*** *that lead to careers that are identified in the Workforce Framework for Cybersecurity (NICE Framework)*"
  - Objective 1.4: "*Provide information and tools about cybersecurity-related career options to those who influence career choices (e.g.,* ***teachers*** *and faculty,* ***school***

***counselors**, career coaches, career development personnel, mentors, and **parents or guardians**)"*

- Goal 2: "*Transform **Learning** to Build and Sustain a Diverse and Skilled Workforce*"
  - Objective 2.1: "*Foster proven **learning** methods and experiences shown to effectively build and sustain a diverse, inclusive, and skilled cybersecurity workforce*"
  - Objective 2.2: "*Advocate for **multidisciplinary** approaches that integrate cybersecurity **across varied curricula** that support **diverse learners** from **a variety of backgrounds and experiences***"
  - Objective 2.3: "*Improve the quality and availability of **credentials** (e.g., **diplomas**, degrees, **certificates**, **certifications**, **badges**) that validate competencies*"
  - Objective 2.4: "*Facilitate increased use of performance-based **assessments** to measure competencies and the capability to perform NICE Framework tasks*"
  - Objective 2.5: "*Encourage the use of **Learning** and Employment Records to document and communicate skills between **learners**, employers, and **education and training providers***"
  - Objective 2.6: "Champion the development and recognition of teachers, faculty, and instructors as part of the in-demand workforce"
- Goal 5: "*Drive **Research** on **Effective Practices** for Cybersecurity Workforce Development*"
  - Objective 5.3: "*Prioritize research on the most effective and proven practices for **blending successful learning practices across education**, training, and workforce development settings*"
  - Objective 5.4: "*Utilize research results to inform **programs and curriculum design**, foster **continuous learning** opportunities, impact **learner success**, and ensure **equitable access***"

On 7th December 2021, as part of its work on the NICE 2021-25 strategic plan, the **NIST** announced the ***National K12 Cybersecurity Education ROADMAP*** (NIST, 2021d), for guiding K12 cyber security education in the whole US. The ROADMAP defines five major elements:

1. "*Increase Cybersecurity Career Awareness: Grow and sustain youth and public engagement in promoting cybersecurity career awareness and exploration*"
2. "*Engage Students Where Disciplines Converge: Identify, design, and share cybersecurity resources for the future STEM and cybersecurity workforce*"
3. "*Stimulate Innovative Educational Approaches: Enrich K12 cybersecurity education instruction and learning*"
4. "*Promote Cybersecurity Career Pathways: Cultivate youth pursuing cybersecurity or cybersecurity-related credentials (e.g., diplomas, degrees, certificates, certifications, badges)*"
5. "*Prioritize Research: Enhance efficiency and effectiveness of K12 cybersecurity education programs and instructional practices*"

At least two other US governmental bodies have their separate cyber security strategy. The **Department for Homeland Security**'s ***Cybersecurity Strategy*** (U.S. Department for Homeland Security, 2018) includes awareness of cyber security roles and education about them as one of the objectives, however, children and young people, or pre-university educational provision is not mentioned in this particular strategy (p25). The **Department of Defense**'s ***Cybersecurity Strategy*** (U.S. Department of Defense, 2018), which supersedes their previous 2015 strategy, explicitly mentions pre-university education. Topics to be focused on at ISCED levels 1-4

include: science, technology, engineering, mathematics, and foreign language (STEM-L) (ibid, p6). In addition, growth of the cyber security talent pool is also mentioned, with *'establishing standards in training, education, and awareness'* of cyber security careers given as a key action (ibid, p6).

In the context of foreign policies, the US created the **Office for the Co-ordinator for Cyber Issues** (**S/CCI**) in 2011 (U.S. Department of State, nd). It pulls together '*diplomatic efforts across the full range of international cyber policy issues that impact U.S. foreign policy, national security, human rights, and economic imperatives*'. Due to its focus on diplomatic efforts and international cyber policies, this office does not seem to have any specific activities on pre-university education.

In addition to the above-mentioned policies at the federal level, there are also policies at state level, too. For instance, in October 2021 the **State of California** announced '***Cal-Secure: State of California Executive Branch Multi-Year Information Security Maturity Roadmap 2021***', which states that an initiative for aligning with the national initiative NICE (Office of Governor of California, 2021; California Department of Technology, 2021). Due to the large number of states in the US, we decided to focus on the federal level for the policy landscape.

5.3. Educational landscape

Education in each of the countries included in this section operates through slightly different systems, and is impacted by whether the country is a unitary or a federal state. Unitary countries tend to have an education system that is guided by the central government, whereas in federal countries regional governments shape the education systems of different states in the country.

Much like the differences between the four nations within the UK, there is a diversity in the way that cyber security education appears within the five countries covered in this section, which is detailed below.

5.3.1. Australia

In spite of Australia being a federal country, it has a national curriculum named the ***Australian Curriculum***. However, it is the choice of each state to implement and follow this curriculum. Many Australian states and terrorities seem to use the Australian Curriculum as it is published (ACARA, nd-a), with only two territories making any changes, in spite of the opportunity they have to adapt it to their unique context:

> *"We have the National Curriculum, which then the states and territories take and they adapt and adopt that to suit the context of their state. But generally, across the country, the Australian Curriculum is taught as is." – A/Curriculum Specialist Technologies, Australian Curriculum, Assessment and Reporting Authority (ACARA), Australia*

The Australian Curriculum is divided into two main parts: ***foundation to year 10*** (ACARA, nd-a; Australian Curriculum, nd-a) and ***senior secondary*** (ACARA, nd-c) with subsequent curricula (ACARA, nd-a, nd-b; Australian Curriculum, nd-a). It has three complementary dimensions: ***learning areas***, ***general capabilities*** and cross-curriculum priorities. Learning areas are basically subjects, general capabilities span across all learning areas, and cross-curriculum priorities are about three selected unique priorities for Australian pupils (which are not directly related to cyber security or online safety).

For cyber security and online safety education, the most relevant learning areas in the Australian Curriculum is ***Digital Technologies***, and the most relevant general capability is the ***Information and Communication Technology (ICT) capability***. The Digital Technologies learning area is compulsory from foundation (5-6-year-olds) to year 8 (13-14-year-olds) (Trevallion, 2014) and elective in years 9 and 10 (Education Matters, nd; Passey, 2016). Table 21 summarises the cyber security and online safety related content of each band level (year groups) defined in the Australian Curriculum: Digital Technologies.

Table 21: A summary of cyber security and online safety related content of each band level in the Australian Curriculum: Digital Technologies (Australian Curriculum, nd-b)

Band level (ISCED level(s) and ages)	Content in the Digital Technologies learning area
ISCED level 1 (5-8 years)	*"Through discussion with teachers, students learn to apply safe and ethical practices to protect themselves and others as they interact online for learning and communicating."*
ISCED level 1 (8-10 years)	*"When sharing ideas and communicating in online environments they develop an understanding of why it is important to consider the feelings of their audiences and apply safe practices and social protocols agreed by the class that demonstrate respectful behaviour."*
ISCED level 1-2 (10-12 years)	*"When engaging with others, they take personal and physical safety into account, applying social and ethical protocols that acknowledge factors such as social differences and privacy of personal information. They also develop their skills in applying technical protocols such as devising file naming conventions that are meaningful and determining safe storage locations to protect data and information."*
ISCED level 2 (12-14 years)	*"They further develop their understanding of the vital role that data plays in their lives, and how the data and related systems define and are limited by technical, environmental, economic and social constraints."* *"When communicating and collaborating online, students develop an understanding of different social contexts, for example acknowledging cultural practices and meeting legal obligations."*
ISCED level 3 (14-16 years)	*"Students consider how human interaction with networked systems introduces complexities surrounding access to, and the security and privacy of, data of various types. They interrogate security practices and techniques used to compress data, and learn about the importance of separating content, presentation and behavioural elements for data integrity and maintenance purposes."* *"They consider the privacy and security implications of how data are used and controlled, and suggest how policies and practices can be improved to ensure the sustainability and safety of information systems."* *"When creating solutions, both individually and collaboratively, students comply with legal obligations, particularly with respect to the ownership of information, and when creating interactive solutions for sharing in online environments."*
ISCED level 4 (16-18 years)	No curriculum available

The ICT capability defines a range of important elements across all learning areas. It includes a central element on ***'Applying social and ethical protocols and practices when using ICT'*** (ACARA, 2015; Australian Curriculum, nd-c). This element involves making pupils '*recognise **intellectual property***', '*apply digital information **security practices***', '*apply personal **security protocols***', and '*identify the impacts of ICT in society*", which are all relevant cyber security related skills. Another relevant element is '***Managing and operating ICT***", which involves making pupils '*apply technical knowledge and skills to efficiently and **securely** manage and maintain digital data*'. A third relevant element is '***Investigating with ICT***', which covers the aim

of making pupils '*apply criteria to **verify the integrity** and value of the digital data*', a major cyber security task (data integrity).

As part of the need to cover the ICT capability, in addition to Digital Technologies, some other learning areas also have relevant coverage on online safety (Australian Curriculum, nd-c), including the following (relevant keywords highlighted in ***boldface***):

- ***The Arts***: "*Students learn to apply social and ethical protocols and practices in a digital environment, particularly in relation to the appropriate acknowledgment of **intellectual property** and the **safeguarding of personal security** when using ICT.*"
- ***Humanities and Social Sciences (HASS)***: "*Students learn about and have opportunities to use social media to collaborate, communicate, share information and build consensus on political, legal and social issues, reflecting on **safety awareness** and ethical protocols for ICT use.*"
- ***Health and Physical Education***: "*… enhances ICT learning by helping students to effectively and **safely access online** health and physical activity **information and services** to manage their own health and wellbeing. … Students become confident and critical consumers of a multitude of **wellbeing apps** that can assist them to seek help, relax, be mindful, **report bullying**, and so on.*"
- ***Work Studies***: "*Students learn how to **access online** career, employment and work **information and services** effectively and **safely**. … They learn different workplace strategies to **minimise the risk of harm through the use of ICT**.*"

Curriculum connections resources on the Australian Curriculum's website (Australian Curriculum, nd-d) provide guidance to teachers and educators in applying the curriculum, with a specific curriculum connection on online safety (ACARA, nd-c). This curriculum connection includes aspects such as identity theft and breaches of privacy, and provides pupils and teachers with online safety resources including many provided by various organisations. It has a highlighted mention of Australia's **eSafety Commissioner**, with which the following five dimensions of learning about online safety have been developed (Australian Curriculum, nd-d): "*Values, rights and responsibilities*", "Wellbeing", "Respectful relationships", "Digital media literacy" and "Informed and safe use of information and devices".

The *Australian Curriculum* has been under review since June 2020 (ACARA, nd-d). It has been reported that cyber security is to be more significant in the new curriculum, with 5-year-olds being taught the basics of cyber security (for example, not sharing personal information and password etiquette (Sharwood, 2021; RT.com, 2021)). Our interview with the Australian representative also confirmed that the new curriculum will include more explicit mention of cyber security, as the current curriculum does not mention the term 'cyber security' explicitly, leading to many questions in how to teach cyber security:

> *"So what we could see in those reports is a lot of questions over the past six years. Where do we find cyber security in the curriculum? How do I teach that to my students? So during the review, which we've just undertaken, we had a look at that and we could see that cyber security was there, but it was very much inferred – it was hidden behind all the other texts." – A/Curriculum Specialist Technologies, Australian Curriculum, Assessment and Reporting Authority (ACARA), Australia*

5.3.2. Canada

Canada is a federal country, and there is no national curriculum in Canada, with provinces and territorial governments driving their own policies and initiatives under **their own Ministry of Education** (NCEE, nd). Compulsory schooling is generally between ages 6-16 years old,

however in Ontario pupils are required to remain in school until the age of 18 (NCEE, 2021). Each province develops their own assessments and operates their own system to measure teacher accountability, quality and efficacy (similar to Ofsted in the UK). However, '***A Digital World: A Pan-Canadian K-12 Computer Science Education Framework***' (Canada Learning Code, 2020) is currently being designed to better align education across the provinces.

The two areas of particular interest on the ***'Pan-Canadian K-12 Computer Science Education Framework'*** include: ***'Computing and Networks'*** (includes cyber security), and ***'Technology and Society'*** (includes ethics, safety and the Law).

Given that Canada is a federal country, we will focus on the two states given above (Ontario and British Columbia) that we explored in regards to the policy landscape. Each province and territory is responsible for th eir education regimes, and they are also provinces that have both an English and a separate French or Catholic school system.

In Ontario, all schools are required to use the ***Ontario Curriculum*** (OASDI, nd), and computing studies are only available at ISCED level 4 (ages 16-18). One key aspect of the computing curriculum is 'professional and ethical responsibility' (Ontario Ministry of Education, 2008, p4). There are three types of computer studies courses in Ontario: 'university preparation' (preparation for university studies); 'college preparation' (preparation for community college studies or workplaces); and 'open courses' (not designed for entering tertiary education or the workplace) (ibid, p7). There are two university courses, two college courses and one open course (ibid, p8). These all have slightly different foci:

- University preparation courses – heavier theory base, designing software, and topics such as **cryptography and artificial intelligence (linked to cyber security)**
- College preparation courses – computer programming languages, problem solving strategies, creating and adjusting programmes and using database management systems (no link to cyber security).
- Open course (age 14-15 only) – how computers solve problems, designing computer systems and basic programming skills (ibid, p7).

Assessment outcomes are graded by teachers. All levels achieved demonstrate a pass.

Online safety is also covered as part of the secondary ***Health and Physical Education Curriculum*** from ISCED level 3 (age 14-15) (Ontario Ministry of Education, 2015, p101) to ISCED level 4 (age -17-18) (Ontario Ministry of Education, 2015, p154). Mandatory learning on online safety was added into the Curriculum in 2019 for ages 6-9, 12-13 and 14-15, meaning all age groups and ISCED levels learn about online safety (Ontario Ministry of Education, 2022). Parent resources are also available (Ontario Ministry of Education, 2021a). Health and Physical Education is compulsory until ISCED level 3 (age 14-15) (Ontario Ministry of Education, 2019, p21). The Ontario Secondary School Literacy Test must be passed, or a literacy course completed in ISCED level 4 (age 17-18), to graduate (NCEE, nd).

There is no computing in elementary curriculum, however, online safety is covered as part of the Health and Physical Education course (Ontario Ministry of Education, 2019, p42) as early as second grade (ibid, p123) up to grade 8 (age 13-14) (ibid, p236).

In British Columbia, cyber security and computing more broadly falls under the ***'Applied Design, Skills, and Technologies' curriculum***. Schools can choose which 'module' of technology to take, for example computing, digital literacy, food studies, media arts, metalwork, robotics and textiles (British Columbia Ministry of Education, 2016a, p6). Computing knowledge and digital literacy first appears on the curriculum in grade 6 as an option, with internet safety, digital footprint, legal and ethical considerations and cyber bullying

all part of the ISCED level 1-2 curriculum (ages 10-12) (ibid, p7). At ISCED level 2 (age 13-14) digital citizenship is introduced (ibid, p14). Digital literacy and computing do not appear as an option for grade 9 (ages 14-15) (ibid, pp21-25). At ISCED level 3 (ages 15-18), computer studies can be taken as an option. Table 22 shows the course name, grade and content.

Table 22: Cyber security and online safety related courses in British Columbian secondary schools

Course title	Age	Content relevant to cyber security
Computer Studies 10	15-16	"*computer security risks, ethical considerations of technology use, digital literacy and digital citizenship*" (British Columbia Ministry of Education, 2018a)
Computer Information systems 11	16-17	"*appropriate use of technology, including digital citizenship, etiquette, and literacy*" and "*ongoing preventive maintenance, including data security and online/offline backup solutions*" (British Columbia Ministry of Education, 2018b)
Computer Programming 11	16-17	"*appropriate use of technology, including digital citizenship, etiquette, and literacy*" (British Columbia Ministry of Education, 2018c)
Computer Information Systems 12	17-18	"*awareness and understanding of digital security risks*", "*network management tools, including security, imaging, backup, and remote access*", "*design requirements of network devices, cabling, test equipment, management plans, operation manuals and documentation, deployment strategies, ongoing upgrades, maintenance, and security*", "*appropriate use of technology, including digital citizenship, etiquette, and literacy*" (British Columbia Ministry of Education, 2018d)
Computer Programming 12	17-18	"*appropriate use of technology, including digital citizenship, etiquette, and literacy*" (British Columbia Ministry of Education, 2018e)

Unlike in Ontario, Health and Physical Education courses in British Columbia do not include content on cyber security, online safety or related topics (British Columbia Ministry of Education, 2016b; British Columbia Ministry of Education, 2018f). The **PHE BC** (Physical & Health Education in British Columbia) provides online resources for teachers; however none are on online safety or cyber security (PHE BC, nd).

The **Government of British Columbia** gives a list of resources on Cyber Security (Government of British Columbia, nd-a) however this list is focused on tertiary education mainly with courses provided by universities. ***Cyber Security Awareness month*** is also promoted by the Government of British Columbia with an online quiz and linked resources (Government of British Columbia, nd-b), including links to the **Ontario Cyber Security Centre of Excellence**. Information is also available for the general population (Government of British Columbia, nd-c; nd-d), with no focus on children and young people.

5.3.3. New Zealand

Teaching in New Zealand is guided by two curricula (Ministry of Education (New Zealand), 2021a): (1) the ***New Zealand Curriculum*** for English medium schooling and (2) ***Te Marautanga a Aoteroa*** for Māori medium schooling. In reference to the *New Zealand Curriculum*, the first update to the curriculum since 2007 and noticeably on the technologies strand, came into use in January 2020 (Education Central, 2017). This made digital technologies a compulsory part of *the New Zealand Curriculum* (Education Central, 2017). Digital technologies are a part of the technological practice strand, as shown in (Ministry of Education, 2019, p3): "*They also learn to consider ethics, legal requirements, protocols, codes of practice, and the needs of and potential impacts on stakeholders and the environment.*"

The way in which technologies are taught in New Zealand also takes the approach of being part of a holistic design process, rather than teaching discrete skills:

> *"Whatever the technology subject area is, there's a technology process which is involved, and the focus is on design thinking and using inquiry processes to create technological outcomes." – Director of Research and Policy, Netsafe, New Zealand*

In ISCED level 1, digital technologies are embedded into other subjects or topics and themes which cross multiple subject areas (ibid, p3). By the end of ISCED level 3, pupils are to "*understand the role of systems in managing digital devices, security and application software, and they are able to apply file management conventions using a range of storage devices*" (ibid, p3) and by the end of year 13, pupil need to "*take into account a synthesis of social, ethical and end-user considerations*" (ibid, p3).

Digital technologies are an approved subject for university entrance in New Zealand universities and a selectable element from the ***National Certificate of Educational Achievement (NCEA)*** (NZQA, nd-a) including at all three levels (NZQA, nd-b). The only requirement of the NCEA is that literacy and numeracy requirements were met (10 credits in literacy and 10 credits in numeracy (NZQA, nd-c). Literacy and numeracy may be embedded into other subjects rather than studying mathematics and English; many schools have no compulsory subjects for years 12 and 13 however many students do have to study English, maths and science in year 11 (NZQA, nd-d).

The Māori language curriculum, *Te Marautanga a Aoteroa*, encourages e-learning including using information technology and ICT (Ministry of Education (New Zealand), 2017, p13). There is substantial awareness that IT is critical to this generation of students (Ministry of Education (New Zealand), 2017, p13), however it is not a specific strand (embedded into various other themes and strands of the curriculum rather than a discrete subject). Technology is as a part of the curriculum, however there is no distinct focus on digital skills (Ministry of Education (New Zealand), 2017, p61; p63). Electronics and Control Technology as a topic area within technology is the closest fit to cyber security; online safety, ethics or computing are not mentioned (Ministry of Education (New Zealand), 2017, p63).

In reference to both curricula used in New Zealand, it appears that schools in New Zealand still have a relative amount of autonomy about the content which is covered in schools, and the teaching methods used. This is despite New Zealand being a unitary country:

> *"In New Zealand, the way in which the school system is organised is currently still quite decentralised. All individual schools make a decision about how they deliver the curriculum. So they're self-managing." – Director of Research and Policy, Netsafe, New Zealand*

The nature of the curriculum is also quite different to some other countries in this report (e.g., England); the content of the curriculum is not so much a directive, but as a guide for teachers:

> *"That's quite an important aspect of the New Zealand system to understand, because the curriculum basically is … the guiding framework … a set of values, a set of principles, etc., … rather than a prescriptive document." – Director of Research and Policy, Netsafe, New Zealand*

5.3.4. Singapore

In the curriculum used in Singapore at ISCED level 1 (ages 7-12), discrete ICT, computing or digital skills is not compulsory (Ministry of Education (Singapore), nd-c) and these are not

marked as key areas of the curriculum at ISCED level 1 (Ministry of Education, 2020b, p4). This also is the case at ISCED levels 2-4.

Aspects of cyber security and online safety are however embedded within ***Character and Citizenship Education (CCE)*** for ISCED level 1 (ages 10 to 12) regarding online friendships, communicating online and managing online bullying (Ministry of Education (Singapore), 2012, p22). CCE is compulsory for all pupils in primary school in Singapore.

Aspects of cyber security also continue to be embedded throughout CCE throughout ISCED levels 2 and 3 (ages 12-17) with ***Cyber Wellness*** (***CW***) a key aspect of the syllabus, notably including teaching regarding: wellbeing of students online, positive online presence, using ICT for positive means and being safe and responsible users of ICT (Ministry of Education (Singapore), 2020a, p13, nd-c). Further detail is given in the secondary syllabus as to how this information may be shared with pupils: through discrete CCE lessons (recommended two periods per week) (Ministry of Education (Singapore), 2020a, p15) and whole school initiatives (ibid, p19). There is no formal assessment of CCE completed by teachers, however, it is recommended that students set and complete their own goals (ibid, p24). CCE is compulsory across all bands of secondary education (Singapore's secondary education system is streamed; see (Ministry of Education (Singapore), 2020c)). Interestingly, in the Social Studies curriculum for upper secondary school students (approximately ISCED level 3), there is a topic '*Security impact on countries and individuals*', which covers sub-topics such as '*security and vulnerability*' and '*cyber security challenges*' (Ministry of Education (Singapore), 2016).

Some schools do offer an ***Ordinary (O-) Level*** (22 schools in 2020; 16% of secondary schools; Coding Lab, 2020) and ***Advanced (A-) Level*** (8 schools in 2020; 73% of pre-university schools; Coding Lab, 2020) in computing for pupils who are in the integrated, express and normal-academic streams. For pupils who are in a normal - technical stream, computer applications as a subject is compulsory at both ISCED level 2 and 3, and an option for pupils in the normal-academic stream (Ministry of Education (Singapore), nd-d).

5.3.5. US

Education is a local and state-level responsibility in the US (U.S. Department of Education, 2021). Subsequently, there are no national curricula in the US (U.S. Department of Education, 2008) as they have been banned after the introduction of the ***Elementary and Secondary Education Act (ESEA) of 1965*** (United States Congress, 1965). The US have no national curriculum for ICT/computing, but the ***'K–12 Computer Science Framework'*** (K–12 Computer Science Framework Steering Committee, 2016) informs the development of state-level curriculum. The framework is a joint effort of multiple stakeholders including companies, education organisations and individual experts from a wide range of organisations (k12cs.org, nd). One of the core concepts of this framework is *'networks and the internet'*, which includes cyber security; and '*impacts of computing*' core concept includes safety, law and ethics. Table 23 includes suggested achievements of the framework.

Table 23: Achievements by the ISCED level and age (adapted) in the US' K–12 Computer Science Framework (K–12 Computer Science Framework Steering Committee, 2016)

ISCED level (Age)	Achievement
ISCED level 1 (Age 6-8)	authentication measures should be used to protect devices and information from unauthorised access harmful behaviours, such as sharing private information and interacting with strangers, should be recognized and avoided

ISCED level 1 (Age 8-11)	security measures can be physical and/or digital the ease to send/receive media on the Internet can create the opportunity for unauthorised use (online piracy, copyright, attribution)
ISCED level 2 (Age 11-14)	security measures (encryption, access control) should proactively protect personal and private data people can be tricked into revealing personal information when more public information is available about them online
ISCED levels 3 and 4 (Age 14-18)	network security depends on a combination of hardware, software, and practices; needs of users and sensitivity of data determine security level laws govern many aspects of computing (privacy, data, property, information, and identity)

There also appears to be some extra recommendations that certain standards be upheld to guide education and topics taught (U.S. Department of Education, 2008a), e.g., **Common Core State Standards Initiative** (CCSSO and NGA Center, 2010), ISTE standards (ISTE, nd) and **ISTE National Educational Technology Standards** (**NETS**; notably 'Social, ethical, and human issues' (NCES, 2002)). States individually develop their own curricula, including the requirements for graduation (U.S. Department of Education, 2021). School districts are important in the governance of public schools, as they govern the policies and regulations of the schools within that district (U.S. Department of Education, 2008b). Since the introduction of Every Student Succeeds Act (United States Congress, 2015), state governments have been given new responsibility and power in regards to standards and evaluations. In regards to the age of schooling, this can be broken into 3 sections (U.S. Department of Education, nd): elementary school (ISCED level 1; ages 5-11); middle school (ISCED level 2; ages 11-14); and high school (ISCED levels 3 and 4; ages 14-18).

It is important to note this is one example of the US education system (the example above represents **California**'s school system), with various differing groupings of age across the US (for example, the difference between middle schools and junior high schools (U.S. Department of Education, 2008b)). The education system in the US takes a comprehensive model, with all pupils following a variety of educational paths all studying together in the same establishment (U.S. Department of Education, 2008b). Given that the US is a federal country, we use the same four states to illustrate differences between US states in regards to educational provision for cyber security at pre-university level. The states we chose in alphabetical order are: **California, New York State, Texas** and **Utah**. Our rationale for these is that two are Republican states and two are Democratic states, demonstrating differing political foci.

'***Computer Science standards for California***' begun development in 2016 for all age groups (California Department for Education, 2021). Table 24 shows the relevant standards to cyber security education for schools in California. Computer science is not a requirement for graduation, nor do schools have to offer computer science (Public Policy Institute of California, 2018). Courses have also been reported not to be sufficiently robust to prepare pupils for studying computer science at the higher education level (ibid).

Table 24: Computer science standards in California (California Department for Education, 2018)

ISCED level (Age)	Standard relevant to cyber security
ISCED level 1 (ages 5-8)	*"K-2.NI.5 Standard: Explain why people use passwords."*
ISCED level 1 (ages 8-11)	*"3-5.NI.5 Standard: Describe physical and digital security measures for protecting personal information."* *"3-5.NI.6 Standard: Create patterns to protect information from unauthorized access."*

ISCED level 2 (ages 11-14)	*"6-8.NI.5 Standard: Explain potential security threats and security measures to mitigate threats."* *"6-8.NI.6 Standard: Apply multiple methods of information protection to model the secure transmission of information."*
ISCED levels 3 and 4 (ages 14-18)	*"9-12.NI.6 Standard: Compare and contrast security measures to address various security threats."* *"9-12.NI.7 Standard: Compare and contrast cryptographic techniques to model the secure transmission of information."* *"9-12S.NI.5 Standard: Develop solutions to security threats."* *"9-12S.NI.6 Standard: Analyze cryptographic techniques to model the secure transmission of information."*

Computer science and digital fluency learning standards were adopted in 2020 in the State of New York, with cyber security being one of the five core concepts which the new standards focus on (New York State Education Department, 2020). Each standard is broken down into three core areas; for cyber security these are: risks, safeguards and response (New York State Education Department, 2020). Each standard has specific items for age group in compulsory education. An example standard for each domain and each age group is given in Table 25.

In spite of the presence of digital learning standards, and associated resources, there appears no one set way to teach these standards, with schools being afforded flexibility in how they teach the standards (New York State Education Department, nd-a). Furthermore, computer science courses currently count as either elective credit, or a third unit of credit in mathematics or science and are not compulsory for graduation.

Table 25: Example standards from the Computer Science and Digital Fluency Standards of the New York State Education Department (2020)

Domain area	ISCED level 1 (age 5-7)	ISCED level 1 (age 7-9)	ISCED levels 1-2 (age 9-12)	ISCED level 2 (age 12-14)	ISCED levels 3-4 (age 14-18)
Risks	K-1.CY.1 Identify reasons for keeping information private	2-3.CY.1 Compare reasons why an individual should keep information private or make information public	4-6.CY.1 Explain why different types of information might need to be protected	7-8.CY.1 Determine the types of personal information and digital resources that an individual may have access to that needs to be protected	9-12.CY.1 Determine the types of personal and organizational information and digital resources that an individual may have access to that needs to be protected
Safeguards	K-1.CY.2 Identify simple ways to help keep accounts secure	2-3.CY.2 Compare and contrast behaviors that do and do not keep information secure	4-6.CY.2 Describe common safeguards for protecting personal information	7-8.CY.2 Describe physical, digital, and behavioral safeguards that can be employed in different situations	9-12.CY.2 Describe physical, digital, and behavioral safeguards that can be employed to protect the confidentiality, integrity, and accessibility of information

Response	K-1.CY.5 Identify when it is appropriate to open and/or click on links or files	2-3.CY.5 Identify unusual activity of applications and devices that should be reported to a responsible adult	4-6.CY.5 Explain suspicious activity of applications and devices	7-8.CY.5 Describe actions to be taken before and after an application or device reports a security problem or performs unexpectedly	9-12.CY.5 Recommend multiple actions to take prior and in response to various types of digital security breaches

As part of the computing curriculum, there are courses which can be taught to pupils over a wide age range and ISCED levels. Courses and programmes which include elements of cyber security include (Computer Science For All, 2021):

- ***Software engineering program junior*** (ISCED level 1; ages 5-11)
- ***CODE.ORG Computer Science Discoveries*** (ISCED level 2; ages 11-14)
- ***Software engineering program*** (ISCED levels 2-4; ages 11-18)
- ***Computer Science Principles*** (ISCED levels 3-4; ages 15-18) – focus on data privacy
- ***Advanced placement computer science A*** (ISCED levels 3-4; ages 15-18) – focus on the ethical and social implications of computing

Note only the latter two include explicit mention of content relevant to cyber security. Programme requirements are due to be recommended to the **Board of Regents** in Autumn 2021 (New York State Education Department, nd-a). Currently health, physical education, and family and consumer sciences do not teach aspects of cyber security and online safety (New York State Education Department, nd-b).

'Standards for Texas Essential Knowledge and Skills (TEKS) for Technology Applications' include aspects of digital citizenship for ISCED levels 1 and 2 (ages 5-14) (TEA, 2012a, 2012b) with computer science courses being a mandatory part of what school districts are required to offer high school students (ISCED levels 3 and 4, ages 15-18) (TEA, 2021). The *TEKS* are based on the ***NETS*** standards (TEA, 2012a, 2012b). Table 26 gives detail about the TEKS for ISCED levels 1 and 2. For ISCED levels 3 and 4 we did not find TEKS standards defined.

Table 26: An overview of the TEKS for ISCED levels 1-2 (ages 5-14) in Texas (TEA, 2012a, 2012b)

ISCED level (age)	TEKS digital citizenship standard
ISCED level 1 (age 5-11)	Digital citizenship. The student practices safe, responsible, legal, and ethical behavior while using digital tools and resources. The student is expected to: (A) adhere to acceptable use policies reflecting appropriate behavior in a digital environment; (B) comply with acceptable digital safety rules, fair use guidelines, and copyright laws; and (C) practice the responsible use of digital information regarding intellectual property, including software, text, images, audio, and video
ISCED level 2 (age 11-14)	The student practices safe, responsible, legal, and ethical behavior while using technology tools and resources. The student is expected to: (A) understand copyright principles, including current laws, fair use guidelines, creative commons, open source, and public domain; (B) practice ethical acquisition of information and standard methods for citing sources; (C) practice safe and appropriate online behavior, personal security guidelines, digital identity, digital etiquette, and acceptable use of technology; and (D) understand the negative impact of inappropriate technology use, including online bullying and harassment, hacking, intentional virus setting, invasion of privacy, and piracy such as software, music, video, and other media.

Upon examining computer science courses, it does appear that digital citizenship is part of the curriculum for computer science courses for pupils at ISCED levels 3-4 (14-18) (WeTeach, 2020). College readiness tests do not examine computer science or information technology, only mathematics and English (Texas Higher Education Coordinating Board, nd).

There are core standards for computer science all ages in **Utah**. The impact of computing standard refers to digital citizenship, privacy, copyright, accessibility, ethics (Utah Education Network, 2019a, 2019b) and '*the network and the internet standard*' also contains aspects of cyber security. Table 27 gives a summary of the impact of computing standards.

Table 27: An overview of the Computing standards in Utah (Utah Education Network, 2019a, 2019b)

ISCED level (age)	Relevant Network and the Internet or Impact of computing standard
ISCED level 1 (age 5-6)	No relevant standards for this age group
ISCED level 1 (age 6-7)	*"Standard 1.IC.1 Develop and demonstrate the ability to work respectfully and responsibly with others whether communicating face-to-face or digitally."*
ISCED level 1 (age 7-8)	*"Standard 2.NI.1 Explain what a password or pass phrase is, why it is used, and be able to create a secure password."* *"Standard 2.IC.1 Describe how technology has impacted society over time."* *"Standard 2.IC.2 Describe rationales for keeping login information private, and for logging off devices appropriately."*
ISCED level 1 (age 8-9)	*"Standard 3.NI.1 Describe physical and digital security measures for protecting personal information."* *"Standard 3.NI.2 Develop personal patterns of behavior to protect information from unauthorized access."* *"Standard 3.IC.1 Evaluate how computing technologies have changed the world, and express how those technologies influence, and are influenced by, cultural practices."* *"Standard 3.IC.2 Describe reasons creators might limit the use of their work."*
ISCED level 1 (age 9-10)	*"Standard 4.IC.1 Evaluate computing technologies that have changed the world and express how those technologies influence and are influenced by cultural practices."* *"Standard 4.IC.2 Propose ways to improve the accessibility and usability of technology products for the diverse needs and wants of users."*
ISCED level 1 (age 10-11)	*"Standard 5.IC.1 Propose ways to improve the accessibility and usability of technology products for the diverse needs and wants of users."* *"Standard 5.IC.2 Seek and explain the impact of diverse perspectives for the purpose of improving computational artifacts."*
ISCED level 2 (age 11-12)	*"Standard 6.NI.1 Explain potential security threats and practice protective measures to reduce these threats."* *"Standard 6.IC.1 Recognize and discuss issues of bias and accessibility in existing technologies."*
ISCED level 2 (age 12-13)	*"Standard 7.IC.1 Compare tradeoffs associated with computing technologies that affect people's everyday activities and career options."*
ISCED level 2 (age 13-14)	No relevant standards for this age group
ISCED level 3 (age 14-16)	*"Standard 9/10.IC.1 Evaluate how computing has impacted and/or impacts personal, ethical, social, economic, and cultural practices."*
ISCED level 4 (age 16-18)	*"Standard 11/12.NI.1 Identify types of security threats, and then compare and contrast measures that can be used to address, resolve, and/or prevent identified threats."* *"Standard 11/12.NI.2 Compare and contrast cryptographic techniques to model the secure transmission of information (data)."* *"Standard 11/12.IC.1 Evaluate and discuss the ways computing impacts personal, ethical, social, economic, and cultural practices."*

There is also a current push in **Utah** to increase the profile of computing education in pre-university education, with a recent report by Bonilla and Paul (Bonilla & Paul, nd), which are guidelines to assist the provision of computer science being available to all pupils by 2022. One aspect of this report is the call for standards in the curriculum and increasing awareness of computer science work (ibid, p11).

5.4. Implementation landscape

The way in which various policy is enacted into initiatives is diverse and although there are similarities across the countries in some ways (in the provision of cyber security centres and the existence of educational policy), how centralised this is from various governments and departments is variable.

5.4.1. Government and national agency action and initiatives

As stated in Section 4.4.1, children's commissioners can be important sources of information for online safety. Table 28 gives an overview of whether the countries covered in this section have a children's commissioner and any relevant work occurring in the realm of cyber security and online safety:

Table 28: Existence of a children's commissioner in countries covered in Section 5

Country	Children's Commissioner?	Any relevant work to cyber security and online safety
Australia	Yes – named **eSafety Commissioner**	Online resources and programmes on cyber bullying, online abuse and illegal online content. This includes programmes for children and young people; teachers, parents, professionals. (eSafety Commissioner (Australia), nd-a; nd-b; nd-c). Directory of information for young people about: unwanted content, cyber bullying, privacy and security (eSafety Commissioner (Australia), nd-d). The eSafety Commissioner plays a key role in Safer Internet Day (SID) (eSafety Commissioner (Australia), nd-e). ***'Best Practice Framework for Online Safety Education'*** launched by eSafety Commissioner, covering the following topics (eSafety Commissioner (Australia), 2021): "*Students rights and responsibilities in the digital age*", "*Resilience and risk*", "*Effective whole school approaches*", "*Integrated and specific curriculum*", and "*Continuously improved through review and evaluation*". A toolkit for schools is also available (eSafety Commissioner, nd-f), with further teaching resources to be used with pupils available (eSafety Commissioner (Australia), nd-g).
Canada	No – but bill introduced in 2020 (Children First Canada, 2020; Parliament of Canada, 2020)	Not relevant
New Zealand	Yes	Publication of '***Safer Viewing Online for Children and Young People***' (Children's Commissioner (New Zealand), 2019). Links to useful resources (Children's Commissioner (New Zealand, nd) Links to Netsafe on their website (Netsafe, nd-a)

Singapore	No	Not relevant
US	No – but some states have a statewide commissioner (e.g., Utah; (Utah Department of Human Services, nd))	None from the states included in this report

We will now take each country in turn in regards to actions and initiatives of other governmental bodies and national agencies.

5.4.1.1. Australia

The **ACSC** (**Australian Cyber Security Centre**), part of the **Australian Signals Directorate**, is a centre leading the government's efforts to improve cyber security (ACSC, nd-a). The ACSC has provided educational resources and information for parents and carers, however these are self-directed and for parents' and carers' own actions, rather than for use with children and young people (ACSC, nd-b). There are campaigns and events launched and run by the ACSC, however none of these appear to be targeted at children or young people and seem to be targeting the general population more widely (ACSC, nd-c). The educational programmes run by the ACSC also currently appear to be focused on professionals and businesses, rather than children and young people (ACSC, nd-d).

The Australian Government's **Student Wellbeing Hub** has a collection of freely available resources and information – some of which are self-directed (for children and young people to do themselves), some for teachers, and some for parents (Student Wellbeing Hub, 2020a). The Cyber A.C.E.S (Activities in Cybersecurity Education for Students) Program is a part of the hub, and provides hands on activities on the topic of cyber security (Student Wellbeing Hub, 2020b). Four modules are provided and each is tailored for a different age group (module one – age 5-7; module 2 – age 8-10; module 3 – age 11-13; module 4 age – 14-15) (Paloato, nd).

The **Digital Industry Group Inc** published 'Australian Code of Practice on Disinformation and Misinformation' (DIGI, 2021). The aim is to 'provide safeguards against harms from the spread of disinformation and misinformation on digital platforms' (AMCA, 2021). No other mention of any cyber security or online safety was found to date from AMCA.

Grok Academy (in conjunction with Australian government and Australian Signals Directorate) have run the schools cyber security challenge since February 2019. This is for children at ISCED level 1 (age 5-12) and consists of three activities:

- ***Grok Cyber Comp*** – 1x 45 min activity to be done online
- ***Grok Cyber Pursuit*** – a series of CTF-style events (between July and September 2021)
- ***Grok Cyber Live*** – November 2021 event

These appear to be 'opt in' activities. Grok Academy also has information available for pupils and teachers and/or parents in addition to the Cyber Security Challenge (Grok Academy, nd-a). Grok Cyber Pursuit runs in four bandings according to age groups: 12-14, 14-16, 16-17 and 17-18 (Grok Academy, nd-b).

Grok Academy have further resources and online training for children and young people of a variety of ages, including on privacy, phishing and data encryption and Australian pupils have access via their school, or subsidised access via their school (Grok Academy, nd-c).

5.4.1.2. Canada

At the **Canadian Centre for Cyber Security**, resources and infographics are available for self-directed learning (Canadian Centre for Cyber Security, 2021a). However, there is no specific

guidance for children or young people in the information section (ibid). The Canadian Centre for Cyber Security also hosts a Learning Hub, including courses on COVID-19 Cyber Threat Awareness, Discovering Cyber Security and Cyber Security for Educators (Canadian Centre for Cyber Security, 2021b). Of particular interest is the course ***Cyber Security for Educators***, which includes the following (Canadian Centre for Cyber Security, 2021b):

- '*basic knowledge of cyber security concepts such as cyber terminology*'
- '*cyber protection measures*'
- '*cyber security in the classroom and careers in cyber security*'

The annual ***Cyber Security Awareness Month*** (Canadian Centre for Cyber Security, nd) is promoted and academic outreach is also advertised, however, this appears to be aimed at tertiary education rather than primary or secondary (Canadian Centre for Cyber Security, 2021c). There are, however, teaching resources for elementary and high school pupils in both English and French (Canadian Centre for Cyber Security, 2021d). The resources are differentiated by age, including:

- ISCED level 1-2 (ages 5-12)
- ISCED levels 2-4 (ages 12-18)

Resources for both pupils and teachers are included, and ***Common Sense Education*** is recommended as a source.

Get Cyber Safe is a national public awareness campaign about cyber security, online safety and keeping personal information safe online by the **Government of Canada** (Government of Canada, 2022). Information is available on keeping passwords safe, securing devices and connections. *Get Cyber Safe* ran a challenge called ***Get Cyber Safe Challenge 2021*** (Government of Canada, 2021b), with each week focused on one area of cyber security for participants to action. This included: week 1 – strong passphrases, week 2 – multifactor authentication, week 3 – system updates and week 4 – securing your Wi-Fi. Further information, infographics and apps to track progress are also linked. This information is likely to be useful to young people, however this campaign does not target them directly. Regular blogs are posted as part of the campaign, with the ability to filter blogs for young people, however these are not solely targeting young people (Government of Canada, 2021c).

5.4.1.3. New Zealand

At **New Zealand**'s **National Cyber Security Centre** (NCSC-NZ), cyber crime can be reported (NCSC-NZ, nd-a) and an online training module is available; '***Charting Your Course: Cyber Security Governance***' (NCSC-NZ, nd-b). This is aimed at businesses, in particular senior leadership and practitioners. Resources suggested by the NCSC-NZ notably include SANS Internet Storm Center (2021), which pitches information at a more technical level and less towards pre-university level education. In 2021, it was reported that NCSC-NZ offered teachers cyber security training (Computer Weekly, 2021) however nothing has been found to date on offering to children and young people. There is also an online interactive storybook named ***Inter-Yeti*** provided through the Department of Internal Affairs (nd-a) for children aged 5-11 years old. The content covered in this resource includes: staying safe online, inappropriate content, cyber bullying, sharing of personal information and online grooming (Department of Internal Affairs (New Zealand), nd-b).

CERT NZ (**National Computer Emergency Response Team New Zealand**) also plays an educational role in New Zealand, mainly via its Cyber Smart programme, which tries to 'Cyber Up' the general public's cyber security and online safety awareness and basic skills (CERT NZ, nd).

5.4.1.4. Singapore

The ***Singapore Cyber Security Strategy 2021*** highlights ***SG Cyber Youth*** (CSA Singapore, nd-a), a **CSA Singapore**-led national programme for guiding children and young people (especially those in secondary schools) towards a cyber security career pathway, supported by the academia, community, and industry (CSA Singapore, 2021a, p53). A number of important activities relevant for pre-university cyber security education are mentioned in the 2021 Strategy as parts of SG Cyber Youth: 1) ***Youth Cyber Exploration Programme*** (**YCEP**) for introducing pre-university pupils to cyber security and encouraging them to consider a cyber security career (CSA Singapore, nd-b); 2) ***Student Volunteer & Recognition Programme*** (***SVRP***) (CSA Singapore, nd-a); 3) ***Cybersecurity Learning Journeys*** (CSA Singapore, nd-a); and 4) ***SG Cyber Olympians programme*** (CSA Singapore, nd-a). There is also a ***Cybersecurity Career Mentoring Programme*** (***CCMP***) for providing tertiary (i.e., higher education) students and young professionals with career guidance shared by industry mentors (CSA Singapore, nd-c), which is less about pre-university education. As part of the SG Cyber Youth programme, CSA Singapore also created ***SG Cyber Youth Odyssey*** (CSA Singapore, 2021b), a learning roadmap for key initiatives under *SG Cyber Youth*, including ***YCEP***, ***Advanced YCEP*** (***A.YCEP***), and ***SG Cyber Olympians***. The SG Cyber Youth Odyssey was developed by CSA Singapore '*in consultation with educators, industry practitioners and training partners*'. The initiative sets a four-staged learning roadmap: 'Excite', 'Explore', 'Experience' and 'Excel'. Table 29 shows more details of the first three stages of the initiative.

Table 29: The first three stages of the SG Cyber Youth Odyssey initiative, adapted from the table in (CSA Singapore, 2021b)

Odyssey Stage	'Excite'	'Explore'	'Experience'
Target Audience	Pre-university pupils with *no* cyber security knowledge and may have never heard of cybersecurity	Pre-university pupils with *limited* cyber security knowledge and curious to learn more	Pre-university pupils with *some* cyber security knowledge who are considering cyber security as a (future) career option
Focus	Overview	Blue teaming / Defending networks	Red teaming / Ethical hacking
Example Activities	School Assembly Talks, Visits to Companies	YCEP, Infocomm Club Activities	A.YCEP
Typical Hands-on Exercises	Securing mobile devices (most applicable and easiest to adapt in schools)	Network security (e.g., wireless security)	Web applications, IoT and penetration testing

Singapore's ***Safer Cyberspace Masterplan*** (CSA Singapore, 2020a) builds on the second pillar of the *Singapore Cybersecurity Strategy 2016*. One key aspect of the masterplan that links to pre-university cyber security education is *'empowering the cybersavvy population'*, including through ***outreach in schools*** and introducing a cyber security module as part of the ***Code for Fun programme*** for upper primary pupils (CSA Singapore, 2020a, p49).

A major programme of outreach in schools in Singapore's *Safer Cyberspace Masterplan* is the ***SG Cyber Safe Students Programme*** (CSA Singapore, nd-d), which has a focus on online safety and cyber hygiene. Content is available to be used in CCE lessons, including videos (CSA Singapore, nd-e). Content includes how to protect yourself from cyber crime and hacking, using safe passwords and exploring the digital world in a safe way. Printable materials are also

available, with pupils being able to use these in their own time, or teachers using these materials as part of lesson plans (CSA Singapore, nd-f).

As part of the *SG Cyber Safe Students Programme*, three outreach activities are highlighted in Singapore's Safer Cyberspace Masterplan (CSA Singapore, 2020a, p49): ***Cyber Safety Activity Book***, ***Go Safe Online Drama Skit***, and ***Cyber Savvy Machine Pop-up***. The ***Go Safe Online Drama Skit*** as is a 30-minute interactive drama skit that aims to educate pupils on cyber security. Pupils will get a chance to make choices on behalf of the characters and influence how the storyline progresses. A pilot of the skit was run with secondary schools in 2019, reaching out to nearly 40,000 pupils (ibid). Due to the success of the pilot, the skit was extended to primary and secondary schools since August 2021, under a slightly different name '***Go Safe Online Awareness Skit***' (CSA Singapore, nd-g). The ***Cyber Safety Activity Book*** is a programme of CSA Singapore, in collaboration with the **Personal Data Protection Commission** from 2016 to 2019 and then with the **Singapore Police Force** (**SPF**) in 2020, leading to five issues of the Cyber Safety Activity Book for raising awareness of cyber security and personal data protection, and the "***Cyber Safety: The Interactive Handbook***" to help pupils stay safe online (CSA Singapore, 2020b). Nearly 250,000 issues of the Cyber Safety Activity Book series and handbook were distributed to Primary 5 students according to (CSA Singapore, 2020a, p49). The ***Cyber Savvy Machine Pop-Up*** launched in 2018 consists of an interactive vending machine and information panels, showcasing cyber security tips and a quiz for the public to test their knowledge. It travelled to many public places including schools over 16 months in a tour ended in February 2020, and over 100,000 quiz attempts were recorded. This programme is still active, but under a new name '***Go Safe Online Pop-up***'.

CSA Singapore also runs a separate programme called ***SG Cyber Safe Programme*** (CSA Singapore, nd-h) targeting businesses, and another programme called ***SG Cyber Safe Seniors Programme*** (CSA Singapore, nd-o) targeting senior citizens, neither of which has a focus on the pre-university education setting. In addition, CSA Singapore co-chairs the ***Cyber Security Awareness Alliance***, which comprises representatives from the government, private enterprises, trade associations and non-profit organisations (CSA Singapore, nd-i). The Alliance's tagline is '***Go Safe Online***' (***GSO***), and currently there is a dedicated microsite as part of the CSA Singapore's website (CSA Singapore, nd-j). GSO aims to increase awareness of safety online among the general population and businesses (including SMEs). It also provides general online safety information for pupils and parents, mainly through tips and information (CSA Singapore, nd-k, nd-l, nd-m).

In addition to the above programmes and activities, as part of the SG Cyber Safe Students Programme, cyber experts from CSA Singapore and the Cyber Security Awareness Alliance also conduct talks at schools to share their knowledge on cyber security with students through case studies, hacking demonstrations and online quizzes.

Another group of public bodies in Singapore that has relevant activities are law enforcement agencies, especially the **SPF** and the **NPCC** (**National Police Cadet Corps**). The NPCC is a youth uniformed group targeting school pupils aged between 13-17, supported by three public bodies in Singapore: **Ministry of Home Affairs**, **Ministry of Education** and the **SPF** (NPCC, nd; Wikipedia, nd-b). As mentioned before, Singapore's Cybersecurity Strategy 2021 also refers to the ***NPCC Cybercrime Prevention Programme*** (CSA Singapore, 2021a). The **SPF** also runs the ***Collaborative Social Programme*** (***CoSP***) mentioned in Section 5.2.4, as part of the ***National Cybercrime Action Plan*** (***NCAP***) stated in Singapore's Cybersecurity Strategy 2016 (CSA Singapore, 2016). The CoSP involves working between the SPF and schools, with a focus more on cyber crime prevention and vulnerable groups rather than on pre-university education.

5.4.1.5. US

The **NIST**'s ***National Initiative for Cybersecurity Education*** (***NICE***) holds responsibility for cyber security education and workforce development in the US. Some of the educational offering provided by the NICE does not target at children and young people within a pre-university educational context, e.g., ***Federal Cybersecurity Workforce Summit*** (NIST, 2021h). However, there are initiatives targeting the general population, e.g., '***What is Cybersecurity Career Awareness Week?***' (NIST, 2021e), which is also directly advertised to schools (NIST, 2020b). The NICE also helps advertise other pre-university cyber security education and awareness programmes (not necessarily offered by the NICE itself), including ***GenCyber, CyberPatriot*** and ***SANS CyberStart*** (see below and Section 5.4.3 for more details of these programmes). The NICE also has a ***K12 Cybersecurity Education Community of Interest***, which acts as a community of practice between teachers, other school staff, government departments and industry (NIST, 2021b). Its four active programmes are:

- *Removing roadblocks to Cybersecurity Experiences in K12*
- *Career Technical Education Programs of Study*
- *K12 Educational Materials: Content Review and Repository Recommendations*
- *K12 Cybersecurity Educational Instructional Professional Development (PD) Series*

Cybersecurity Career Awareness Week is an active project of this subgroup.

Partnered with iKeepSafe (iKeepSafe, nd-a) as the host, the NICE also supports the ***National Cyber Signing Day*** as part of the ***NICE K12 Cybersecurity Education Conference*** to celebrate high school students and recent graduates at ISCED levels 3-4 for their achievements in cyber security (iKeepSafe, nd-b). This is, particularly for those who have undertaken an internship, undertaken a community project, or training or certification relevant to cyber security. This event is organised in the form of a pre-recorded presentation, which announces pupils' achievements in a 'sports announcer style', and presents their future goals in cyber security.

The **CISA** (**Cybersecurity and Infrastructure Security Agency**) (CISA, nd-a) leads the US' work on cyber security and provides a list of services particularly aimed at businesses, such as ***Cyber Essentials*** (CISA, nd-b); ***Cyber Resource Hub*** (CISA, nd-c); and ***Cybersecurity Training and Exercises*** (CISA, nd-d). Their cyber security education and career development offer (CISA, 2020) targets employees, business and graduates instead of children and young people, echoing some of the provision of the CSA Singapore (e.g., the Cybersecurity Career Mentoring Programme). The **CISA** also support ***National Cyber Security Awareness Month*** (CISA, nd-e), along with **Department of Homeland Security**. This initiative targets the general population each October about cyber security and what to do in the case of a cyber incident. The hashtag ***#BeCyberSmart*** is used to promote and share involvement in the US' ***National Cybersecurity Awareness Month***.

The ***STOP. THINK. CONNECT.™ campaign*** (STOP. THINK. CONNECT., nd) is an initiative led by the U.S. Department of Homeland Security, and its development is a joint effort between the **Anti-Phishing Working Group** (**APWG**) and the **National Cyber Security Alliance** (**NCSA**). It targets the general population in raising awareness of cyber threats and how to be safer online.

GenCyber is a programme led by the **National Security Agency** (**NSA**), with financial support from the **National Science Foundation** (**NSF**) and other federal partners on an annual basis (NSA, nd). It provides students and teachers at the K-12 level with summer cyber security camp experiences. The main goals include (ibid):

- *"Ignite, sustain, and increase awareness of K12 cybersecurity content and cybersecurity postsecondary and career opportunities for participants through year-round engagement;*
- *Increase student diversity in cybersecurity college and career readiness pathways at the K-12 level; and*
- *Facilitate teacher readiness within a teacher learning community to learn, develop, and deliver cybersecurity content for the K-12 classroom in collaboration with other nationwide initiatives."*

5.4.2. Communities of practice and resources

In **Ontario, Canada**, the **Cyber Security Centre of Excellence** educates school boards on cyber security and promotes ***Cyber Security Awareness Month*** (Ontario Ministry of Government and Consumer Services, 2021). Online teaching modules are also available, but this appears not to be targeted at children or young people, rather businesses (Cyber Security Ontario, nd). A community of practice network is also available to join for those who are interested in cyber security, as well as the Cyber Security Centre of Excellence (Cyber Security Ontario, nd). People who can join are from the public sector as a whole; it is not specific to education and school boards, but likely covers them.

Ontario also has a ***Digital and Data Strategy*** (2021), with one of the challenges being reskilling and retraining people in digital skills. However, there is no mention of education, training or upskilling children or young people and appears to focus on working age adults, businesses and the public sector.

In the US, the **National Initiative for Cybersecurity Careers and Studies** (NICCS) does do work with school teachers (elementary, middle and high school) in terms of providing lesson plans, curricula, quizzes and worksheets (NICCS, 2021) and support pupils with classes and career profiles (Cyber.org, nd).

5.4.3. Companies, charities and non-government organisations (NGOs)

Companies, charities and other non-government organisations also provide aspects of pre-university cyber security education, often either supplementing what is already provided by government organisations, or providing input where there is not already input. As in Section 5.4.1., each country in this section is presented in turn.

5.4.3.1 Australia

Digital technologies hub and Education Services Australia provides information for students of a self-directed learning nature (Digital Technologies Hub, nd-a), including on cyber safety (Digital Technologies Hub, nd-b). The information is for grades 3-12 and stratified for different age groups. Information on cyber bullying and safe internet use. Information for teachers is also available too (Digital Technologies Hub, nd-c), which includes lesson plans, supporting documents for the ***Digital Technologies Curriculum*** and training for teachers. **Education Services Australia (ESA)** provides a link to Digital Technologies Hub in regards to resources for the Digital Technologies Curriculum for both parents and teaching staff (Digital Technologies Hub, nd-d).

5.4.3.2. Canada

In regards to the **Information and Communications Technology Council (ICTC)**, the federal budget of Canada is funding $80 million over three years to ISED Canada. This will be used to help ***CanCode*** reach 3 million further pupils (ISCED levels 1-4; age 5-18 k) and 120,00 teachers (ICTC, 2021). Although the core of the programme is programming, this supports the introduction of digital skills into classrooms (a key aspect of cyber security education) (Government of Canada, 2019).

The ***CyberSci Canadian championships*** competition is not for school aged children and young people (CyberSci, nd), however it follows a similar pattern to other cyber security challenges in other countries.

CTRL-F is a Canadian initative for schools on digital media literacy, which is built around lateral reading strategies that fact checkers use (CIVIX, nd). These lateral reading strategies are: investigate the source; check the claim; and trace the information. Classroom tools are also available for teachers and other school staff to use, including: lesson plans, videos, slide decks, practice examples, activity sheets, and assessments. Videos are also available and the resources are available in both English and French.

5.4.3.3 New Zealand

Netsafe (Netsafe, nd-a) advises teachers on how to teach digital citizenship, highlighting that digital citizenship should be embedded into both New Zealand's Curricula (Netsafe, 2018, p3). Note that Netsafe's guidance is not designed to address the technology curriculum learning area. The role of Netsafe is to support schools to be able to educate children and young people about online safety:

> *"When we talk about being safe and secure online, we're really talking about in the context of schools and kura supporting children, to have conversations with whānau [families], to provide the right environment for safe online learning to take place. And so that is the focus of the programme, really. It's about preparing schools in whatever context they decide to deliver the whole curriculum and to provide them with support to do that." – Director of Research and Policy, Netsafe, New Zealand*

Successful teaching of digital citizenship is described by Netsafe where it is *'deliberately weaved into the curriculum, across learning areas'* (Netsafe, 2018, p14). Netsafe have also input into ***School Evaluation Indicators***, which support and guide the implementation of the New Zealand Curriculums (ERO, 2016), with a focus on learners being ready for the digital world at the end of their schooling (Netsafe, 2018, p17).

Furthermore, Netsafe provides information on online bullying (Netsafe, 2020) and managing digital footprints (Netsafe, 2021). Information is also available for parents (Netsafe, nd-b) and teachers/facilitators (Netsafe, nd-c). Netsafe also has a schools programme which evaluates growth and commitment to teaching and a culture of online safety, comprising the following levels (Netsafe, nd-d):

- '***Beginning*** *– Te Kākano: This tier reflects a commitment to creating a safer online learning environment.*
- ***Growing*** *– Tipu ma toro: This tier reflects a pro-active approach to online safety, citizenship and wellbeing initiatives.*
- ***Mature*** *– Te Puāwaitanga: These schools have met the Growing – Tipu ma toro expectations and are willing to share their practices to help other schools and kura.*

Schools can nominate themselves here and Netsafe will announce the recipients twice a year.'

In order to gain this accreditation, schools must fill out the ***Netsafe Schools Review Tool***, with the tier relevant to their outcome being the tier they earn (Netsafe, nd-d). The tool is built to encourage educators' engagement with aspects of cyber security policy, practices and teaching at a pre-university level:

> *"So, because the tool is not mandated, we have to make it as engaging as possible to encourage schools to participate in the programme. The aim is to provide a way for schools to show the progress they are making, it's not an accreditation model involving inspection or external assessment of certain criteria and levels met. It's a lot broader approach, for example, to get schools to think and talk about their development, create active plans, and demonstrate progress around that." – Director of Research and Policy, Netsafe, New Zealand*

Teaching and classroom resources are also available for teachers and facilitators in regards to lesson planning (Netsafe, nd-e).

The ***New Zealand Cyber Security Challenge*** (Cyber Security Challenge (New Zealand), 2021, nd)) has 3 rounds: qualifying (rounds 0, (capture the flag style), 1 (incident response round) and 2 (capture the flag style). Participants must compete alone. The competition is not only for young people, however there is one category for secondary school pupils (years 9-13). Content of the tasks include:

- Cryptography
- Steganography
- Web Security
- Reverse Engineering
- Social Engineering
- Digital Forensics

5.4.3.4 US

CyberPatriot is the National Youth Cyber Education Program of the not-for-profit organisation **AFA** (**Air Force Association**) (AFA, nd-a). At the centre of this programme is a ***National Youth Cyber Defense Competition*** for pupils age 14-18 (ISCED 3-4) and pupils aged 11-14 (ISCED level 2). ***CyberPatriot*** also hosts ***AFA CyberCamps*** held during summer months, where basics of cyber security are taught to participants (AFA, nd-b). Provision for pupils aged 5-11 is through online modules which are available for the pupils to do in their own time at home or in school. There are two types of AFA CyberCamps: the standard ones teach beginners about basics of cyber security, and advanced ones target pupils who have participated one standard camp or the National Youth Cyber Defense Competition. CyberPatriot also has an ***Elementary School Cyber Education Initiative*** (***ESCEI***), which offers three free learning modules aimed at increasing cyber security and online safety awareness among K-6 students (AFA, nd-a). CyberPatriot's ***Cyber Education Literature series*** launched in 2017 publishes books for young children and pupils in ISCED 0-1 stages. Its first book, ***Sarah the Cyber Hero***, was published in 2017 (AFA, 2017; nd-c). In addition to the above activities for children and young people, CyberPatriot also has ***CyberGenerations*** for senior citizens and ***Tech Caregiver Program*** for student and adult volunteers who want to be ***CyberGenerations*** trainers, which are less related to pre-university education (AFA, nd-a).

In addition to CyberPatriot programme, the **US** has a variety of other cyber security camps and CTF-style competitions that target at children and young people. One such example is ***SANS***

Cyber Camp for teenagers (SANS Institute, nd), a camp run by the cyber security not-for-profit company **SANS Institute** (SANS Institute, 2022). There is no lower age limit for this camp, but if you are under the age of 13, a parent or carer must register the child or young person onto SANS Cyber Camp rather than the child or young person themselves signing up. The camps contain hands on workshops, learning how to protect yourself online and exploring different career paths in cyber security. The last camp was held in December 2020 due to the COVID-19 pandemic.

Among other activities, the not-for-profit organisation **Common Sense Media** provides information for parents on privacy, online safety and social media (Common Sense Media, nd-a, nd-b), as well as other topics such as suitability of different media (e.g., books and movie reviews). Information is stratified by age group, with differing recommendations per age group from ISCED level 0 (ages 2-4) to ISCED levels 2-4 (age 13 and above). Common Sense Media take an online safety approach to cyber security education, with articles and blogs giving tips and advice for parents on Zoom, Google Classroom and data protection. There are also videos in addition to the written material (Common Sense Media, nd-b).

5.5. Socio-cultural landscape

Just as digital skills are perceived as inherently **important in the job market** in the UK, digital skills were seen as equally important in all the five countries focused upon in this section. The governments may prioritise cyber security as an area to focus on, including pre-university education of children and young people.

> *"…, governments, particularly here in Australia, they've invested a lot of money into cyber security, into defence, into upskilling people. We've got some great pathways from school onwards into industry that are all working on that and the government have the funding to support that. They do see it as a crucial part." – A/Curriculum Specialist Technologies, Australian Curriculum, Assessment and Reporting Authority (ACARA), Australia*

Diversity in cyber security is also perceived to be highly important, echoing our findings from the UK. Again, women and girls appear to be the most targeted group for cyber security educational provision, both at pre-university and university levels (CSA Singapore, nd-n).

> *"In Singapore, we have launched the SG Cyber Women initiative to interest and engagement more females, from as young as pre-tertiary age, in cybersecurity. Under SG Cyber Women, we partner with professional bodies and communities to roll out career talks, industry sharing, mentoring, and CTFs, to build up their cybersecurity knowledge and skills." – Senior Assistant Director, Ecosystem Development, Cyber Security Agency of Singapore, Singapore*

Another finding echoing the UK was the **divide** between computational thinking and ICT, in this case being described as 'having a security mindset'. This was seen to impact the talent pipeline, and was something that needed to be addressed at a pre-university level to improve the numbers of people interested in cyber security and uplift the cyber security workforce.

> *"But they were having people coming into the tertiary courses with very limited understanding that they had programming skills [and] they could code. They could do that fun stuff, but they really didn't have [done it] well, they didn't have that security mindset." – A/Curriculum Specialist Technologies, Australian Curriculum, Assessment and Reporting Authority (ACARA), Australia*

After-school interest groups and clubs in some of the countries covered in this section may also take a **form different from those in the UK**. In particular, Australia was described as having

many extra-curricular activities focusing on sports, which influences the offer that can be made in relation to pre-university cyber security education:

> *"So students often participate in sport training after school rather than dedicated Digital Technologies activities." – A/Curriculum Specialist Technologies, Australian Curriculum, Assessment and Reporting Authority (ACARA), Australia*

How to **engage** pupils and keep them interested in cyber security educational content was also vital, especially for younger pupils.

> *"There are suggestions that the resources to engage younger students should be gamified, in order to keep their interests on the topic." – Senior Assistant Director, Ecosystem Development, Cyber Security Agency of Singapore, Singapore*

The **nature of the countries** in this section were also quite different, with New Zealand in particular having many schools in rural areas and smaller schools on the whole. This seems to impact the pre-university cyber security offer within the school curriculum, as sometimes specialists may be harder to recruit to some areas and the teacher's own knowledge shapes the content taught in the classroom, and subsequent clubs that may be set up.

> *"New Zealand's schools and kura range in size from just a few ākonga [pupils] up to a roll of around 2,000 … Many are in rural locations … Size and location can both potentially create challenges, for example, when it comes to recruiting digital technology teachers, or providing opportunities for ākonga to experience specialist computing science areas … such as cyber security." – Director of Research and Policy, Netsafe, New Zealand*

Some of the countries only offer cyber security education at a pre-university level as extra-curricular to the curriculum, in particular content not focusing on online safety. There were expressed wishes on embedding such more technical cyber security content into the national curriculum in the future given its importance.

Finally, because of the **impact of and heavy reliance on immigration** among some of the countries in this section, it is crucial to understand the socio-cultural context. Not everyone that ends up working in cyber security in these countries, in particular Australia and New Zealand, will have grown up in those respective countries, and therefore will have accessed other counties' cyber security educational content, including at pre-university level. This suggests that it is essential to consider within a global context, echoing the focus of this report.

> *"New Zealand draws on inward immigration to the country for jobs where there are skill shortages, those become priorities within the immigration system. It's similar to the Australian and recent UK points-based system. So, …, that can draw in people from all around the world who have desirable skill sets where the need can't necessarily be met by home-grown talent." – Director of Research and Policy, Netsafe, New Zealand*

5.6. Summary

Between the five countries in this section, a variety of approaches to pre-university cyber security education can be observed, with Singapore taking more of a government-led approach, whereas New Zealand rely on Netsafe to support the dissemination of online safety teaching. There is also a diversity in the socio-cultural contexts of each country, which impacts the access to, and uptake of cyber security educational provision at a pre-university level, including the culture of after school clubs and whether cyber security is embedded into the

school curriculum. Also of note in this section is the difference in the number of initiatives across the countries, with the US having eleven alone, and the range for the other countries being between four and seven. Echoing findings from the UK, diversity is aimed for in the workforce, particularly aimed at women in this sample. The fragmentation of provision and lack of clarity is also echoed from the UK findings, further impacted by teacher choice and location and size of schools. We cannot say if unitary countries experience more or less fragmentation than federated countries, however there does appear to be a move towards federated countries adopting country-wide frameworks which cover all of the states within that country, in addition to individual states' own frameworks.

6. Estonia, Greece, Mexico, the Netherlands, Norway, Portugal, South Africa

This section will explore pre-university cyber security and online safety education in the following countries within our groups 2 and 3: **Estonia**, **Greece**, **Mexico**, the **Netherlands**, **Norway**, **Portugal**, and **South Africa**. They cover three continents: Europe, Latin America and Africa. Each country will be explored though five perspectives or landscapes as stated in Sections 4 and 5: stakeholder landscape, educational landscape, policy landscape, implementation landscape, and socio-cultural landscape. Each subsection will be supported by excerpts from interviews undertaken with stakeholders from each country.

It is important to note that not all documentation may be available in English for the countries in this section, and where documentation is not available in English, it may not have been included. Although this may limit some of what we present, we acknowledge this and leave this for our future work.

6.1. Stakeholder landscape

Some of the countries in this section have fewer stakeholders involved, due to the underdeveloped nature of their pre-university cyber security education provision. Some documentation was also not available in English, which also made tracing all stakeholders even more complex. Therefore, we have provided an outline of stakeholders involved in the countries in this section.

One key stakeholder in each of the countries in this section, appears to be **governments or government departments** who are responsible for national cyber security strategies or similar **policy** (where there is one), and **national cyber security centres** (where they exist). Cyber security strategies will set priorities, which may include a focus on pre-university cyber security education, and examples of these are given in Table 30.

Table 30: Governments, government departments and cyber security centres who are stakeholders in pre-university cyber security education in the countries in Section 6

Country	Governmental bodies and national cyber security centres
Estonia	**Ministry of Economic Affairs and Communications**; **Estonian Defense League's Cyber Unit**
Greece	**National Cybersecurity Authority**
Mexico	**Gobierno de México** (**Federal Government of Mexico**)
The Netherlands	**Government of the Netherlands**; **National Cyber**; **National Cybersecurity Centre** (**NCSC-NL**)
Norway	**Norwegian Ministry of Justice and Public Security**; **National Cyber Security Centre**; **Ministry of Defence**
Portugal	**Centro Nacional de Cibersegurança** (**CNCS**) (**Portuguese National Cybersecurity Centre**)
South Africa	**State Security Agency**

As can be observed above, some countries have multiple stakeholders in this domain (e.g., Norway), whereas others have only one stakeholder (e.g., Mexico). National cyber security centres have been added to this section to reflect that they are in some cases, the named organisation publishing a country's national cyber security strategy, (e.g., the Netherlands).

National cyber security centres may also be important stakeholders in the implementation of pre-university cyber security education too. In this case, they will be repeated later in this subsection to reflect their dual role.

In addition to government departments which are responsible for policy, **governments** and **government departments** are also important stakeholders in the organisation of a country's **education system** and national curriculum (where one exists). In the case of Greece and Mexico, these departments are also responsible for school textbooks which are used by pupils. Table 31 outlines the stakeholders in each respective country who are responsible for education systems, curricula and resources (in the case of Greece and Mexico).

Table 31: Governments and government departments regarding educational matters who are stakeholders in pre-university cyber security education in the countries in Section 6

Country	Bodies responsible for educational matters at governmental level
Estonia	**Ministry of Education**
Greece	**Ministry of Education, Research and Religion**
Mexico	**Secretaria de Educacíon Pública**
The Netherlands	**Government of the Netherlands; Ministry of Education, Culture and Science**
Norway	**Norwegian Ministry of Education and Research**
Portugal	**Direção-geral da educação**
South Africa	**Department of Basic Education**

In addition to any content implemented into curricula and frameworks in the seven countries, other stakeholders either supplement, provide support for teachers, or have their own provision of pre-university cyber security education. Table 32 gives a brief overview of stakeholders who provide initiatives or actions for pre-university cyber security education in the countries in this section.

Table 32: Stakeholders providing actions or initiatives in the countries in Section 6

Country	Stakeholders providing initiatives or actions
Estonia	**Chancellor of Justice; Ministry of Defense; Safer Internet Centre**
Greece	**Cyber Crime Unit of the Hellenic Police; Ministry of Citizen Protection; Safer Internet Centre**
Mexico	None found
The Netherlands	**Kennis.net; Safer Internet Centre**
Norway	**Norwegian Ombudsperson for Children; Safer Internet Centre**
Portugal	**Centro Nacional de Cibersegurança; Department of Administrative Modernization; Department of Science, Technology and Higher Education; Department of Education; Department of Labor; Department of Planning and Infrastructure; Department of Economy; Safer Internet Centre**
South Africa	**Department of Telecommunications and Postal Services; Cybersecurity Hub; University of South Africa**

As can be observed above, there are a variety **of government departments, units or figures**, **companies** and other educational establishments (e.g., **universities**), along with **Safer Internet Centres**. **Safer Internet Centres** were found in six of the seven countries in this section (see Section 6.4.2.) with provision for children, young people, parents and teachers across the

countries in this section. Another key figure in the provision of pre-university cyber security education are **children's commissioners**, with only Estonia (Chancellor of Justice) and Norway (Norwegian Ombudsperson for Children) having a children's commissioner or an equivalent figurehead. This is in contrast to Sections 4 and 5, where all countries in Section 4, and two of the countries in Section 5 had a children's commissioner.

Each of the six countries where stakeholders were found to provide initiatives or actions had a stakeholder who were from a governmental department or unit (e.g., **Cyber Crime Unit of the Hellenic Police** in Greece). Where a governmental department or unit (including national cyber security centres) did not provide initiatives or actions, other stakeholders filled the gap. This can notably be seen in South Africa, with the **University of South Africa**. The tables in this subsection show some significant differences among countries covered in this section, with some countries having more stakeholders than others (e.g., Mexico with two, Portugal with seven and the Netherlands with six). These differences across the countries demonstrate the **idiosyncrasy** of approach and responsibility, with each country having different stakeholders in charge of actions and initiatives.

There appears to be **no uniform approach** to how the stakeholders interact with each other across the countries in this section; each country has a different landscape in regards to stakeholder interaction. However, cyber security education for children and young people is not one individual's responsibility alone:

> *"And we need all governments … they can't do it alone, …, you need private sector, you need academia, you need all the stakeholders to develop a cyber security plan in general. And from there and you have to work together with other stakeholders to get this, not only education or public education, but to accomplish, to change the curriculum at schools … to get conferences or to get programmes that can help kids, teachers and parents to learn about cyber security and all." – Specialist Professor in Digital Law and Cybersecurity, Mexico*

This reiterates how crucial it is that different stakeholders are aware of each other, and are aware of the unique responsibilities they each hold in this context.

Parents (including legal guardians and carers) and **teachers** remain important stakeholders for the countries in this section. In particular in Mexico, it was found that parents can steer the level and content of pre-university cyber security education in schools:

> *"All these efforts on that programme? But over out of their private schools, maybe we can have these talks, but all like a response or an emergent response to the situation of all platforms … but I don't think public schools have [such things]." – Specialist Professor in Digital Law and Cybersecurity, Mexico*

This iterates parents and carers as important stakeholders, particularly in certain contexts where there may be fewer other stakeholders to steer to the direction and content of pre-university cyber security education.

6.2. Policy landscape

The policy landscape varies across each of the countries in this section, with the application of policy in regards to pre-university cyber security education impacted by the nature of the government in each country. Using the same definitions for unitary and federated as in Section 5.2, Table 33 gives and overview of the types of government in each country covered in this section.

Table 33: Types of governments of countries covered in Section 6

Country	Federal or unitary state?
Estonia	Unitary
Greece	Unitary
Mexico	Federal
The Netherlands	Unitary
Norway	Unitary
South Africa	Unitary

As can be seen, the majority of countries within this section are unitary countries, with the exception of Mexico.

6.2.1. Cyber security strategies

Each of the countries in this section have a cyber security strategy, mentioning cyber security education at pre-university level to varying degrees.

Estonia's ***Cybersecurity Strategy 2019–2022*** (Ministry of Economic Affairs and Communications (Estonia), 2019), published by the Ministry of Economic Affairs and Communications describes one of the key objectives as 'a cyber literate society and ensures sufficient and forward-looking talent supply'. This includes raising awareness among the general population (which includes children and young people, but does not target them directly). Targeted work will also be undertaken with pupils and teachers, with pupils' and teachers' knowledge being measured, along with training in cyber security for schools. The importance of targeting pupils at a pre-university level is recognised in this strategy from Estonia, and the vital role of teachers is highlighted within the nationwide shortage of specialist teachers. The training mentioned in this strategy seeks to move dissemination of information from a project based model, to a model integrated as part of the broader education system in Estonia. This is not the first cyber security strategy, with Estonia having two previous cyber security strategies in the periods of 2008-2013, and 2014-2017.

In **Greece**, the ***National Cyber Security Strategy 2020-2025*** (NCSA (Greece), 2020) was released in 2020, by **National Cybersecurity Authority** (**NCSA**), which is part of the **Ministry of Digital Governance**. The strategy evolved from the older ***National Cyber Security Strategy*** (Version 3.0) released in 2017 (Ministry of Digital Governance (Greece), 2018). According to the Strategy, one of the key critical goals is the capacity building, which includes the increase cyber security awareness of ICT users (citizens) and strengthening relevant training and educational programmes (NCSA (Greece), 2020, p20-22). The responsibility for enacting actions from the Strategy sits with the NCSA, but for the above goal some other stakeholders are involved such as the Ministry of Education (NCSA (Greece), 2020, p29-30). '***Citizen Awareness***' is a key action of the strategy, including targeting children and young people at a pre-university level. Education targeting children and young people at ISCED levels 1-4 is mentioned, with the **Ministry of Education** outlined as responsible for campaigns. Further educational activities are suggested with collaboration from higher education providers.

The **Mexican** ***Cyber Security Strategy*** (Gobierno de México, 2017) is the first cyber security strategy for Mexico. Cyber security culture (including awareness) is one of the pillars for action, however, children and young people are not mentioned. A future action that could have relevance to pre-university cyber security education is capacity building, but this action contains no mention of children or young people or school settings, either.

The **National Cyber Security Centre** in **the Netherlands** (NCSC-NL), part of the Dutch Ministry of Justice and Security, implements the ***National Cybersecurity Agenda*** (**NCSA**) of the Netherlands (NCSC-NL, 2018), which was announced in 2018. One of the key pillars mentioned in this strategy is that of cyber security knowledge; '*the Netherlands leads the way in the field of cyber security knowledge development*' (NCSC-NL, 2021). Within this pillar, there was a revision of the curriculum for primary and secondary curriculums for digital literacy to be a theme. Proposals for this were due to start from 2018 onwards, however interviews from the Netherlands indicate that the process may have taken longer and been slower than expected:

> *"The main challenge right now is the political one. We have more or less a crisis here in this country on a political level, and that slows the development of … the curriculum. So that challenge is what has to be met first of all." – Strategic advisor digital literacy: ethics, Kennisnet, the Netherlands*

This may have impacted outcomes in regards to this pillar on the strategy, and therefore only be mentioned in policy rather than have any tangible initiatives or curriculum documents to supplement this.

The ***National Cyber Security Strategy*** **for Norway** is Norway's 4th cyber security strategy to date, since the first such strategy introduced in 2003 (Norwegian Ministries, 2019). The strategic goal 'competence' includes actions relevant to cyber security education: "*Pupils and apprentices have digital skills, including competence in secure use and security, that enable them to experience life skills and to succeed in further education, working life and participation in society*" (ibid, p17).

The majority of actions at this level appear to be targeting university level education and higher (ISCED levels 5 and above), with specific mention given to undergraduate and postgraduate study, and apprenticeships.

South Africa's ***National Cybersecurity Policy Framework*** (NCPF), published by its **State Security Agency**, has some relevant guidance including cyber security education, notably the need to create an environment which is enabling for cyber security education (State Security Agency (South Africa), 2015, p13) and promoting and providing guidance "*to the process of the development and implementation of need to create an environment which is enabling for cyber security education*" (State Security Agency (South Africa), 2015, p16).

6.2.2. Other strategies complementary to cyber security education

Ministry of Digital Governance of **Greece** defined a Digital Transformation Strategy 2020-2025 (Māra Jākobsone, 2021; Ministry of Digital Governance (Greece), nd)[7]. One of its primary objectives is '*Development of digital skills for all citizens*', which highlights a number of goals with an explicit mention of or direct relevancy for pre-university education:

- "*Enhancing the integration of innovative technologies in the educational process of primary and secondary education.*"
- "*Institutionalisation of weekly information technology (IT) hours in all classes of secondary education.*"

[7] Since none of the authors of the report can read Greek, we used a third-party English summary (Māra Jākobsone, 2021) to inform our understanding of Greece's Digital Transformation Strategy 2020-2025 whose official version can be found at (Ministry of Digital Governance (Greece), nd). The quotations included in this report are extracted from (Māra Jākobsone, 2021).

- *"Launching training programmes for all ages, social backgrounds and professionals from a variety of sectors via a lifelong learning approach."*

Pre-university education is also mentioned as part of 'Upskilling goals' of the 'Digital Skills Pillar':

- Under '*Goal #1 Digital Investment in the Human Resources of the Country*':
  - *"Fostering and developing digital skills of pupils, students and teachers across educational levels."*
- Under '*Goal #2 Citizens' Digital Academy – the national portal for digital capabilities in Greece*':
  - *"Increasing the availability and accessibility of education and training programmes for the acquisition of digital skills in the context of the entire Greek population – at basic, intermediate and advanced level."*
  - *"Offering a variety of educational programmes both online (through modern and asynchronous education) and in face-to-face."*
  - *"Creating a 'Collaboration Platform' to act as the central hub for cooperation between public and private digital education providers."*

Although digital skills are broader than cyber security and online safety, they no doubt will cover some part of the latter.

In **Norway**'s '***National strategy for digital security competence***' (Norwegian Ministries, 2019) the main goal of this strategy is to improve cyber security capacity and competences in society to reflect the current need and demand. This strategy is not targeting pre-university level education, and appears to be more focused on businesses and the general population.

6.3. Educational landscape

Education in each of the countries included in this section operates through slightly different systems, much like the diversity we have shown so far in the previous two sections. Each education system from each country will be taken in turn for closer examination.

6.3.1. Estonia

In **Estonia**, education is broken down to basic education, and general secondary education. Both of these need to be passed in order for pupils to be considered for Higher Education. Table 34 gives an overview of the stages of education in Estonia.

Table 34: Stages of pre-university education in Estonia (Estonian Ministry of Education and Research, 2020)

School attended	Stage of education	ISCED level (age)
Basic school	Stage I	ISCED level 1 (ages 6-9)
	Stage II	ISCED level 1 (ages 9-11)
	Stage III	ISCED level 2 (ages 11-14)
Secondary school	General secondary education	ISCED level 3 (ages 14-17)

Estonia does have a national curriculum, and as part of this there is content relevant to cyber security education within the curriculum. For ages 6-14, the topics covered coding,

multimedia, and cyber hygiene (Lorenz, 2021), with the topic having differing names at differing educational stages – '***Digital Safety***' for ages 6 and 9, '***Digital Hygiene***' for ages 9-11 and '***Cyber Hygiene***' for ages 11-14. Table 35 shows some of the key content covered in the Estonian curriculum.

Table 35: Key content covered in the Estonian national curriculum

Stage of education	ISCED level (age)	Curriculum includes (Lorenz, 2021)
Stage I	ISCED level 1 (ages 6-9)	Difference between online and offline worlds What makes a good password Why to follow privacy regulations Differences between free and paid services Where to get help and support Knows how to avoid and manage health risks Basic problem solving
Stage II	ISCED level 1 (ages 9-11)	Knows how to behave online Recognising fake news Knows how to protect their digital identity and devices Explains and avoids health risks Solving basic technological problems
Stage III	ISCED level 2 (ages 11-14)	Can demonstrate a software lock and how to bypass it Understands policies, regulations and the law in regards to digital technology Understands how technology changes life Can create a security audit of their home Uses correct cyber security terminology Can foresee future threats

The key content shown in the table above and what two interviewers told us seem to suggest that the national curriculum focuses more on online safety than other (more technical) specific cyber security topics:

> *"… in our national curriculum, we have digital competences, which is where there are eight competencies, digital competence is one of them, and in curricula it's written like really short descriptions … But next to it, we have digital competencies model, which is based on … DigComp [https://ec.europa.eu/jrc/en/digcomp]. And under that, there is one topic [which] is digital safety. So it's something that all the teachers should cover in their lessons, more or less so that it's integrated in their lessons and integrated on the topics they are covering." – Curriculum Specialist, Ministry of Education and Research, Estonia*

> *"But the problem between that is just the teachers that their education is still digital safety, not cyber security. And therefore we don't have informatics teachers and we don't have all of that cyber security teachers. So this part, this is lacking in Estonia." – Researcher at Tallinn University of Technology, School of Information Technologies, Department of Software Science and Development manager (IT) at Pelgulinna Gymnasium, Estonia*

There is also currently no curriculum for pupils aged 14-17 in regards to cyber security and online safety education, although there is an awareness of how much of the provision is extra-curricular in Estonia:

> *"So we have developed the syllabus for one sixth grade and then we have materials. And this is focused more in digital safety. Then we have a kind of a syllabus seven to nine graders, but it has*

not been implemented. Therefore, in that age group, there is nothing going on. And then we have a cyber security curriculum developed by the Ministry of Defence and NATO's some organisation, and it has been implemented 2017. And we have a material as well. So we have a workbook there. And otherwise, everything is extra-curricular activities." – Researcher at Tallinn University of Technology, School of Information Technologies, Department of Software Science and Development manager (IT) at Pelgulinna Gymnasium, Estonia

Therefore, there is recognition of where there are gaps in provision and an awareness of to what degree cyber security is part of the national curriculum, and where it forms part of extra-curricular activities.

6.3.2. Greece

In **Greece**, education is compulsory between the ages of 4 and 15 years (ISCED levels 0-2), with education between the ages of 15 and 18 (ISCED level 3) as optional. Table 36 gives an outline of the stages of education in the Greek school system.

Table 36: Stages of pre-university educations in Greece

Stage of education	ISCED level (age)	Compulsory?
Pre-school (2 stages): stage 1(Προνηπιαγωγείο); stage 2 Nipiagogeio (Νηπιαγωγείο)	ISCED level 0 (ages 4-6)	Yes
Primary school, *Dimotiko sxoleio* (Δημοτικό σχολείο,)	ISCED level 1 (ages 6-12)	Yes
Junior High school, *Gimnasio (*Γυμνάσιο)	ISCED level 2 (ages 12-15)	Yes
High school, *Lykeio (*Λύκειο)	ISCED level 3 (ages 15-18)	No

ICT is part of the Greek National Curriculum. ICT is taught in junior high schools (all three years). School textbooks put together by the Institute of Educational Policy, so all pupils have access to the same school textbooks throughout Greek schools. The topics covered include: hardware, the Internet, careers using computing, programming and computing in society (Ministry of Education, Research and Religions, 2006). There appears to be no mention of cyber security or online safety in this textbook.

6.3.3. Mexico

In **Mexico**, education is mandatory between the ages of 6 and 18, with the main stakeholder in the oversight of schools being the Secretaría de Educación Pública (Secretariat of Public Education). Table 37 shows the age ranges in Mexico for each stage of education with the corresponding ISCED levels and age.

Table 37: Stages of pre-university education in Mexico

Stage of education	ISCED level (age)
Elementary school, *primaria*	ISCED level 1 (ages 6-12)
Junior high school, *secundaria*	ISCED level 2 (ages 12-15)
High School, preparatoria or bachillerato	ISCED level 3 (ages 15-18)

As can be seen above, there are two main streams of high school in Mexico: the *preparatoria* and the *bachillerato* (Wise.com, 2017). *Preparatoria* high schools in Mexico prepare students for higher education, therefore there tends to be some level of specialisation of subjects after having followed a general curriculum at the beginning of the *preparatoria. Bachillerato* high schools provide vocational training for skilled work in trades, or for roles like accounting. The **SEP Incorporated Preparatoria** uses a curriculum which is mandated and run by the government via the Secretariat of Public Education, whereas the **University Incorporated Preparatoria** is closely affiliated with a local university, who establishes the curriculum.

An examination of the curriculum and available textbooks for schools, children and young people found no textbooks or course material for computing related subjects or online safety related subjects (Gobierno de México, nd). This includes technology subjects, which computing related subjects may be part of.

> *"But the biggest problem is that we are not teaching. We are not preparing the teachers. So if the teacher doesn't know how to guide the kids, what is really going to be hard on parents [who] are not prepared." – Specialist Professor in Digital Law and Cybersecurity, Mexico*

6.3.4. The Netherlands

Education in **the Netherlands** starts at ISCED level 1 between ages 4-12, with all children in mainstream schools following the same curriculum. The Netherlands also exercises a stratified secondary school system. Table 38 illustrates the options available in regards to high school education in the Netherlands.

Table 38: Options available in high school education in the Netherlands

Type of school	Duration of study (years)	Aim/target
Preparatory vocational secondary education (VMBO)	4	Preparation for vocational training. Four pathways are available: the basic vocational pathway the advanced vocational pathway the combined pathway the theoretical pathway Pupils who complete the theoretical pathway may be able to transition to senior general education (HAVO) (European Commission, nd)
Senior general secondary education (HAVO)	5	Preparation for university studies (Government of the Netherlands, nd)
University preparatory education (VWO)	6	Preparation for university studies (Government of the Netherlands, nd)

HAVO and VWO pupils follow the same curriculum for the first three years. In years four and five of the HAVO and years four, five and six of the VWO, science and technology is a subject combination which is available (Government of the Netherlands, nd). The main difference between HAVO and VWO is that HAVO pupils take seven subjects, and VWO pupils take eight, and that HAVO prepares pupils for applied sciences universities, whereas VWO pupils are prepared for research universities. There is no national curriculum in the Netherlands, however there is a framework in which schools must perform, and school boards assist the governance of schools. In regards to cyber security and online safety, this means although this may be encouraged, implementation may be idiosyncratic:

"It's not mandatory, but all schools, all primary schools, they really feel the urge to talk about it. But again, it's quite ad hoc." – Strategic advisor digital literacy: ethics, Kennisnet, the Netherlands

"I think almost all schools are active, but on a voluntary basis, all schools, they make their own choices. We all look for clarity. So they want to do the right thing." – Strategic advisor digital literacy: ethics, Kennisnet, the Netherlands

This means that education on matters of cyber security and online safety may not be accessible to all pupils.

6.3.5. Norway

Education in **Norway** is composed of three stages, of which can be seen in the table below. School is compulsory between the ages of 6-16 years, and comprises the stages shown in Table 39.

Table 39: Stages of pre-university education in Norway

Type of school	ISCED level (age)
Primary school, *Barneskole*	1 (6-13 years)
Lower secondary school, *Ungdomsskole*	2 (13-16 years)
Upper secondary school, *Videregående skole*	3 (16-19 years)

In Norway, digital skills in a broad sense are embedded into subjects across the curriculum. Digital skills forms a part of the '***Framework of Basic Skills***' (2012) along with oral skills, reading, writing skills and numeracy. Each skill develops continuously throughout their educational journey, and are incorporated into all subjects (Utdanningsdirektoratet, nd). All teachers in all subjects have responsibility for the development of these basic skills, however some skills may be more emphasised in some subjects than others (ibid). Aspects of cyber security are added into digital skills, notably under the action 'digital judgement'. Table 40 shows an overview of the digital judgement thread of the basic digital skills.

Table 40: Digital judgment threat of the digital skills (Norwegian Ministry of Education and Research, 2012; Utdanningsdirektoratet, nd)

Level	Digital judgement
Level 1	*"Can follow basic rules for digital interaction. Knows basic rules for protection of personal privacy on the Internet."*
Level 2	*"Can apply basic netiquette and knows about rules for protection of personal integrity on the Internet."*
Level 3	*"Can apply netiquette and follow rules for protection of personal integrity on the Internet and in social media."*
Level 4	*"Can use the Internet and social media efficiently and appropriately."*
Level 5	*"Can reflect ethically on and assess the Internet and social media as a communications and information channel."*

The *'Framework for Basic Skills'* is covered at each age group of compulsory schooling. This has been reported to be a challenge for some teachers who perhaps teach subjects that could be perceived to be quite disconnected from digital judgement, and digital skills more broadly:

"All teachers in all subjects have to make sure they also teach the basic skills, including digital skills. Hereunder e-safety and cyber security." – Head of partnership and government relations, Norwegian Centre for Information Security, Norway

Embedding cyber security and online safety educational content into the curriculum in this manner ensures all pupils are exposed to some teaching on these topics.

6.3.6. *Portugal*

In **Portugal**, education operates in Ciclo (cycles), with each cycle referring to a different stage in a pupils' education. Table 41 gives an overview of the cycles and how they compare to ISCED levels and how long each cycle lasts. The table also marks where ICT teaching occurs in the national curriculum in Portugal (which was most recently updated in 2018).

Table 41: Stages of pre-university education in Portugal

Stage of education	ISCED level (age)
1º Ciclo / Escola Primária	ISCED level 1 (ages 5-9)
2º Ciclo*	ISCED level 1 (ages 9-11)
3º Ciclo*	ISCED level 2 (ages 11-14)
Ensino Secundário	ISCED level 2 (ages 14-17)

*where ICT is taught within the Portuguese national curriculum

The previous iteration of the Portuguese national curriculum (Direção-geral da educação, 2012) only taught ICT between the ages of 12-14, whereas the 2018 curriculum teaches ***ICT*** from age 10 through to age 15, covering the whole of Ciclo 2 and 3. This includes aspects of cyber security and online safety. Table 42 gives an overview of the content covered at each stage of the curriculum.

Table 42: Relevant cyber security content at each stage of the Portuguese national curriculum

Ciclo	ISCED level (age)	Relevant content
2º Ciclo	ISCED level 1 (ages 10-11)	understand copyright, understand the need for safe digital practices, have a thoughtful and respectful attitude (República Portuguesa Educação, 2018a, p6)
	ISCED level 1 (ages 11-12)	have a thoughtful and respectful attitude, understand safe digital practices on apps and the internet, know copyright rules, be aware of impact of ICT in day to day life (República Portuguesa Educação, 2018b, p6)
3º Ciclo	ISCED level 2 (ages 12-13)	critical, thoughtful and responsible attitude, know security mechanisms and different operating systems, know safe online behaviour and behave safely online, respect copyright rules, fake and spam messages – be able to identify, identify inappropriate use of video and images online (República Portuguesa Educação, 2018c, p6)
	ISCED level 2 (ages 13-14)	Critical, thoughtful and responsible attitude, *"Adopt safe practices for the use of digital applications and Internet browsing; Know and use validation criteria for information published online; Know and use the (related) standards with copyright, with intellectual property and with licensing) regarding the resources and content that it mobilizes in its works, fighting plagiarism;*

		Know and use the recommendations regarding accessibility, in the context of the creation and publication of digital content, even if in an elementary way; Know behaviours aimed at protecting privacy; *Adopt safe behaviours in the use of digital applications*" (República Portuguesa Educação, 2018d, p6)
	ISCED level 2 (ages 14-15)	*"Be aware of the impact of emerging technologies (for example: virtual reality, augmented reality and artificial intelligence) on society and in everyday life;* *Adopt safe practices of use of mobile devices (for example: access risks via public networks, installation of applications for mobile devices from credible sources and data collected during their use);* *Analyze criteria for selection and installation of applications on mobile devices;* *Know configuration features of mobile devices that constrain privacy (for example: geo-referencing, access to the device's camera and microphone);* *Know and use the standards related to copyright, intellectual property and licensing related to the use and creation of applications for mobile devices;* *Know and use the accessibility recommendations, the scope of creating applications for mobile devices, even if in an elementary way*" (República Portuguesa Educação, 2018e, p6)

6.3.7. South Africa

Education in **South Africa** starts at the age of 6 and is mandatory through to age 15 (Scholaro Pro, nd), with three further years of education to receive a school certificate. The school system is broken down further as shown in Table 43.

Table 43: Stages of pre-university education in South Africa

Stage of education	ISCED level (age)
Junior preparatory school	ISCED level 1 (ages 6-9)
Senior preparatory school	ISCED level 1 (ages 10-13)
High school / College	ISCED level 2 and 3 (ages 13-18)

Currently in the South Africa Curriculum, there is no cyber security education. This includes computing, of which is only available between the ages of 16 and 18 and is optional, and within the ***life skills curriculum***, which is taught at all ages (Department of Basic Education (South Africa), 2011a, 2011b, 2018). Informal information and resources exists for young people, but this content is not government mandated (e.g., see (Kritzinger, 2017) for Grades 4 and 6) covering cyber security, however this is only for primary school aged pupils .

> *"We understand the concept of why it (cyber safety education) is needed. We understand it is important and we understand very clearly that something must be done. There must be something (some kind of cyber safety initiatives) in place to assist schools and school learners to improve cyber safety awareness. But the physical implementation of it (cyber safety education) is a lacking." – Professor, University of South Africa, South Africa*

Further need for development in the provision of cyber security education at pre-university level has been recognised in this instance.

6.4. Implementation landscape

How educational initiatives and policies are implemented is idiosyncratic and dependent on many factors. As mentioned in Section 4.4, the **fragmentation** and **disconnected nature** of many initiatives is echoed in countries with multiple stakeholders, or where initiatives operate in silos and do not appear to be disseminated widely:

> *"I'd say [that] the children have a lot of training, but they're not so organised, maybe." – Cyber security research and development advisor, Department of National Cyber Security, Estonia*

> *"Africa (including South Africa) has a silo-based approach in my viewpoint. There are initiatives and there are politics and there is legislation related to cyber safety education, but each have a silo-based approach, and they're not speaking (linking) to one another." – Professor, University of South Africa, South Africa*

> *"There are quite a few resources and initiatives both for teachers and pupils, but they are not very holistic. The resources are developed by several different actors, both public and private, and they cover quite narrow themes." – Head of partnership and government relations, Norwegian Centre for Information Security, Norway*

In addition, it appears that many initiatives and cyber security education at pre-university education more broadly are not long lasting, or rely on the goodwill of teachers or other educators to share information and teach on cyber security or online safety:

> *"But … in many of the initiatives, is only focused on specific communities for a short time, so it is a one-off initiative." – Professor, University of South Africa, South Africa*

> *"But we still too much depend on goodwill and [are] dependent on growth of awareness and training programmes that are transversal to different subjects." – an interviewee (whose role and affiliation are anonymised per their request)*

Some of the countries covered in this section have external organisations (such as schools and colleges) deliver pre-university level cyber security education, demonstrating the multiplicity of stakeholders which are involved in cyber security education at this level:

> *"They're mostly delivered by organisations outside schools. And they are companies, but we also have very active libraries. So our public libraries are very active on this issue." – Strategic advisor digital literacy: ethics, Kennisnet, the Netherlands*

6.4.1. Government and national agency action and initiatives

As stated in Sections 4.4.1 and 5.4.1, children's commissioners can be important sources of information for online safety. Table 44 gives an overview of whether the countries covered in this section have a children's commissioner and any relevant work occurring in the realm of cyber security and online safety.

Table 44: Existence of a children's commissioner in countries covered in Section 6

Country	Children's Commissioner?	Any relevant work to cyber security and online safety
Estonia	Role played by the Chancellor of Justice (Chancellor of Justice (Estonia), nd)	Not relevant

Greece	One of the deputy ombudsman of Citizen's Advocate (Ombudsman) of Greece, Deputy Ombudsman for Children's Rights, plays the role of a children's commissioner in other countries (Greek Ombudsman, nd; Wikipedia, nd-c).	No work on pre-university cyber security or online safety education
Mexico	No	Not relevant
The Netherlands	Yes	No work on online safety or cyber security found (Netherlands' Ombudsman for Children, nd)
Norway	Yes	Yes – a report on *Young People's Thoughts on the Digital Environment* (2019), including recommendations on how to keep young people safe online (Norwegian Ombudsperson for Children, nd, 2019)
Portugal	Not for children but provision for children with a toll-free telephone line (Provedor de Justiça, nd)	Not relevant
South Africa	Only in Western Cape province (Abrahams, 2020; Western Cape Government, nd)	No work on online safety or cyber security found (Western Cape Government, nd)

We will now take each country covered in turn in regards to actions and initiatives of other governmental bodies and national agencies.

6.4.1.1 Estonia

Estonia has a variety of competitions available to children and young people, including ***CyberPin*** (for ages 6-11, connected to ***Safer Internet Day*** (***SID***)); ***CyberCracker*** (for ages 10-15; based on cyber security terminology; problem solving and attitudes towards safety); and ***CyberDrill*** (ages 13 and above, team-based CTF competition) (Lorenz, 2021). ***CyberSpike*** is also available for ages 14-25, which include ages 14-18 of the pre-university education level. CyberSpike is Estonia's preliminary for the ECSC, and CyberSpike contestants also get invited to a ***Cyber Camp*** (Lorenz, 2021). This wide variety of competitions in their cyber security offer provides various opportunities for children and young people to access pre-university extra-curricular cyber security education.

6.4.1.2 Greece

Greece's ***CyberKid***, which is run by the **Cyber Crime Unit of the Hellenic Police**, has online information accessible for children and young people of a variety of ages, including ages 6-10, ages 11-14, and ages 15-18 (Cyber Crime Unit of the Hellenic Police, nd-a, nd-b, nd-c). ***Information for parents*** is also provided (Cyber Crime Unit of the Hellenic Police, nd-d). ***Career guidance*** is available online for children and young people aged 15-18 who would like to know more about how to get into a career in cyber security and cyber crime, specifically in regards to the Cyber Crime Unit. Careers outside of the Cyber Crime Unit are not mentioned. A mobile app with the same name is also provided for easier access of the information from mobile devices, for all three main mobile OSs (Android, iOS and Windows Mobile) (Cyber Crime Unit of the Hellenic Police, nd-e).

CyberAlert is another online safety awareness programme run by the **Cyber Crime Unit of the Hellenic Police**, which is target at mainly businesses and consumers (Cyber Crime Unit of the Hellenic Police, nd-f). Although this programme is not directly on pre-university pupils or parents, its coverage on consumers should be able to reach at least young people closer to their adulthood (since they are often also young consumers). An important part of CyberAlert is ***FeelSafe***, a website and a mobile app (for Android and iOS) that help the general public and

businesses stay safe online (Cyber Crime Unit of the Hellenic Police, nd-g). FeelSafe is a joint effort between the Hellenic Police's Cyber Crime Unit and two other organisations in Greece: **Ministry of Citizen Protection**[8] and **Hellenic Confederation of Commerce and Entrepreneurship (ESEE)**[9].

Greece's **Ministry of Citizen Protection** provides ***online lectures via Zoom*** (and face to face prior to the COVID-19 pandemic) for the general public, including about online safety. 126 lectures in total have been given (Ministry of Citizen Protection (Greece), 2021).

The **National Digital Academy** is a newly established body in Greece, working on enhancing cyber security awareness, especially for parents, teachers, students and all citizens as it is open and free for the public (National Digital Academy (Greece), nd).

6.4.1.3 The Netherlands

The Netherlands promotes ***Safer Internet Day*** (***SID***) and ***Media Literacy Week*** to raise awareness of digital literacy, as part of their cyber security offer:

> *"We also have … Safer Internet Day in February that's also initiated by the Ministry of Economic Affairs with a lot of programmes as well. So we have surplus programmes on a national scale that is subsidised by the government and on. Schools are participating in that." – Strategic advisor digital literacy: ethics, Kennisnet, the Netherlands*

> *"We have a media literacy week every year in November, and it's called Media Literacy Week. It's funded and initiated by the Ministry of Education and in this media literacy weekly. It's money for primary education. We have about 150,000 pupils participating in the game media literacy game Media Masters. It's very successful." – Strategic advisor digital literacy: ethics, Kennisnet, the Netherlands*

However, given the nature of the education system within the Netherlands, such awareness events are likely to be opt-in ones for schools.

6.4.1.4 Portugal

The **CNCS** (**Centro Nacional de Cibersegurança**; **Portuguese National Cybersecurity Centre**) provides online courses on cyber security and cyber hygiene courses for the general population (CNCS, 2021a; PTSIC, nd-a, nd-b), and a CTF-style competition called ***Cyber Security Challenge (PT)***. **InCoDe.2030** is another Portuguese initiative which is supported by many government areas (e.g., Administrative Modernization; Science, Technology and Higher Education; Education; Labour; Planning and Infrastructure; and Economy), with the aim to strengthen Portugal's position in the European Commission's 2017 DESI (Digital Economy & Society Index) (FCT, nd). The initiative was launched in 2017, and appears to be targeting the

[8] The name of the ministry shown on CyberAlert's English web page for FeelSafe (Cyber Crime Unit of the Hellenic Police, nd-f) is '**Ministry of Interior and Administrative Reconstruction**'. This ministry went through a number of changes of its structure and name (Wikipedia, nd-d), and the part of this ministry in charge of CyberAlert become an independent ministry in 2018 under the name of '**Ministry of Citizen Protection**', which is the one managing public security services such as Hellenic Police (Wikipedia, nd-e). We feel it is more accurate to list Ministry of Citizen Protection as the ministry behind CyberAlert at present.

[9] ESEE's full name and acronym in Greek are **Εθνική Συνομοσπονδία Ελληνικού Εμπορίου** (**Ε.Σ.Ε.Ε.**). Their English name is shown as '**National Confederation of Greek Commerce**' on CyberAlert's English web page for FeelSafe (Cyber Crime Unit of the Hellenic Police, nd-f), but on its official website (ESEE, nd) the English name shown is '**Hellenic Confederation of Commerce and Entrepreneurship**'. We decided to use the latter.

general population and businesses, or pre-university cyber security education specifically. The focus appears to be on digital skills and digital citizenship (FCT, nd). Young people are one of the target groups for digital skills training through InCoDe.2030 (FCT, nd).

6.4.1.5 South Africa

South Africa's **Cybersecurity Hub** is mandated by the NCPF (Department of Telecommunications & Postal Services (South Africa), nd) and provides information through awareness of cyber security through campaigns, advice, posters and a '*schools project*'. The schools project includes workbooks for pupils, teachers and principals. The target audience in regards to pupils remains unclear as no target age group is given. The topics covered include digital footprint, online privacy, cyber risks and threats, cyber bullying, malware protection, password management, inappropriate content, and cyber scams (Cybersecurity Hub, 2020a).

The Cybersecurity Hub also has workbooks for pupils (Cybersecurity Hub, nd a) focused on online safety, and an accompanying teacher's guide and workbook which can be used in the classroom (Cybersecurity Hub, nd b). This is not part of the national curriculum in South Africa, so these materials are extra-curricular or for teachers to build into their lessons as they see fit. South Africa's **Film and Publications Board** (**FPB**) also run awareness campaigns in schools, however no mention is made of cyber security or online safety (2021).

6.4.2. Companies, charities and non-government organisations (NGOs)

In the context of the **EU**, ***Safer Internet Day*** (***SID***) is the 'flagship event' of the ***Better Internet for Children strategy*** (Safer Internet Day, 2021b). In a recent report, the importance of education by parents/carers and schools in regards to internet safety and cyber security was highlighted (Safer Internet Day, 2021a). The report recommends further input into spotting misleading content and ongoing conversations to help children and young people navigate the digital world. However, specific teaching goals are not mentioned.

Safer Internet Day is part of a wider global strategy, and not merely a UK-only initiative, with 170 countries having taken part in Safer Internet Day 2021 (European Commission, 2021). Safer Internet Day was started in 2004 and has been marked annually since (European Commission, 2021). In the UK, there were over 2.4 million views of films by Safer Internet Day and over 1.5 million downloads of educational resources (UK Safer Internet Centre, 2021a) and in Australia there were over 300,000 views of Safer Internet Day videos (eSafety Commissioner (Australia), nd-e).

In addition to the Safer Internet Day, **Safer Internet Centres** are another group of important add-ons to the cyber security and online safety pre-university educational provision. Safer Internet Centres exist across EU member states plus Iceland, Norway and the UK (Better Internet for Kids, nd-a). It appears that many of the centres are relatively active in their outreach activities (Better Internet for Kids, nd-b): they run the Safer Internet Day in their representing country, and provide online safety information for children and young people aged 3-19 (UK Safer Internet Centre, nd-a; nd-b). At the 2021 Safer Internet Day, some Safer Internet Centres partnered to create a ***Young People's Charter*** (UK Safer Internet Centre, 2021b), which includes cyber security and online safety education as one of the four elements.

In the following, we explain the more country-specific activities.

The **Portuguese Safer Internet Centre** (**PTSIC**; known as the **Centro Internet Segura** in Portuguese) has an awareness centre managed by the CNCS, which goes into schools and

holds awareness sessions, including some on online safety and privacy (Better Internet for Kids, nd-c; PTSIC, nd-a). The centre also provides teaching resources to help teachers (PTSIC, nd-b).

In **Estonia**, the **Safer Internet Centre** supports the various competitions and provides training for teachers:

> *"We have a project called Safer Internet Centre in Estonia. So it's the European project in safer and better internet for kids. This is just the Estonian branch, and they have done a lot of training via that programme." – Researcher at Tallinn University of Technology , School of Information Technologies, Department of Software Science and Development manager (IT) at Pelgulinna Gymnasium, Estonia*

In **Norway**, the **Safer Internet Centre** produces information and resources for parents and teachers, and helps increase the digital skills of children and young people (Better Internet for Kids, 2021).

In the Netherlands, online safety is more of a focus than cyber security, e.g., the **Dutch Safer Internet Centre** hosts a hotline for children and young people who are facing problems on the internet (Better Internet for Kids, 2020). Another Dutch organisation, **Kennisnet**, supports the implementation of ICT and digital literacy in all types of school (Kennisnet, nd-a). Information is readily available for school boards and teachers, including information on online learning (Kennisnet, nd-b); research and practice about teaching ICT and digital literacy (Kennisnet, nd-b, nd-c); and up to date research from Kennisnet on ICT education (Kennisnet, nd-d).

In **Greece**, the **Safer Internet Centre** also provides information relating to online safety more than cyber security, e.g., how to use YouTube videos (SaferInternet4Kids.gr, 2020). The Safer Internet Day is of particular importance in regards to cyber security and online safety pre-university education: webinars are run for the general public (SaferInternet4Kids.gr, nd), and schools are expected to take part in events as part of this day. A brochure was released to parents after the 2021 Safer Internet Day (SaferInternet4Kids.gr, 2021), describing the events and highlights of the day.

> *"All the recent years, there have been a wider number of children (students and pupils) and teachers engaged in Safer Internet Day. … more and more schools of the country are participating in this event." – Police General (ret) Hellenic Police and Expert in Cyber crime, Greece*

> *"… the schools have a chance to participate in the Safer Internet Day activities and actions, encouraging the efforts of the pupils to raise the cybersecurity awareness. If they succeed there is no space for cyber crime …" – Police General (ret) Hellenic Police and Expert in Cyber crime, Greece*

In **Mexico**, much of the extra-curricular activities which occur appear to be initiated by **parents**, in particular those who come from **higher socio-economic backgrounds**, and such initiatives appear not to be equally distributed, indicating an imbalance of access:

> *"All these efforts on that programme? But over out of their private schools, maybe we can have these talks, but all like a response or an emergent response to the situation of all platforms and but I don't think public schools have [such things]." – Specialist Professor in Digital Law and Cybersecurity, Mexico*

6.5. Socio-cultural landscape

Much like the socio-cultural landscapes in Sections 4 and 5, digital skills were seen as important and wanted by both pupils and teachers in school settings:

> *"People, the school teachers want, students want. … We have people who want to do the content and everything." – Researcher at Tallinn University of Technology , School of Information Technologies, Department of Software Science and Development manager (IT) at Pelgulinna Gymnasium, Estonia*

There appear to be some **barriers to changes** to curricula and the rolling out of further work to assist the pre-university cyber security education of children and young people. One of these barriers in some of the countries appears to be political, with changes to curricula held up by difficulties in government:

> *"The main challenge right now is the political one. We have more or less a crisis here in this country on a political level, and that slows the development of … the curriculum. So that challenge is what has to be met first of all." – Strategic advisor digital literacy: ethics, Kennisnet, the Netherlands*

Another way in which government issues can slow down policy and subsequent implementation of cyber security initiatives at pre-university level is **a lack of continuity of government**, with each government having different and new priorities, therefore not necessarily carrying on with initiatives which have begun. This appeared to be a significant issue for **Mexico** in particular:

> *"But with the change of administration, …, we don't have that continuity. That's one of the biggest problems we have in Latin America." – Specialist Professor in Digital Law and Cybersecurity, Mexico*

> *"… the government doesn't follow the strategy, the national strategy." – Specialist Professor in Digital Law and Cybersecurity, Mexico*

Funding of initiatives also seemed to impact the longevity and continuity of initiatives. One interviewee from **Estonia** in particular mentioned this in regards to their initiatives:

> *"People, the school teachers want, students want. There's no funds for that. At least we have asked, like for years. Nobody's giving. We have people who want to do the content and everything. … This is one thing and the other is that we are also working as a project based this year. Maybe the project ends, we may be done to get funding, then Estonia basically falls apart." – Researcher at Tallinn University of Technology , School of Information Technologies, Department of Software Science and Development manager (IT) at Pelgulinna Gymnasium, Estonia*

Governments may also have **other priorities** which are more important than pre-university cyber security education. For example, in **South Africa** the priority of building and implementing a cyber security curriculum, and implementing this across the country, is competing with priorities such as food shortages and gender-based violence:

> *"There're just too many other problems at the moment: human-related problems, gender-based violence, food shortages, lack of work and educational opportunities. So there're so many other human-related issues that cyber safety awareness is not even on many people's agenda. You cannot educate school learners regarding cyber safety awareness if they don't have food at school*

to eat. But … in many of the initiatives, is only focused on specific communities for a short time, so it is a one-off initiative." – Professor, University of South Africa

Those in these countries who are socio-economically more comfortable may also have more access to pre-university cyber security education, especially in school contexts. The **digital divide** also impacts access to pre-university cyber security education, with money again demonstrated to be a potential barrier to access:

"I know that private schools are doing this for. But I don't know if the federal secretariat made this effort." – Specialist Professor in Digital Law and Cybersecurity, Mexico

"The problem in South Africa is because of the digital divide. Some schools have the funding. The majority of the schools in South Africa do not have enough funding to include cyber safety education as an additional task or activity." – Professor, University of South Africa

At the other end of the spectrum, for countries that have established cyber security policies, it was also seen as important to tackle **lack of diversity**, echoing both Sections 4.5 and 5.5 with other countries in this report. Girls and women, much like in Section 5.5, were the target of diversity schemes and drives. Even in countries like **Estonia**, which reports having a lot of female students in computing-related subjects, further diversity was seen as desirable:

"Estonia's leading country and having a lot of the female IT students now in Europe, and this is good, but at the same time, is 25-30% enough? I don't think it's enough." – Researcher at Tallinn University of Technology, School of Information Technologies, Department of Software Science and Development manager (IT) at Pelgulinna Gymnasium, Estonia

These somewhat disparate and contrasting priorities in this group of countries illustrates the variety of socio-economic situations and socio-cultural contexts impacting the implementation of pre-university cyber security education.

6.6. Summary

Between the seven countries covered in this section, a variety of approaches to pre-university cyber security education can be observed, as with Sections 4 and 5. This demonstrates the diversity of pre-university cyber security education, not only among this group of countries but also in comparison to the countries covered in Sections 4 and 5 too. The socio-cultural contexts of each country in this section also differ, with some countries having implemented and established cyber security education at a pre-university level, either integrated across all subjects (e.g., Norway) or discretely as a separate subject (e.g., Estonia), and other countries not having widely implemented pre-university cyber security education, and potential barriers and other priorities impacting dissemination and action (e.g., Mexico, South Africa). The Safer Internet Centre across some of these countries seems to also take a variety of supportive forms, and Safer Internet Day is of variable importance in terms of raising awareness (e.g., in Greece this is very important whereas less so in Norway). We cannot say if unitary countries experience more or less fragmentation than federated countries among this sample, as only Mexico is a federated country, however it appears down to teacher choice in some countries (e.g., Portugal) as to how much cyber security or online safety is taught in the classroom.

7. Conclusions

In this final section, we summarise key findings from our research work in all three stages, including the results from the SLR in Stage 1. Based on the key findings, we make some recommendations to relevant stakeholders on what can be done to improve pre-university cyber security education in different countries and worldwide.

7.1. Key Findings

The key findings from our research can be summarised below:

- **Two main approaches to embedding cyber security and online safety content in the curriculum** were identified for countries covered in this report: content added as part of a technological subject area such as computing / computer science / ICT / (digital) technology, and content added to a range of non-technological subjects.
- For both approaches identified above, especially the first one related to more technological subjects, there tends to be **a lack of practical cyber security skills**, **a lack of security mindset** and **a lack of enough skill-set coverage built-in**, towards a cyber security related career path. For example, when programming is taught, critical thinking about cyber security (secure coding) is often not approached.
- There was a concern across the board regarding **lack of teacher training**, which led to **insufficient teacher skills** in delivering cyber security education with sufficient coverage (e.g., on important knowledge areas, the presence of external specialists, and practical and engaging opportunities). In addition, **teachers also struggled with finding enough time** to cover cyber security content in class.
- For many countries studied, **multiple stakeholders in different sectors** are active in different aspects of pre-university cyber security education, e.g., curricular and extracurricular activities, career awareness, and security/safety best practices. Such a presence of multiple stakeholders in cyber security education is encouraging. However, as a result, such activities are **often fragmented** and tended to **operate quite disjointly**. There is **confusion**, for example, about whose responsibility it is to ensure a certain **standard** of cyber security and online safety education, especially as some countries rely almost exclusively on outside organisations to deliver cyber security and safety content.
- **Economics has a direct impact** on pre-university cyber security education. Given limited resources, teaching more traditional subjects, including survival-focused skills, is often a higher priority than teaching cyber security skills.
- **Different levels of development/maturity of pre-university cyber security education** were identified among the countries studied:
    - Pre-university cyber security education is mature and explicitly embedded into a national curriculum which is mandatory (although there are countries which allow exceptions to this rule);
    - Pre-university cyber security education is dictated by a framework which is encouraged to be adopted across different states/provinces in a country with a federated government as a way to make it uniform and consistent;
    - Pre-university cyber security is embedded into citizenship/ethics education;
    - Pre-university cyber security education is recognised as a priority and is currently being designed;

- Pre-university cyber security education is not part of the country's priorities for development.

- **A top-down approach to curriculum design is the norm** adopted across countries studied, whether this is in the formal education sector or by extra-curricular bodies. Here, the term 'top-down' refers to activities driven by organisations at a higher level (e.g., relevant governmental bodies) rather than schools, teachers, parents and legal guardians and pupils, or employers who need more employees with relevant cyber security skills.
- In some countries studied, even where a national cyber security curriculum is in place, teachers and schools have a lot of control over what cyber security content they teach. This creates **freedom and autonomy for teachers**, but there are often concerns about a **lack of direction**.
- There is a **perceived general lack of interest and awareness among children** in developing cyber skills and of cyber security **as a potential career path**. One key problem indicated here is a **lack of diversity in terms of student enrolment in optional courses and training events**. It is still the case that such enrolment is dominated by white, male students in Western countries covered in our research. A key concern among many countries, particularly in the UK, is to increase student diversity in cyber security education in order to enhance the skills pipeline.

7.2. Main Recommendations

The following are main recommendations we would like to give to different stakeholders in pre-university cyber security education.

- For governments in countries and regions managing its own educational affairs: **setting up a national or regional steering body or working group with overall responsibility for cyber security and online safety education**, covering both pre-university stages and the higher education stage. Such a body or working group can help in the following areas:
  - decreasing fragmentation by coordinating efforts of different stakeholders across different sectors;
  - providing clarity on who is responsible for coordinating cyber security education in a given country;
  - maintaining a single central hub of resources for teachers and parents;
  - advising, organising or even providing up-to date teacher training in online safety and cyber security;
  - providing clear representation to work with other countries and regions to achieve a better international synergy in this space.
- For all stakeholders: **strengthening collaborations and communications between different sub-communities**, particularly those focusing on pre-university education, those on higher education, and those on cyber security profession. This will help ensure smooth transitions between pre-university education and higher education, and between higher education and CDP (continuing and professional development, or life-long education and learning). **Setting up a single community-wide body covering all stages of cyber security education** will help avoid gaps between different stages.
- For organisations setting school curricula and/or qualification standards: **embedding cyber security and online safety skills more widely across school curricula, qualification and exam specifications**. This will help accomplish two goals. First, it will enhance the skills of more pupils and raise awareness more widely throughout the curriculum, and

the overall cyber security skills and awareness of pupils more generally. Secondly, it will address the diversity issues currently plaguing cyber security education by bringing awareness and skills, and, importantly, the relevance of cyber security, to a wider audience, therefore enhancing the cyber security skills pipeline in a longer term.

- For all stakeholders: **making more efforts to attract more children and young people to cyber security education and a future career path**, especially from **less-covered and 'non-traditional' groups** (such as girls, ethnic minorities, and pupils from low income backgrounds). This will help create a more diverse knowledge and skills pipeline in different professions where cyber security plays a role (not just the more technical cyber security profession).
- For all stakeholders: **covering different aspects of cyber security and online safety education more systematically beyond pure technology-centric content**. The following **six broad aspects of content related to cyber security and digital literacy education** discussed in our SLR (Sağlam et al, 2021) can help as a systematic categorisation scheme of the different aspects: technological awareness, procedural awareness, data awareness, identity awareness, socio-cultural awareness, and consumer awareness.
- For organisations setting or participating in setting school curricula and/or qualification standards: **designing school curricula and qualification standards on cyber security and online safety by incorporating a more bottom-up (participatory) approach**, engaging with **a wider range of stakeholders**, including parents / legal guardians / carers, school teachers and staff, and employers with a need of cyber security workforce. For instance, regular surveys and opinion-seeking workshops can be organised with different stakeholders to collect opinions to help evolve school curricula and qualification standards in a more dynamic and targeted manner, and to align timing and order of content better. Employing a more bottom-up approach can help align school curricula and qualification standards with children's contemporary interests, concerns, and internet use, and needs of employers and society at large.
- For stakeholders conducting or funding cyber security, online safety and/or education-related research and innovation activities: **conducting and funding more research that can help inform policy makers and educators about how to better conduct pre-university cyber security and online safety educational activities**. This will help provide more solid scientific evidence and useful new tools to support relevant policies, school curricula, qualification standards, planning and evaluation of various activities. We recommend that such research and innovation activities should be conducted following **a participatory (co-creation) approach to engage with a wider range of stakeholders**, especially pupils, parents and legal guardians, school teachers and staff, who can then contribute actively throughout the process. Some examples of such research activities are given below:
    - a more comprehensive study on cyber security education in pre-university settings across the world, probably working with the ITU to engage national and state-level governments of all member states of the UN;
    - a review of cyber security education in both pre-university and higher education settings, and a mapping between them, in order to better understand how pupils are prepared for cyber security education at higher education institutions;
    - a more systematic evaluation (with a proper control group for scientific rigour) of the performance of existing educational activities in cyber security and online safety, in order to provide more solid evidence to relevant stakeholders to adjust policies, best practices and guidelines;

- systematic evaluation of existing cyber security and online safety educational solutions, methods, tools and procedures (e.g., educational games, CTF platforms, and pedagogical methods) in the pre-university setting;
- development of new cyber security and online safety educational solutions, methods, tools and procedures to enhance performance and to enrich options of end users; and
- research on how we can provide more effective cyber security and online safety education to people who are more vulnerable, e.g., those with learning disabilities or difficulties accessing digital resources.

- For solution providers and other stakeholders: **developing, encouraging, rewarding and adopting new innovative solutions to support cyber security and online safety educational activities**. Note that solution providers include not only industry, but also researchers, open-source developers (which may include some pupils, parents and teachers), teachers, research units of public bodies, NGOs, etc. We also recommend that the solution development and evaluation process involves **cross-sectoral collaboration** and **a participatory (co-creation) approach to engaging with end users**, which can ensure that any new solutions can truly meet the needs of end users and their performance be rigorously evaluated.

References

Abrahams, A., 2020, "A Children's Commissioner in every province is a game changer in the protection of children's rights". Retrieved from: https://www.da.org.za/2020/12/a-childrens-commissioner-in-every-province-is-a-game-changer-in-the-protection-of-childrens-rights (Accessed 6th January 2022)

ACARA (Australian Curriculum, Assessment and Reporting Authority), 2015, "Information and Communication Technology Capability learning continuum" [PDF]. Retrieved from: https://docs.acara.edu.au/resources/General_capabilities_-_ICT_-_learning_continuum.pdf (Accessed 5th January 2022)

ACARA, 2017, "Senior Secondary: Overview" [PDF]. Retrieved from: https://www.australiancurriculum.edu.au/media/3627/ss_info-sheet_overview.pdf (Accessed 5th January 2022)

ACARA, nd-a, "Foundation – Year 10 curriculum (Version 8.4)". Retrieved from: https://www.acara.edu.au/curriculum/foundation-year-10 (Accessed 6th January 2022)

ACARA, nd-b, "Senior secondary curriculum". Retrieved from: https://www.acara.edu.au/curriculum/senior-secondary (Accessed 6th January 2022)

ACARA, nd-c, "Online safety | The Australian Curriculum". Retrieved from: https://www.australiancurriculum.edu.au/resources/curriculum-connections/portfolios/online-safety/ (Accessed 6th January 2022)

ACARA, nd-d, "Review of the Australian Curriculum". Retrieved from: https://www.acara.edu.au/curriculum/curriculum-review (Accessed 6th January 2022)

ACM (Association for Computing Machinery), nd, "ACM Europe Council". Retrieved from: https://europe.acm.org/ (Accessed 5th January 2022)

ACSC (Australian Cyber Security Centre), nd-a, "About the ACSC". Retrieved from: https://www.cyber.gov.au/acsc (Accessed 5th January 2022)

ACSC, nd-b, "Family Resources". Retrieved from: https://www.cyber.gov.au/acsc/view-all-content/guidance/family-resources (Accessed 6th January 2022

ACSC, nd-c, "View all news – Individuals and families". Retrieved from: https://www.cyber.gov.au/acsc/view-all-content/news/individuals-and-families (Accessed 5th January 2022)

ACSC, nd-d, "View all programs". Retrieved from: https://www.cyber.gov.au/acsc/view-all-content/programs (Accessed 6th January 2022)

ACT (Association for Citizenship Teaching, UK), nd, "Media Literacy teaching resources". Retrieved from: https://www.teachingcitizenship.org.uk/resource/media-literacy-teaching-resources (Accessed 7th February 2022)

AFA (Air Force Association, US), 2017, "Cyber Education Literature Series: Sarah the Cyber Hero". Retrieved from: https://www.uscyberpatriot.org/Pages/Announcements/Sarah-the-Cyber-Hero.aspx (Accessed 28th December 2021)

AFA, nd-a, "What is CyberPatriot?". Retrieved from: https://www.uscyberpatriot.org/Pages/About/What-is-CyberPatriot.aspx (Accessed 5th January 2022)

AFA, nd-b, "AFA CyberCamp Overview". Retrieved from: https://www.uscyberpatriot.org/Pages/Special%20Initiatives/AFA%20CyberCamp%20Overview.aspx (Accessed 5th January 2022)

AFA, nd-c, "Sarah the Cyber Hero". Retrieved from: https://www.uscyberpatriot.org/Pages/Special%20Initiatives/Sarah-the-Cyber-Hero.aspx (Accessed 5th January 2022)

AMCA (Australian Communications and Media Authority), 2021, "Online misinformation". Retrieved from: https://www.acma.gov.au/online-misinformation (Accessed 6th January 2022)

AQA (Assessment and Qualifications Alliance), 2019, "AS and A-Level Computer Science, AS (7516) A-level (7517)" [PDF]. Retrieved from: https://filestore.aqa.org.uk/resources/computing/specifications/AQA-7516-7517-SP-2015.PDF (Accessed 5th January 2022)

AQA, 2020, "GCSE Computer Science (8520)" [PDF]. Retrieved from: https://filestore.aqa.org.uk/resources/computing/specifications/AQA-8520-SP-2016.PDF (Accessed 5th January 2022)

Australian Curriculum, nd-a, "Learning areas (Version 8.4)". Retrieved from: https://www.australiancurriculum.edu.au/f-10-curriculum/learning-areas/ (Accessed 6th January 2022)

Australian Curriculum, nd-b, "Digital Technologies". Retrieved from: https://www.australiancurriculum.edu.au/f-10-curriculum/technologies/digital-technologies/?year=12983&year=12984&year=12985&year=12986&year=12987&strand=Digital+Technologies+Knowledge+and+Understanding&strand=Digital+Technologies+Processes+and+Production+Skills&capability=ignore&capability=Literacy&capability=Numeracy&capability=Information+and+Communication+Technology+%28ICT%29+Capability&capability=Critical+and+Creative+Thinking&capability=Personal+and+Social+Capability&capability=Ethical+Understanding&capability=Intercultural+Understanding&priority=ignore&priority=Aboriginal+and+Torres+Strait+Islander+Histories+and+Cultures&priority=Asia+and+Australia%E2%80%99s+Engagement+with+Asia&priority=Sustainability&elaborations=true&elaborations=false&scotterms=false&isFirstPageLoad=false (Accessed 6th January 2022)

Australian Curriculum, nd-c, "Information and Communication Technology (ICT) Capability (Version 8.4)". Retrieved from: https://www.australiancurriculum.edu.au/f-10-curriculum/general-capabilities/information-and-communication-technology-ict-capability/ (Accessed 5th January 2022)

Australian Curriculum, nd-d, "Curriculum connections". Retrieved from: http://australiancurriculum.edu.au/resources/curriculum-connections/ (Accessed 5th January 2022)

Barefoot Computing, nd-a, "Supporting primary school teaching | Barefoot Computing". Retrieved from: https://www.barefootcomputing.org/ (Accessed 6th January 2022)

Barefoot Computing, nd-b, "Cyber | EN | Barefoot Computing". Retrieved from: https://www.barefootcomputing.org/cyber (Accessed 6th January 2022)

Barefoot Computing, nd-c, "Barefoot Computing primary classroom resources". Retrieved from: https://www.barefootcomputing.org/primary-computing-resources (Accessed 6th January 2022)

Barefoot Computing, nd-d, "Barefoot Computing primary teacher resources". Retrieved from: https://www.barefootcomputing.org/concepts-and-approaches (Accessed 6th January 2022)

BBC, 2021, "State of the Nations". Retrieved from: https://www.bbc.co.uk/programmes/b087b9qx (Accessed 12th December 2021)

Better Internet for Kids, 2020, "Dutch Safer Internet Centre". Retrieved from: https://www.betterinternetforkids.eu/en-GB/sic/netherlands (Accessed 6th January 2022)

Better Internet for Kids, 2021, "Norwegian Safer Internet Centre". Retrieved from: https://www.betterinternetforkids.eu/en-GB/sic/Norway (Accessed 6th January 2022)

Better Internet for Kids, nd-a, "Insafe and INHOPE". Retrieved from: https://www.betterinternetforkids.eu/policy/insafe-inhope (Accessed 6th January 2022)

Better Internet for Kids, nd-b, "Awareness". Retrieved from: https://www.betterinternetforkids.eu/en-GB/practice/awareness (Accessed 6th January 2022)

Better Internet for Kids, nd-c, "Portuguese Safer Internet Centre". Retrieved from: https://www.betterinternetforkids.eu/en-GB/sic/portugal (Accessed 6th January 2022)

Bonilla, S. and Paul, B., 2019, "Utah Computer Science Education Master Plan" [PDF]. Retrieved from: https://www.schools.utah.gov/file/abb4c31f-f599-4ec5-b57e-3a51404506ba (Accessed 5th January 2022)

British Columbia Ministry of Education, 2016a, "Area of Learning: Applied Design, Skills, and Technologies" [PDF]. Retrieved from: https://curriculum.gov.bc.ca/sites/curriculum.gov.bc.ca/files/curriculum/adst/en_adst_k-9_elab.pdf (Accessed 6th January 2022)

British Columbia Ministry of Education, 2016b, "Area of Learning: Physical and Health Education" [PDF]. Retrieved from:

https://curriculum.gov.bc.ca/sites/curriculum.gov.bc.ca/files/curriculum/physical-health-education/en_physical-health-education_k-9_elab.pdf (Accessed 6th January 2022)

British Columbia Ministry of Education, 2018a, "Area of Learning: APPLIED DESIGN, SKILLS, AND TECHNOLOGIES — Computer Studies Grade 10". Retrieved from: https://curriculum.gov.bc.ca/sites/curriculum.gov.bc.ca/files/curriculum/adst/en_adst_10_computer-studies.pdf (Accessed 6th January 2022)

British Columbia Ministry of Education, 2018b, "Area of Learning: APPLIED DESIGN, SKILLS, AND TECHNOLOGIES — Computer Information Systems Grade 11". Retrieved from: https://curriculum.gov.bc.ca/sites/curriculum.gov.bc.ca/files/curriculum/adst/en_adst_11_computer-information-systems.pdf (Accessed 6th January 2022)

British Columbia Ministry of Education, 2018c, "Area of Learning: APPLIED DESIGN, SKILLS, AND TECHNOLOGIES — Computer Programming Grade 11". Retrieved from: https://curriculum.gov.bc.ca/sites/curriculum.gov.bc.ca/files/curriculum/adst/en_adst_11_computer-programming.pdf (Accessed 6th January 2022)

British Columbia Ministry of Education, 2018d, "Area of Learning: APPLIED DESIGN, SKILLS, AND TECHNOLOGIES — Computer Information Systems Grade 12". Retrieved from: https://curriculum.gov.bc.ca/sites/curriculum.gov.bc.ca/files/curriculum/adst/en_adst_12_computer-information-systems.pdf (Accessed 6th January 2022)

British Columbia Ministry of Education, 2018e, "Area of Learning: APPLIED DESIGN, SKILLS, AND TECHNOLOGIES — Computer Programming Grade 12". Retrieved from: https://curriculum.gov.bc.ca/sites/curriculum.gov.bc.ca/files/curriculum/adst/en_adst_12_computer-programming.pdf (Accessed 6th January 2022)

British Columbia Ministry of Education, 2018f, "Area of Learning: PHYSICAL AND HEALTH EDUCATION Grade 10". Retrieved from: https://curriculum.gov.bc.ca/curriculum/physical-health-education/10/core (Accessed 6th January 2022)

Business Resilience Centre for the North East, nd, "Services". Retrieved from: https://www.nebrcentre.co.uk/services (Accessed 6th January 2022)

Cabinet Office (UK), 2021, "National Cyber Strategy 2022". Retrieved from: https://www.gov.uk/government/publications/national-cyber-strategy-2022/national-cyber-security-strategy-2022 (Accessed 25th December 2021)

California Department for Education, 2018, "Computer Science Standards". Retrieved from: https://www2.cde.ca.gov/cacs/cs (Accessed 6th January 2022)

California Department for Education, 2021, "Computer Science Education". Retrieved from: https://www.cde.ca.gov/be/st/ss/computerscicontentstds.asp (Accessed 6th January 2022)

California Department of Technology, 2021, "Cal-Secure: State of California Executive Branch Multi-Year Information Security Maturity Roadmap 2021" [PDF]. Retrieved from: https://cdt.ca.gov/wp-content/uploads/2021/10/Cybersecurity_Strategy_Plan_FINAL.pdf (Accessed 28th December 2021)

Cambridge Dictionary, 2022, "Country". Retrieved from: https://dictionary.cambridge.org/dictionary/english/country (Accessed 6th January 2022)

Canada Learning Code, 2020, "Learning in the Digital World: A Pan-Canadian K-12 Computer Science Education Framework" [PDF]. Retrieved from: https://k12csframework.ca/wp-content/uploads/Learning-for-the-Digital-Future_Framework_Final.pdf (Accessed 6th January 2022)

Canadian Centre for Cyber Security, 2020, "National Cyber Threat Assessment" [PDF]. Retrieved from: https://cyber.gc.ca/sites/default/files/publications/ncta-2020-e-web.pdf (Accessed 6th January 2022)

Canadian Centre for Cyber Security, 2021a, "Information & Guidance". Retrieved from: https://cyber.gc.ca/en/information-guidance (Accessed 6th January 2022)

Canadian Centre for Cyber Security, 2021b, "Learning Hub". Retrieved from: https://cyber.gc.ca/en/learning-hub (Accessed 6th January 2022)

Canadian Centre for Cyber Security, 2021c, "Academic Outreach and Engagement". Retrieved from: https://cyber.gc.ca/en/academic-outreach-and-engagement (Accessed 6th January 2022)

Canadian Centre for Cyber Security, 2021d, "Elementary and Highschool Resources". Retrieved from: https://cyber.gc.ca/en/guidance/elementary-and-highschool-resources (Accessed 6th January 2022)

Canadian Centre for Cyber Security, nd, "Cyber Security Events". Retrieved from: https://cyber.gc.ca/en/cyber-security-events (Accessed 6th January 2022)

CAS (Computing at School, UK), nd-a, "Computing at School (CAS) Home Page". Retrieved from: https://www.computingatschool.org.uk/ (Accessed 5th January 2022)

CAS, nd-b, "About CAS Communities". Retrieved from: https://www.computingatschool.org.uk/about-cas-communities (Accessed on 6th January 2022)

CCEA (Council for the Curriculum, Examinations and Assessment), 2007, "The Northern Ireland Curriculum: Primary" [PDF]. Retrieved from: http://www.nicurriculum.org.uk/docs/key_stages_1_and_2/northern_ireland_curriculum_primary.pdf (Accessed 5th January 2022)

CCEA, 2019a, "The Statutory Curriculum at Key Stage 3" [PDF]. Retrieved from: https://ccea.org.uk/downloads/docs/ccea-asset/Curriculum/The%20Statutory%20Curriculum%20at%20Key%20Stage%203.pdf (Accessed 5th January 2022)

CCEA, 2019b, "Guidance on Teaching, Learning and Assessment at Key Stage 4" [PDF]. Retrieved from:

https://ccea.org.uk/downloads/docs/ccea-asset/General/Guidance%20on%20Teaching%2C%20Learning%20and%20Assessment%20at%20Key%20Stage%204.pdf (Accessed 5th January 2022)

CCEA, 2019c, "CCEA GCSE Specification in Digital Technology" [PDF]. Retrieved from: https://ccea.org.uk/downloads/docs/Specifications/GCSE/GCSE%20Digital%20Technology%20%282017%29/GCSE%20Digital%20Technology%20%282017%29-specification-Standard_0.pdf (Accessed 5th January 2022)

CCEA, 2019d, "GCE Digital Technology" [PDF]. Retrieved from: https://ccea.org.uk/downloads/docs/Specifications/GCE/GCE%20Digital%20Technology%20%282016%29/GCE%20Digital%20Technology%20%282016%29-specification-Standard_1.pdf (Accessed 5th January 2022)

CCEA, nd-a "eSafety". Retrieved from: https://ccea.org.uk/legal/help/esafety (Accessed 5th January 2022)

CCEA, nd-b "Statutory Curriculum at Key Stage 3". Retrieved from: https://ccea.org.uk/learning-resources/statutory-curriculum-key-stage-3 (Accessed 5th January 2022)

CCEA, nd-c, "Curriculum | CCEA". Retrieved from: http://www.nicurriculum.org.uk/curriculum_microsite/pdmu/living_learning_together/home.asp (Accessed 5th January 2022)

CCSSO (Council of Chief State School Officers) and NGA Center (National Governors Association Center for Best Practices), nd, "Common Core State Standards Initiative". Retrieved from: http://www.corestandards.org/ (Accessed 6th January 2022)

CDN (College Development Network, Scotland, UK), nd, "The college landscape". Retrieved from: https://www.cdn.ac.uk/home/the-college-landscape/ (Accessed 13th January 2022)

CEOP (Child Exploitation and Online Protection Command, part of National Crime Agency, UK), nd, "Safety Centre". Retrieved from: https://www.ceop.police.uk/Safety-Centre/ (Accessed 6th January 2022)

CEPIS (Council of European Professional Informatics Societies), nd, "CEPIS - CEPIS". Retrieved from: https://www.cepis.org/ (Accessed 5th January 2022)

CERT NZ (National Computer Emergency Response Team New Zealand), nd, Get Cyber Smart. Retrieved from: https://www.cert.govt.nz/cybersmart/ (Accessed 20th January 2022)

Chancellor of Justice (Estonia), nd, "Protection of the rights of children and youth". Retrieved from: https://www.oiguskantsler.ee/en/protection-rights-children-and-youth (Accessed 6th January 2022)

Childline, nd, "Staying Safe Online". Retrieved from: https://www.childline.org.uk/info-advice/bullying-abuse-safety/online-mobile-safety/staying-safe-online/ (Accessed 6th January 2022))

Childnet International, nd-a, "Talking to young children about online safety". Retrieved from: https://www.childnet.com/teachers-and-professionals/hot-topics/talking-to-young-children-about-esafety (Accessed 6th January 2022)

Childnet International, nd-b, "Educators Pack for Online Safety Awareness". Retrieved from: https://www.childnet.com/resources/educators-pack-for-online-safety-awareness (Accessed 6th January 2022)

Childnet International, nd-c, "Digiduck Stories". Retrieved from: https://www.childnet.com/resources/digiduck-stories/ (Accessed 7th February 2022)

Childnet International, nd-d, "STAR SEND Toolkit". Retrieved from: https://www.childnet.com/resources/star-send-toolkit/ (Accessed 7th February 2022)

Childnet International, nd-e, "Childnet Digital Leaders Programme". Retrieved from: https://digital-leaders.childnet.com/ (Accessed 7th February 2022)

Children First Canada, 2020, "Children First Canada Welcomes Introduction of Bill in Senate of Canada Calling for Federal Commissioner for Children and Youth". Retrieved from: https://childrenfirstcanada.org/press-releases/children-first-canada-welcomes-introduction-of-bill-in-senate-of-canada-calling-for-federal-commissioner-for-children-and-youth/ (Accessed 6th January 2022)

Children's Commissioner (New Zealand), 2019, "Safer viewing online for children and young people" [PDF]. Retrieved from: https://www.occ.org.nz/assets/Uploads/Submission-from-Office-of-Childrens-Commissioner-on-classification-of-CVOD.pdf (Accessed 5th January 2022)

Children's Commissioner (New Zealand), nd, "Info4you". Retrieved from: https://www.occ.org.nz/4youth/info4you/ (Accessed 6th January 2022)

Children's Commissioner for England, nd, "Digital safety and wellbeing kit". Retrieved from: https://www.childrenscommissioner.gov.uk/coronavirus/digital-safety-and-wellbeing-kit/ (Accessed 6th January 2022)

Children's Commissioner for Wales, 2019, "Don't Worry, I'm here for you: Children's experiences of cyberbullying in Wales". Retrieved from: https://www.childcomwales.org.uk/dont-worry-im-here-for-you-childrens-experiences-of-cyberbullying-in-wales-3/ (Accessed 6th January 2022)

CISA, 2020, "Cybersecurity Education & Career Development". Retrieved from: https://www.cisa.gov/cybersecurity-education-career-development (Accessed 5th January 2022)

CISA (Cybersecurity and Infrastructure Security Agency, US), nd-a, "Homepage | CISA". Retrieved from: https://www.cisa.gov/ (Accessed 5th January 2022)

CISA, nd-b, “Cyber Essentials”. Retrieved from: https://www.cisa.gov/cyber-essentials (Accessed 5th January 2022)

CISA, nd-c, “Cyber Resource Hub”. Retrieved from: https://www.cisa.gov/cyber-resource-hub (Accessed 5th January 2022)

CISA, nd-d, “Cybersecurity Training and Exercises”. Retrieved from: https://www.cisa.gov/cybersecurity-training-exercises (Accessed 5th January 2022)

CISA, nd-e, “National Cyber Security Awareness Month”. Retrieved from: https://www.cisa.gov/cybersecurity-awareness-month (Accessed 5th January 2022)

CIS Ontario (Conference of Independent Schools of Ontario), 2021, “Online Learning with eLearning Consortium Canada (ELCC)”. Retrieved from: https://www.cisontario.ca/professional-learning/professional-learning-events/online-learning-with-elearning-consortium-canada (Accessed 6th January 2022)

CIVIX, nd, “CTRL-F: Find the Facts”. Retrieved from: https://ctrl-f.ca/en/ (Accessed 7th February 2022)

CNCS (Centro Nacional de Cibersegurança, Portugal; Portuguese National Cybersecurity Centre), 2021a, “e-learning courses”. Retrieved from: https://www.cncs.gov.pt/pt/cursos-e-learning/?persona=citizen (Accessed 6th January 2022)

CNCS, 2021b, “Capture the Flag”. Retrieved from: https://www.cncs.gov.pt/pt/capture-the-flag/?persona=citizen (Accessed 6th January 2022)

Coding Lab, 2020, “Schools in Singapore offering IB Computer Science, O-Level and A-Level Computing”. Retrieved from: https://www.codinglab.com.sg/schools-singapore-offering-ib-o-level-a-level-computing/ (Accessed 6th January 2022)

Colleges Scotland, nd, “Colleges In Scotland”. Retrieved from: https://collegesscotland.ac.uk/our-members/colleges-in-scotland (Accessed 13th January 2022)

Common Sense Media, nd-a, “Common Sense Media: Age-Based Media Reviews for Families”. Retrieved from: https://www.commonsensemedia.org/ (Accessed 5th January 2022)

Common Sense Media, nd-b, “Privacy and Internet Safety”. Retrieved from: https://www.commonsensemedia.org/privacy-and-internet-safety (Accessed 5th January 2022)

Computer Science For All, nd, “K-12 Curriculum”. Retrieved from: https://www.blueprint.cs4all.nyc/curriculum/ (Accessed 6th January 2022)

Computer Weekly, 2021, “NCSC offers teachers free cyber security training”. Retrieved from: https://www.computerweekly.com/news/252499637/NCSC-offers-teachers-free-cyber-security-training (Accessed 6th January 2022)

CSA Singapore (Cyber Security Agency of Singapore), 2016, "Singapore's Cybersecurity Strategy" [PDF]. Retrieved from: https://www.csa.gov.sg/news/publications/singapore-cybersecurity-strategy/~/media/0ecd8f671af2447890ec046409a62bc7.ashx (Accessed 6th January 2022)

CSA Singapore, 2019, "Cyber Safety Activity Books". Retrieved from: https://www.csa.gov.sg/News/Publications/Cyber-safety-activity-book (Accessed 6th January 2022)

CSA Singapore, 2020a, "Singapore's Safer Cyberspace Masterplan" [PDF]. Retrieved from: https://www.csa.gov.sg/-/media/Csa/Documents/Publications/Safer-Cyberspace-Masterplan-2020.pdf (Accessed 6th January 2022)

CSA Singapore, 2020b, "Cyber Safety Interactive Handbook" [PDF]. Retrieved from: https://www.csa.gov.sg/-/media/Csa/Documents/Publications/Cyber-Safety-Activity-Book-and-Handbook/Cyber-Safety-Handbook.pdf (Accessed 6th January 2022)

CSA Singapore, 2021a, "The Singapore Cybersecurity Strategy 2021". Retrieved from: https://www.csa.gov.sg/News/Publications/singapore-cybersecurity-strategy-2021 (Accessed 28th December 2021)

CSA Singapore, 2021b, "SG Cyber Youth Odyssey". Retrieved from: https://www.csa.gov.sg/Programmes/SGCyberTalent/SGCyberYouth/sg-cyber-youth-odyssey (Accessed 28th December 2021)

CSA Singapore, nd-a, SG Cyber Youth. Retrieved from: https://www.csa.gov.sg/Programmes/SGCyberTalent/SGCyberYouth (Accessed 28th December 2021)

CSA Singapore, nd-b, Youth Cyber Exploration Programme (YCEP). Retrieved from: https://www.csa.gov.sg/Programmes/SGCyberTalent/SGCyberYouth/YCEP (Accessed 28th December 2021)

CSA Singapore, nd-c, Cybersecurity Career Mentoring Programme. Retrieved from: https://www.csa.gov.sg/Programmes/Cybersecurity-Career-Mentoring-Programme (Accessed 28th December 2021)

CSA Singapore, nd-d, "About SG Cyber Safe Students Programme". Retrieved from: https://www.csa.gov.sg/Programmes/sg-cyber-safe-students/about-sg-cyber-safe-students (Accessed 28th December 2021)

CSA Singapore, nd-e, "Videos". Retrieved from: https://www.csa.gov.sg/Programmes/sg-cyber-safe-students/videos (Accessed 6th January 2022)

CSA Singapore, nd-f, "Reading and Printable Materials". Retrieved from: https://www.csa.gov.sg/Programmes/sg-cyber-safe-students/reading-and-printable-materials (Accessed 6th January 2022)

CSA Singapore, nd-g, "Go Safe Online Awareness Skit". Retrieved from: https://www.csa.gov.sg/Programmes/sg-cyber-safe-students/events-and-activities/go-safe-online-awareness-skit (Accessed 6th January 2022)

CSA Singapore, nd-h, SG Cyber Safe Programme. Retrieved from: https://www.csa.gov.sg/Programmes/Cybersecurity-Career-Mentoring-Programme (Accessed 28th December 2021)

CSA Singapore, nd-i, "Cyber Security Awareness Alliance". Retrieved from: https://www.csa.gov.sg/en/Who-We-Are/committees-and-panels/cyber-security-awareness-alliance (Accessed 13th January 2022)

CSA Singapore, nd-j, "Gosafeonline". Retrieved from: https://www.csa.gov.sg/gosafeonline (Accessed 6th January 2022)

CSA Singapore, nd-k, "Students". Retrieved from: https://www.csa.gov.sg/gosafeonline/Go-Safe-For-Me/For-Students (Accessed 28th December 2021)

CSA Singapore, nd-l, "Parents". Retrieved from: https://www.csa.gov.sg/gosafeonline/Go-Safe-For-Me/For-Parents (Accessed 28th December 2021)

CSA Singapore, nd-m, "SMEs". Retrieved from: https://www.csa.gov.sg/gosafeonline/Go-Safe-For-Business/SMEs (Accessed 28th December 2021)

CSA Singapore, nd-n, "SG Cyber Women". Retrieved from: https://www.csa.gov.sg/Programmes/SGCyberTalent/SGCyberWomen (Accessed 28th December 2021)

CSA Singapore, nd-o, "SG Cyber Safe Seniors Programme". Retrieved from: https://www.csa.gov.sg/programmes/sg-cyber-safe-seniors/about (Accessed 4th February 2022)

Cyber Crime Unit of the Hellenic Police, nd-a, "Ages 6 to 10 years old – cyberkid english". Retrieved from: https://www.cyberkid.gov.gr/en/6-10-%ce%b5%cf%84%cf%89%ce%bd (Accessed 5th January 2022)

Cyber Crime Unit of the Hellenic Police, nd-b, "Ages 11 to 14 years old – cyberkid english". Retrieved from: https://www.cyberkid.gov.gr/en/11-14-%ce%b5%cf%84%cf%89%ce%bd (Accessed 5th January 2022)

Cyber Crime Unit of the Hellenic Police, nd-c, "Ages 15 to 18 years old – cyberkid english". Retrieved from: https://www.cyberkid.gov.gr/en/15-18-%ce%b5%cf%84%cf%89%ce%bd (Accessed 5th January 2022)

Cyber Crime Unit of the Hellenic Police, nd-d, "Parents – cyberkid english". Retrieved from: https://www.cyberkid.gov.gr/en/%ce%b3%ce%bf%ce%bd%ce%b5%ce%af%cf%82/ (Accessed 5th January 2022)

Cyber Crime Unit of the Hellenic Police, nd-e, About Cyberkid. Retrieved from: https://www.cyberkid.gov.gr/en/application/%ce%ba%ce%b1%cf%84%ce%b5%ce%b2%ce%ac%cf%83%cf%84%ce%b5-%cf%84%ce%b7%ce%bd-%ce%b5%cf%86%ce%b1%cf%81%ce%bc%ce%bf%ce%b3%ce%ae/ (Accessed 20th January 2022)

Cyber Crime Unit of the Hellenic Police, nd-f, "CYBERALERT – από τη Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος". Retrieved from: https://cyberalert.gr/ (Accessed 16th January 2022)

Cyber Crime Unit of the Hellenic Police, nd-g, "About FeelSafe". Retrieved from: https://cyberalert.gr/en/?page_id=36008 (Accessed 16th January 2022)

Cyber Resilience Centre for the East Midlands, nd, "Services". Retrieved from: https://www.emcrc.co.uk/services (Accessed 6th January 2022)

Cyber Resilience Centre for the North West, nd, "Services". Retrieved from: https://www.nwcrc.co.uk/services (Accessed 6th January 2022)

Cyber Resilience Centre for the South East, nd, "Services". Retrieved from: https://www.secrc.co.uk/services (Accessed 6th January 2022)

Cyber Resilience Centre for the South West, nd, "Services". Retrieved from: https://www.swcrc.co.uk/services (Accessed 6th January 2022)

Cyber Resilience Centre for Wales, nd, "Services". Retrieved from: https://www.wcrcentre.co.uk/services (Accessed 6th January 2022)

Cyber Resilience Centre for the West Midlands, nd, "Services". Retrieved from: https://www.wmcrc.co.uk/services (Accessed 6th January 2022)

Cyber Security Challenge (New Zealand), nd, "Cyber Security Challenge". Retrieved from: https://cybersecuritychallenge.org.nz/ (Accessed 6th January 2022)

Cyber Security Challenge (New Zealand), 2021, "New Zealand Cyber Security Challenge: Rules and Eligibility" [PDF]. Retrieved from: https://cybersecuritychallenge.org.nz/FILES1/RulesAndEligibility.pdf (Accessed 5th January 2022)

Cyber Security Challenge UK, nd-a, "Home Page - Cyber Security Challenge UK". Retrieved from: https://cybersecuritychallenge.org.uk/ (Accessed 5th January 2022)

Cyber Security Challenge UK, nd-b, "CyberCenturion - Cyber Security Challenge UK". Retrieved from: https://cybersecuritychallenge.org.uk/what-we-do/cybercenturion (Accessed 6th January 2022)

Cyber Security Challenge UK, nd-b, “Cyber Challenge in a Box - Cyber Security Challenge UK”. Retrieved from: https://cybersecuritychallenge.org.uk/what-we-do/schools-programme/cciab (Accessed 6th January 2022)

Cyber Security Ontario, nd, “Cyber Security Ontario Learning Portal”. Retrieved from: https://cybersecurityontario.ca/ (Accessed 6th January 2022)

Cyber.org, nd, “Career Exploration”. Retrieved from: https://cyber.org/career-exploration (Accessed 6th January 2022)

CyberDiscovery, 2021, “What is GIAC?”. Retrieved from: https://help.joincyberdiscovery.com/help/what-is-giac (Accessed 6th January 2022)

CyberDiscovery, nd, “CyberDiscovery”. Retrieved from: https://joincyberdiscovery.com/ (Accessed 6th January 2022)

CyberSci, nd, “Canada’s Cyber Security Challenge”. Retrieved from: https://csc21.cybersecuritychallenge.ca/ (Accessed 6th January 2022)

Cybersecurity Hub, 2020a, “Cyber Safety Awareness Guide” [PDF]. Retrieved from: https://www.cybersecurityhub.gov.za/cyberawareness/images/workbooks/English%20BHC%20-%20Workbook%201%20-%20Cyber%20Safety%20Awareness%20Guide_V0.18.pdf (Accessed 6th January 2022)

Cybersecurity Hub, 2020b, “Cyber Safety Awareness Workbook” [PDF]. Retrieved from: https://www.cybersecurityhub.gov.za/cyberawareness/images/workbooks/BHC%20-%20Workbook%202%20-%20Cyber%20Safety%20Awareness%20Workbook_V0.23.pdf (Accessed 6th January 2022)

CyBOK, 2021a, “Risk Management & Governance Knowledge Area: Version 1.1.1” [PDF]. Retrieved from: https://www.cybok.org/media/downloads/Risk_Management_Governance_v1.1.1.pdf (Accessed 6th January 2022)

CyBOK, 2021b, “Law and Regulation Knowledge Area: Version 1.0.2” [PDF]. Retrieved from: https://www.cybok.org/media/downloads/Law_Regulation_v1.0.2.pdf (Accessed 6th January 2022)

CyBOK, 2021c, “Human Factors Knowledge Area: Version 1.0.1” [PDF]. Retrieved from: https://www.cybok.org/media/downloads/Human_Factors_v1.0.1.pdf (Accessed 6th January 2022)

CyBOK, 2021d, “Privacy & Online Rights Knowledge Area: Version 1.0.2” [PDF]. Retrieved from: https://www.cybok.org/media/downloads/Privacy_Online_Rights_v1.0.2.pdf (Accessed 6th January 2022)

CyBOK, 2021e, “Adversarial Behaviours Knowledge Area: Version 1.0.1” [PDF]. Retrieved from:

https://www.cybok.org/media/downloads/Adversarial_Behaviours_v1.0.1.pdf (Accessed 6th January 2022)

CyBOK, nd, "The Cyber Security Body Of Knowledge". Retrieved from: https://www.cybok.org/ (Accessed 6th January 2022)

CYPCS (Children's and Young People's Commissioner Scotland), nd-a, "Getting Advice". Retrieved from: https://cypcs.org.uk/get-help/parent-or-carer/getting-advice/ (Accessed 6th January 2022)

CYPCS (Children's and Young People's Commissioner Scotland), nd-b, "Where can I find information about online abuse and safety?". Retrieved from: https://cypcs.org.uk/faq/where-can-i-find-information-about-online-abuse-and-safety/ (Accessed 6th January 2022)

DCMS, 2017, "Change of name for DCMS". Retrieved from: https://www.gov.uk/government/news/change-of-name-for-dcms (Accessed 6th January 2022)

DCMS (Department for Digital, Culture, Media and Sport, UK), 2019, "Online Harms White Paper" [PDF]. Retrieved from: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/973939/Online_Harms_White_Paper_V2.pdf (Accessed 5th January 2022)

DCMS, 2020, "UK's booming cyber security sector worth £8.3 billion". Retrieved from: https://www.gov.uk/government/news/uks-booming-cyber-security-sector-worth-83-billion (Accessed 6th January 2022)

DCMS, 2021a, "Understanding the cyber security recruitment pool". Retrieved from: https://www.gov.uk/government/publications/understanding-the-cyber-security-recruitment-pool (Accessed 6th January 2022)

DCMS, 2021b, "Draft Online Safety Bill" [PDF]. Retrieved from: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/985033/Draft_Online_Safety_Bill_Bookmarked.pdf (Accessed 5th January 2022)

DCMS, 2021c, "Online Media Literacy Strategy" [PDF]. Retrieved from: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1004233/DCMS_Media_Literacy_Report_Roll_Out_Accessible_PDF.pdf (Accessed 7th February 2022)

DCMS, 2021d, "Online media literacy resources". Retrieved from: https://www.gov.uk/guidance/online-media-literacy-resources (Accessed 7th February 2022)

DESE, 2021a, "Why is STEM important?". Retrieved from: https://www.dese.gov.au/australian-curriculum/national-stem-education-resources-toolkit/introductory-material/why-stem-important (Accessed 6th January 2022

DESE, 2021b, "Decide what you want to achieve". Retrieved from: https://www.dese.gov.au/australian-curriculum/national-stem-education-resources-toolkit/i-

want-run-stem-education-initiative/decide-what-you-want-achieve (Accessed 6th January 2022)

DESE (Department for Education, Skills and Employment, Australia), 2021c, "Digital Literacy Skills Framework". Retrieved from: https://www.dese.gov.au/foundation-skills-your-future-program/resources/digital-literacy-skills-framework (Accessed 6th January 2022)

DESE, 2021d, "Digital Skills Cadetship Trial". Retrieved from: https://www.dese.gov.au/digitalskillscadetshiptrial (Accessed 6th January 2022)

Department for Education (UK), 2013, "National curriculum in England: computing programmes of study". Retrieved from: https://www.gov.uk/government/publications/national-curriculum-in-england-computing-programmes-of-study/national-curriculum-in-england-computing-programmes-of-study (Accessed 6th January 2022)

Department for Education (UK), 2014a, "National curriculum". Retrieved from: https://www.gov.uk/government/collections/national-curriculum (Accessed 6th January 2022)

Department for Education (UK), 2014b, "Cyberbullying: Advice for headteachers and school staff" [PDF]. Retrieved from: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/374850/Cyberbullying_Advice_for_Headteachers_and_School_Staff_121114.pdf (Accessed 5th January 2022)

Department for Education (UK), 2017, "Preventing and Tackling Bullying" [PDF]. Retrieved from: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/623895/Preventing_and_tackling_bullying_advice.pdf (Accessed 5th January 2022)

Department for Education (UK), 2019, "Teaching online safety in school" [PDF]. Retrieved from: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/811796/Teaching_online_safety_in_school.pdf (Accessed 5th January 2022)

Department for Education (UK), 2021a, "Keeping children safe in education 2021: Statutory guidance for schools and colleges" [PDF]. Retrieved from: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1021914/KCSIE_2021_September_guidance.pdf (Accessed 5th January 2022)

Department for Education (UK), 2021b, "Safeguarding and remote education during coronavirus (COVID-19)". Retrieved from: https://www.gov.uk/guidance/safeguarding-and-remote-education-during-coronavirus-covid-19 (Accessed 6th January 2022)

Department for Employment and Learning (Northern Ireland, UK), 2016, "Further Education Means Success: The Northern Ireland Strategy for Further Education" [PDF]. Retrieved from:

https://www.economy-ni.gov.uk/sites/default/files/publications/economy/FE-Strategy%20-FE-Means-success.pdf (Accessed 12th January 2022)

Department of Basic Education (South Africa), 2011a, "Curriculum and Assessment Policy Statement Grades R-3: Life Skills" [PDF]. Retrieved from: https://www.education.gov.za/Portals/0/CD/National%20Curriculum%20Statements%20and%20Vocational/CAPS%20Life%20Skills%20%20English%20_%20Gr%20R-3%20FS.pdf (Accessed 5th January 2022)

Department of Basic Education (South Africa), 2011b, "Curriculum and Assessment Policy Statement Grades 7-9: Life Skills" [PDF]. Retrieved from: https://www.education.gov.za/Portals/0/CD/National%20Curriculum%20Statements%20and%20Vocational/CAPS%20SP%20%20LIFE%20ORIENTATION%20%20WEB.pdf?ver=2015-01-27-160145-607 (Accessed 5th January 2022)

Department of Basic Education (South Africa), 2018, "Curriculum and Assessment Policy Statement Grades 4-6: Life Skills" [PDF]. Retrieved from: https://www.education.gov.za/Portals/0/Documents/Publications/CAPS%20Commnets/GET/LIFE%20SKILLS%20IP%20GRADES%204%20-%206%20EDITED.PDF?ver=2018-08-29-160753-803 (Accessed 5th January 2022)

Department of Education (Northern Ireland), nd, "Compulsory Education". Retrieved from: https://www.education-ni.gov.uk/articles/compulsory-education (Accessed 6th January 2022)

Department of Foreign Affairs and Trade (Australia), 2017, "The Australian Education System: Foundation Level" [PDF]. Retrieved from: https://www.dfat.gov.au/sites/default/files/australian-education-system-foundation.pdf (Accessed 5th January 2022)

Department of Home Affairs (Australia), 2020, "Australia's Cyber Security Strategy" [PDF]. Retrieved from: https://www.homeaffairs.gov.au/cyber-security-subsite/files/cyber-security-strategy-2020.pdf (Accessed 5th January 2022)

Department of Internal Affairs (New Zealand), nd-a, "The Inter-Yeti". Retrieved from: https://theinteryeti.govt.nz/ (Accessed 6th January 2022)

Department of Internal Affairs (New Zealand), nd-b, "The Inter-Yeti". Retrieved from: https://www.keepitrealonline.govt.nz/theinteryeti (Accessed 6th January 2022)

Department of the Prime Minister and Cabinet (New Zealand), 2020, "National Cyber Policy Office". Retrieved from: https://dpmc.govt.nz/our-business-units/national-security-group/national-security-policy/national-cyber-policy-office (Accessed 24th January 2022)

Department of Telecommunications & Postal Services (South Africa), nd, "Cybersecurity Hub". Retrieved from: https://www.cybersecurityhub.gov.za/ (Accessed 6th January 2022)

Differencebetween.net, nd, "Difference Between Pupil and Student". Retrieved from: http://www.differencebetween.net/language/words-language/difference-between-pupil-and-student/ (Accessed 6th January 2022)

DIGI, 2021, "Australian Code of Practice on Disinformation and Misinformation" [PDF]. Retrieved from: https://digi.org.au/wp-content/uploads/2021/02/Australian-Code-of-Practice-on-Disinformation-and-Misinformation-FINAL-PDF-Feb-22-2021.pdf (Accessed 5th January 2022)

Digital Technologies Hub, nd-a, "Students". Retrieved from: https://www.digitaltechnologieshub.edu.au/students (Accessed 6th January 2022)

Digital Technologies Hub, nd-b, "Students Digital Technologies". Retrieved from: https://www.digitaltechnologieshub.edu.au/students/cybersafety (Accessed 6th January 2022)

Digital Technologies Hub, nd-c, "Teachers". Retrieved from: https://www.digitaltechnologieshub.edu.au/teachers (Accessed 6th January 2022)

Digital Technologies Hub, nd-d, "Onlinear Learning Resources for Teachers and Parents". Retrieved from: https://www.digitaltechnologieshub.edu.au/search#/site-search?cnttype=resource (Accessed 6th January 2022)

Direção-geral da educação, 2012, "Diário da República, 2.ª série — N.º 242" [PDF]. Retrieved from: http://www.dge.mec.pt/sites/default/files/ficheiros/despacho_15971_2012_8.pdf (Accessed 5th January 2022)

Eastern Cyber Resilience Centre, nd, "Education". Retrieved from: https://www.ecrcentre.co.uk/education (Accessed 6th January 2022)

ECSO (European Cyber Security Organisation), nd, "Youth4Cyber". Retrieved from: https://ecs-org.eu/initiatives/youth4cyber (Accessed 5th January 2022)

EdPlace.com, nd, "Understanding National Curriculum Levels". Retrieved from: https://www.edplace.com/blog/edplace-explains/understanding-national-curriculum-levels (Accessed 6th January 2022)

Education Central, 2017, "Digital technology becoming compulsory in school curriculum". Retrieved from: https://educationcentral.co.nz/digital-technology-becoming-compulsory-in-school-curriculum/ (Accessed 6th January 2022)

Education Commission of the States, nd, "50-State Comparison: State K-3 Policies". Retrieved from: https://www.ecs.org/kindergarten-policies/ (Accessed 6th January 2022)

Education Matters, nd, "Introducing the Digital Technologies curriculum". Retrieved from: https://www.educationmattersmag.com.au/digital-tech/ (Accessed 6th January 2022)

Education Scotland, 2015, “Building Society: Young people’s experiences and outcomes in the technologies” [PDF]. Retrieved from: https://education.gov.scot/media/lk3kvmxw/tec8-impactreport.pdf (Accessed 6th January 2022)

Education Scotland, 2017, “Benchmarks: Technologies” [PDF]. Retrieved from: https://education.gov.scot/nih/Documents/TechnologiesBenchmarksPDF.pdf (Accessed 5th January 2022)

Education Scotland, 2018, “Curriculum for Excellence: Technologies. Experiences and Outcomes” [PDF]. Retrieved from: https://education.gov.scot/Documents/Technologies-es-os.pdf (Accessed 5th January 2022)

Education Scotland, 2021, “Assessment within BGE 2020/21 (Update)” [PDF]. Retrieved from: https://education.gov.scot/media/rjeovyau/assessment-within-bge-2020-21-update.pdf (Accessed 12th January 2022)

Education Scotland, nd-a, “About the 3-18 curriculum”. Retrieved from: https://education.gov.scot/parentzone/learning-in-scotland/about-the-3-18-curriculum/ (Accessed 6th January 2022)

Education Scotland, nd-b, “Curriculum levels”. Retrieved from: https://education.gov.scot/parentzone/learning-in-scotland/curriculum-levels/ (Accessed 6th January 2022)

Education Wales, 2018, “Digital Competence Framework guidance: Update – June 2018” [PDF]. Retrieved from: https://hwb.gov.wales/api/storage/337437b8-cfe3-4305-ae32-f47ad82f3e76/digital-competence-framework-guidance-2018.pdf (Accessed 5th January 2022)

Elsevier B.V, nd, “Scopus - Welcome to Scopus”. Retrieved from: https://www.scopus.com/ (Accessed 25th January 2022)

ENISA, nd-a, “About ENISA - The European Union Agency for Cybersecurity”. Retrieved from: https://www.enisa.europa.eu/about-enisa (Accessed 6th January 2022)

ENISA, nd-b, “European Cyber Security Challenge — ECSC”. Retrieved from: https://ecsc.eu/ (Accessed 5th January 2022)

ENISA, nd-c, “EU Cyber Security Month”. Retrieved from: https://cybersecuritymonth.eu/ (Accessed 5th January 2022)

ERO, 2016, “School Evaluation Indicators” [PDF]. Retrieved from: https://ero.govt.nz/sites/default/files/2021-04/School%20Evaluation%20Indicators%202016_0.pdf (Accessed 5th January 2022)

eSafety Commissioner (Australia), 2021, “Best Practice Framework for Online Safety Education”. Retrieved from: https://www.esafety.gov.au/sites/default/files/2021-07/BPF%20Online%20Safety%20Edu%20Fact%20sheet.pdf (Accessed 6th January 2022)

eSafety Commissioner (Australia), nd-a, “Our Programs”. Retrieved from: https://www.esafety.gov.au/about-us/what-we-do/our-programs (Accessed 6th January 2022)

eSafety Commissioner (Australia), nd-b, “Community education and training”. Retrieved from: https://www.esafety.gov.au/about-us/what-we-do/our-programs/training (Accessed 6th January 2022)

eSafety Commissioner (Australia), nd-c, “eSafety Kids”. Retrieved from: https://www.esafety.gov.au/kids (Accessed 6th January 2022)

eSafety Commissioner (Australia), nd-d, “eSafety Young People”. Retrieved from: https://www.esafety.gov.au/young-people (Accessed 6th January 2022)

eSafety Commissioner (Australia), nd-e, “Safer Internet Day 2021”. Retrieved from: https://www.esafety.gov.au/about-us/events/safer-internet-day-2021 (Accessed 6th January 2022)

eSafety Commissioner (Australia), nd-f, “Toolkit for Schools”. Retrieved from: https://www.esafety.gov.au/educators/toolkit-schools (Accessed 6th January 2022)

eSafety Commissioner (Australia), nd-g, “Engage”. Retrieved from: https://www.esafety.gov.au/educators/toolkit-for-schools/engage (Accessed 6th January 2022)

ESEE (Hellenic Confederation of Commerce and Entrepreneurship), nd, “Who We Are – ΕΣΕΕ – Ελληνική Συνομοσπονδία Εμπορίου & Επιχειρηματικότητας”. Retrieved from: https://esee.gr/en/pii-imaste/ (Accessed 16th January 2022)

Estonian Ministry of Education and Research, 2020, “Pre-school, basic and secondary education”. Retrieved from: https://www.hm.ee/en/activities/pre-school-basic-and-secondary-education (Accessed 5th January 2022)

European Commission, nd, “Preparatory secondary vocational education (‘VMBO’) care and welfare profile-theoretical pathway”. Retrieved from: https://europa.eu/europass/en/courses/qualification/cd357e64-f813-4302-a721-0476f47b126b (Accessed 6th January 2022)

Expactica.com, 2021, “South Africa”. Retrieved from: https://www.expatica.com/za/education/children-education/education-in-south-africa-803205/ (Accessed 6th January 2022)

FPB (Film and Publications Board, South Africa), nd, “Outreach and Public Education”. Retrieved from: https://www.fpb.org.za/what-we-do/outreach-public-education-2/ (Accessed 6th January 2022)

FCT (Fundação para Ciência e a Tecnologia, Portugal; Foundation for Science and Technology in English), nd, “Portugal INCoDe.2030”. Retrieved from: https://www.fct.pt/dsi/portugalincode2030/index.phtml.en (Accessed 6th January 2022)

GFCE (Global Forum on Cyber Expertise), 2017, "Delhi Communiqué on a GFCE Global Agenda for Cyber Capacity Building" [PDF]. Retrieved from: https://thegfce.org/wp-content/uploads/2020/04/DelhiCommunique.pdf (Accessed 5th January 2022)

GFCE, 2020a, "GFCE Working Groups: Terms of Reference" [PDF]. Retrieved from: https://thegfce.org/wp-content/uploads/2020/09/GFCE-Working-Groups_Terms-of-Reference-TOR.pdf (Accessed 5th January 2022)

GFCE, 2020b, "Global Cyber Capacity Building Research Agenda 2021" [PDF]. Retrieved from: https://thegfce.org/wp-content/uploads/2020/11/GFCE-Global-CCB-Research-Agenda-2021.pdf (Accessed 5th January 2022)

GFCE, nd, "Who is GFCE?". Retrieved from: https://thegfce.org/who-is-the-gfce/ (Accessed 6th January 2022)

Glow, nd, "Glow Connect – Scotland's digital learning platform". Retrieved from: https://glowconnect.org.uk/ (Accessed 6th January 2022)

Gobierno de México, 2017, "National Cybersecurity Strategy" [PDF]. Retrieved from: https://www.gob.mx/cms/uploads/attachment/file/399655/ENCS.ENG.final.pdf (Accessed 5th January 2022)

Gobierno de México, nd, "CONALITEG". Retrieved from: https://www.conaliteg.sep.gob.mx/ (Accessed 6th January 2022)

Government of British Columbia, nd-a, "Cybersecurity Courses". Retrieved from: https://www2.gov.bc.ca/gov/content/governments/services-for-government/information-management-technology/information-security/professional-development/cybersecurity-courses?keyword=cyber&keyword=security (Accessed 6th January 2022)

Government of British Columbia, nd-b, "October is Cyber Security Awareness Month". Retrieved from: https://www2.gov.bc.ca/gov/content/governments/services-for-government/information-management-technology/information-security/information-security-awareness/cyber-security-awareness-month?keyword=cyber&keyword=security (Accessed 6th January 2022)

Government of British Columbia, nd-c, "Top 10 Cyber Security Tips". Retrieved from: https://www2.gov.bc.ca/gov/content/governments/services-for-government/information-management-technology/information-security/information-security-awareness/top-10-cyber-security-tips?keyword=cyber&keyword=security (Accessed 6th January 2022)

Government of British Columbia, nd-d, "Information Security Online Course". Retrieved from: https://www2.gov.bc.ca/gov/content/governments/services-for-government/information-management-technology/information-security/professional-development/information-security-online-course?keyword=cyber&keyword=security (Accessed 6th January 2022)

Government of Canada, 2019, "CanCode". Retrieved from: https://www.ic.gc.ca/eic/site/121.nsf/eng/home (Accessed 6th January 2022)

Government of Canada, 2021a, “Education in Canada: Types of schooling”. Retrieved from: https://www.canada.ca/en/immigration-refugees-citizenship/services/new-immigrants/new-life-canada/education/types-school.html (Accessed 6th January 2022)

Government of Canada, 2021b, “Get Cyber Safe Challenge 2021”. Retrieved from: https://www.getcybersafe.gc.ca/en/blogs/get-cyber-safe-challenge-2021 (Accessed 6th January 2022)

Government of Canada, 2021c, “Blogs”. Retrieved from: https://www.getcybersafe.gc.ca/en/blogs (Accessed 6th January 2022)

Government of Canada, 2022, “Get Cyber Safe”. Retrieved from: https://www.getcybersafe.gc.ca/en (Accessed 6th January 2022)

Government of the Netherlands, nd, “Senior general secondary education (HAVO) and pre university education (VWO)”. Retrieved from: https://www.government.nl/topics/secondary-education/different-types-of-secondary-education/senior-general-secondary-education-havo-and-pre-university-education-vwo (Accessed 6th January 2022)

Greek Ombudsman, nd, “Children’s Rights”. Retrieved from: https://www.synigoros.gr/?i=childrens-rights.en (Accessed 16th January 2022)

Grok Academy, nd-a, “Schools Cyber Security Challenges”. Retrieved from: https://aca.edu.au/projects/cyber-challenges/ (Accessed 6th January 2022)

Grok Academy, nd-b, “Grok Cyber Pursuit”. Retrieved from: https://aca.edu.au/resources/cyber-pursuit/ (Accessed 6th January 2022)

Grok Academy, nd-c, “Resources”. Retrieved from: https://aca.edu.au/resources/#grok-cyber (Accessed 6th January 2022)

Home Office (UK), 2010, “Cyber Crime Strategy” [PDF]. Retrieved from: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/228826/7842.pdf (Accessed 6th January 2022)

Home Office (UK), 2015, “Online abuse and bullying prevention guide” [PDF]. Retrieved from: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/414118/NSPCC_online_abuse_and_bullying_prevention_guide_3.pdf (Accessed 6th January 2022)

Horta, M. J., Mendoça, F., & Nascimento, R. 2012, “METAS CURRICULARES Tecnologias de Informação e Comunicação 7.º e 8.º anos” [PDF]. Retrieved from: http://www.dge.mec.pt/sites/default/files/ficheiros/eb_tic_7_e_8_ano.pdf (Accessed 5th January 2022)

ICTC (Information and Communications Technology Council), 2021, “ICTC Insights On The 2021 Federal Budget”. Retrieved from: https://www.ictc-ctic.ca/ictc-insights-2021-federal-budget/ (Accessed 6th January 2022)

IFIP (International Federation for Information Processing), nd, "IFIP - Home". Retrieved from: https://www.ifip.org/ (Accessed 5th January 2022)

iKeepSafe, nd-a, "About – iKeepSafe". Retrieved from: https://ikeepsafe.org/ (Accessed 10th February 2022)

iKeepSafe, nd-b, "National Cyber Signing Day Presentations". Retrieved from: https://www.k12cybersecurityconference.org/national-cyber-signing-day-videos (Accessed 10th February 2022)

Informatics Europe, nd, "Informatics Europe - Home". Retrieved from: https://www.informatics-europe.org/ (Accessed 6th January 2022)

Informatics for All, nd, "The Informatics for All Coalition". Retrieved from: https://www.informaticsforall.org/ (Accessed 5th January 2022)

Internet Matters, 2021, "UKCIS Digital Passport". Retrieved from: https://www.internetmatters.org/ukcis-vulnerable-working-group/ukcis-digital-passport/ (Accessed 6th January 2022)

(ISC)2, 2021, "A Resilient Cybersecurity Profession Charts the Path Forward: (ISC)2 Cybersecurity Workforce Study". Retrieved from: https://www.isc2.org//-/media/ISC2/Research/2021/ISC2-Cybersecurity-Workforce-Study-2021.ashx (Accessed 6th January 2022)

ISTE (International Society for Technology in Education), nd, "ISTE Standard: Students". Retrieved from: https://www.iste.org/standards/iste-standards-for-students (Accessed 6th January 2022)

ITU (International Telecommunication Union), 2020a, "ICT Key Facts and Figures 2020" [PDF]. Retrieved from: https://www.itu.int/en/ITU-D/Statistics/Documents/facts/FactsFigures2020.pdf (Accessed 5th January 2022)

ITU, 2020b, "Online safety activity book: Teacher's Guide" [PDF]. Retrieved from: https://www.itu-cop-guidelines.com/_files/ugd/24bbaa_71d2c54c8a6e44d4b97d70193bd92ae9.pdf (Accessed 3rd February 2022)

ITU, 2021a, "Global Cybersecurity Index 2020" [PDF]. Retrieved from: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf (Accessed 5th January 2022)

ITU, 2021b, "The ITU 2021 Global CyberDrill". Retrieved from: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/Cyberdrills-2021.aspx (Accessed 6th January 2022)

ITU, nd-a, "About International Telecommunication Union (ITU)". Retrieved from: https://www.itu.int/en/about/ (Accessed 6th January 2022)

ITU, nd-b, “Global Cybersecurity Agenda (GCA)”. Retrieved from: https://www.itu.int/en/action/cybersecurity/Pages/gca.aspx (Accessed 6th January 2022)

ITU, nd-c, “Child Online Protection”. Retrieved from: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/COP.aspx (Accessed 6th January 2022)

ITU, nd-d, “Child Online Protection | ITU COP Guidelines”. Retrieved from: https://www.itu-cop-guidelines.com/ (Accessed 6th January 2022)

ITU, nd-e, “Global Cybersecurity Index”. Retrieved from: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx (Accessed 6th January 2022)

ITU, nd-f, “Women in Cyber Mentorship Programme”. Retrieved from: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/Women-in-Cyber/Women-in-Cyber-Mentorship-Programme.aspx (Accessed 6th January 2022)

ITU, nd-g, “National CIRT”. Retrieved from: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/national-CIRT.aspx (Accessed 6th January 2022)

ITU, nd-h, “Resources | ITU-COP Guidelines”. Retrieved from: https://www.itu-cop-guidelines.com/resources (Accessed 3rd February 2022)

ITU, nd-i, “Children | ITU-COP Guidelines”. Retrieved from: https://www.itu-cop-guidelines.com/children (Accessed 6th January 2022)

ITU, nd-j, “Workbook | ITU-COP Guidelines”. Retrieved from: https://www.itu-cop-guidelines.com/workbook (Accessed 3rd February 2022)

k12cs.org, nd, “Statements of Support”. Retrieved from: https://k12cs.org/statements-of-support/ (Accessed 28th December 2021)

K–12 Computer Science Framework Steering Committee, 2016, “K–12 Computer Science Framework” [PDF]. Retrieved from: https://k12cs.org/wp-content/uploads/2016/09/K%E2%80%9312-Computer-Science-Framework.pdf (Accessed 5th January 2022)

Kennisnet, nd-a, “Who we are”. Retrieved from: https://www.kennisnet.nl/wie-wij-zijn/ (Accessed 27th October 2021)

Kennisnet, nd-b, “Our services”. Retrieved from: https://www.kennisnet.nl/diensten/ (Accessed 27th October 2021)

Kennisnet, nd-c, “Our publications”. Retrieved from: https://www.kennisnet.nl/publicaties/ (Accessed 27th October 2021)

Kennisnet, nd-d, “Know everything about ICT skills teacher”. Retrieved from: https://www.kennisnet.nl/ict-bekwaamheid-leraar/ (Accessed 27th October 2021)

Kritzinger, E., 2017, "Cyber Safety Educator Workbook, Grade 4 & Grade 6" [PDF]. (Received from the author via email on 9th August 2021)

Livingstone, S., Kardefelt Winther, D. and Saeed, M., 2019, "Global Kids Online Comparative Report" [PDF]. Innocenti Research Report of UNICEF Office of Research. Retrieved from: https://www.unicef-irc.org/publications/pdf/GKO%20LAYOUT%20MAIN%20REPORT.pdf (Accessed 5th January 2022)

Lorenz, B., 2021, "Cybersecurity Education and Competitions in Estonia". Retrieved from: https://docs.google.com/presentation/d/15d-OGUUNe5IbuBkT_agiVBkT0fHI-F4wa-LE_xAWLeU/present?slide=id.p1 (Accessed 5th January 2022)

Māra Jākobsone, 2021, "Greece – Digital Transformation Strategy for 2020-2025". Retrieved from: https://digital-skills-jobs.europa.eu/en/actions/national-initiatives/national-strategies/greece-digital-transformation-strategy-2020-2025 (Accessed 16th January 2022)

McHenry, D., Borges, T., Bollen, A, Shah J.N., and Donaldson, S., Crozier, D. and Furnell, S., 2021, "Cyber security skills in the UK labour market 2021: Findings report" [PDF]. Retrieved from: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/973802/Ipsos_MORI_Cyber_Skills_in_the_UK_2021_v1.pdf (Accessed on 5th January 2022)

Ministry of Citizen Protection (Greece), 2021, "ΔΕΛΤΙΟ ΤΥΠΟΥ". Retrieved from: http://www.astynomia.gr/index.php?option=ozo_content&lang=&perform=view&id=103304&Itemid=2646&lang= (Accessed 6th January 2022)

Ministry of Digital Governance (Greece), 2018, "National Cyber Security Strategy: Version 3.0" [PDF]. Retrieved from: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/national-cyber-security-strategy-greece/@@download_version/50cded9109d442e7839649f42055da60/file_en (Accessed 17th January 2022)

Ministry of Digital Governance (Greece), nd, "Βίβλος Ψηφιακού Μετασχηματισμού 2020-2025". Retrieved from: https://digitalstrategy.gov.gr/ (Accessed 17th January 2022)

Ministry of Economic Affairs and Communications (Estonia), 2019, "Cybersecurity Strategy: Republic of Estonia" [PDF]. Retrieved from: https://www.mkm.ee/sites/default/files/kyberturvalisuse_strateegia_2022_eng.pdf (Accessed 6th January 2022)

Ministry of Education (New Zealand), 2017, "Te Marautanga a Aoteroa" [PDF]. Retrieved from: https://tmoa.tki.org.nz/content/download/3099/22763/file/TMoA%20Whakapa%CC%84keha%CC%84tanga%20Dec%202017%20V1%20.pdf (Accessed on 5th January 2022)

Ministry of Education (New Zealand), 2019, "Technology in the New Zealand Curriculum" [PDF]. Retrieved from:

https://nzcurriculum.tki.org.nz/content/download/168478/1244184/file/NZC-Technology%20in%20the%20New%20Zealand%20Curriculum-Insert%20Web.pdf (Accessed on 5th January 2022)

Ministry of Education (New Zealand), 2020, "Information for students". Retrieved from: https://www.education.govt.nz/our-work/changes-in-education/digital-technologies-and-hangarau-matihiko-learning/information-for-students/ (Accessed 6th January 2022)

Ministry of Education (New Zealand), 2021a, Education in New Zealand. Retrieved from: https://www.education.govt.nz/our-work/our-role-and-our-people/education-in-nz (Accessed 6th January 2022)

Ministry of Education (New Zealand), 2021b, "Protect your school from cyber-attacks and cyber security breaches". Retrieved from: https://www.education.govt.nz/school/digital-technology/protect-your-school-from-cyber-attacks-and-cyber-security-breaches/ (Accessed 6th January 2022)

Ministry of Education (New Zealand), 2021c, "Digital Technologies and Hangarau Matihiko learning". Retrieved from: https://www.education.govt.nz/our-work/changes-in-education/digital-technologies-and-hangarau-matihiko-learning/ (Accessed 6th January 2022)

Ministry of Education, Research and Religions (Greece), 2006, "Informatics (AD, BD, DG High School) – Student Book (Enriched)". Retrieved from: http://ebooks.edu.gr/ebooks/v/html/8547/2759/Pliroforiki_A-B-G-Gymnasiou_html-empl/ (Accessed 6th January 2022)

Ministry of Education (Singapore), 2012, "Character and Citizenship Education Syllabus – Primary" [PDF]. Retrieved from: https://www.moe.gov.sg/-/media/files/primary/characterandcitizenshipeducationprimarysyllabusenglish.pdf (Accessed 5th January 2022)

Ministry of Education (Singapore), 2016, "Social Studies Syllabus – Upper Secondary Express Course – Normal (Academic) Course: Implementation starting with 2016 Secondary Three Cohort" [PDF]. Retrieved from: https://www.moe.gov.sg/-/media/files/secondary/syllabuses/humanities/2016socialstudiesuppersecondaryexpressnormalacademicsyllabus.pdf (Accessed 5th January 2022)

Ministry of Education (Singapore), 2020a, "Character and Citizenship Education Syllabus – Secondary" [PDF]. Retrieved from: https://www.moe.gov.sg/-/media/files/secondary/syllabuses-nt/cce/2021-character-and-citizenship-education-syllabus-secondary.pdf?la=en&hash=B50AE76F6499F6E5F392E690D1E7E084C0A52915 (Accessed 5th January 2022)

Ministry of Education (Singapore), 2020b, "Primary School Education: Preparing Your Child for Tomorrow". Retrieved from: https://www.readkong.com/page/primary-school-education-preparing-your-child-for-tomorrow-8231703 (Accessed 6th January 2022)

Ministry of Education (Singapore), 2020c, "Secondary School Education: Shaping the Next Phase of Your Child's Learning Journey". Retrieved from: https://www.readkong.com/page/secondary-school-education-8832917 (Accessed 6th January 2022)

Ministry of Education (Singapore), 2020d, "Cybersecurity for school websites and online home-based learning". Retrieved from: https://www.moe.gov.sg/news/parliamentary-replies/20200504-cybersecurity-for-school-websites-and-online-home-based-learning (Accessed 6th January 2022)

Ministry of Education (Singapore), nd-a, "Education Levels: Primary". Retrieved from: https://www.moe.gov.sg/primary (Accessed 6th January 2022)

Ministry of Education (Singapore), nd-b, "Education Levels: Secondary". Retrieved from: https://www.moe.gov.sg/secondary (Accessed 6th January 2022)

Ministry of Education (Singapore), nd-c, "Primary school subjects and syllabuses". Retrieved from: https://www.moe.gov.sg/primary/curriculum/syllabus (Accessed 6th January 2022)

Ministry of Education (Singapore), nd-d, "Normal (Technical) course for secondary school". Retrieved from: https://www.moe.gov.sg/secondary/courses/normal-technical (Accessed 2nd August 2021)

Ministry of Education (Singapore), nd-c, "Cyber wellness | MOE". Retrieved from: https://www.moe.gov.sg/programmes/cyber-wellness (Accessed 28th December 2021)

Ministry of Home Affairs (Singapore), 2016, "National Cybercrime Action Plan" [PDF]. Retrieved from: https://www.mha.gov.sg/docs/default-source/media-room-doc/ncap-document.pdf (Accessed 5th January 2022)

Ministry of Justice and Security (The Netherlands), 2018, "Cyber Security Agenda: A cyber secure Netherlands" [PDF]. Retrieved from: https://english.ncsc.nl/binaries/ncsc-en/documents/publications/2019/juni/01/national-cyber-security-agenda/National-Cyber-Security-Agenda.pdf (Accessed 5th January 2022)

Ministry of Justice and Public Security (Norway), 2019, "National strategy for digital security competence" [PDF]. retrieved from: https://www.regjeringen.no/contentassets/8ed748d37e504a469874ce936551b4f8/nasjonal-strategi-for-digital-sikkerhetskompetanse.pdf (Accessed 5th January 2022)

MoodSpark, nd, "Internet safety tips for teens". Retrieved from: https://moodspark.org.uk/internet-safety-tips-for-teens/ (Accessed 6th January 2022)

National Cyber Resilience Centre Group (UK), nd, "Regional Centres - National CRC Group". Retrieved from: https://nationalcrcgroup.co.uk/regional-centres/ (Accessed 8th February 2022)

National Digital Academy (Greece), nd, "Ψηφιακή Ακαδημία Πολιτών". Retrieved from: https://nationaldigitalacademy.gov.gr/ (Accessed 16th January 2022)

NCA (National Crime Agency, UK), 2021a, "Cyber Choices: Hacking It Legal - Helping young people develop cyber skills: Parents/Guardians/Carers" [PDF]. Retrieved from: https://www.nationalcrimeagency.gov.uk/who-we-are/publications/525-cyber-choices-hacking-it-legal-parents-guardians-carers (Accessed 5th January 2022)

NCA, 2021b, "Cyber Choices: Hacking It Legal - Helping young people develop cyber skills: For Teachers" [PDF]. Retrieved from: https://www.nationalcrimeagency.gov.uk/who-we-are/publications/526-cyber-choices-hacking-it-legal-teachers/file (Accessed 5th January 2022)

NCA, nd, "Cyber Choices: Helping you choose the right and legal path". Retrieved from: https://www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/cyber-crime/cyberchoices (Accessed 6th January 2022)

NCCE (National Centre for Computing Education, UK), nd-a, "Teach Computing". Retrieved from: https://teachcomputing.org/ (Accessed 5th January 2022)

NCCE, nd-b, "NCCE and education recovery". Retrieved from: https://teachcomputing.org/education-recovery (Accessed 6th January 2022)

NCEE (National Center on Education and the Economy), nd, "Canada". Retrieved from: https://ncee.org/country/canada/ (Accessed 6th January 2022)

NCES (National Education Center for Statistics), 2002. "Chapter 7: Technology Integration, Technology in Schools: Suggestions, Tools, and Guidelines for Assessing Technology in Elementary and Secondary Education". Retrieved from: https://nces.ed.gov/pubs2003/tech_schools/chapter7.asp (Accessed 6th January 2022)

NCSA (National Cybersecurity Authority, Greece), 2020, "ΕΘΝΙΚΗ ΣΤΡΑΤΗΓΙΚΗ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ 2020 -2025" [PDF]. Retrieved from: https://mindigital.gr/wp-content/uploads/2020/12/%CE%95%CE%B8%CE%BD%CE%B9%CE%BA%CE%B7%CC%81-%CE%A3%CF%84%CF%81%CE%B1%CF%84%CE%B7%CE%B3%CE%B9%CE%BA%CE%B7%CC%81-%CE%9A%CF%85%CE%B2%CE%B5%CF%81%CE%BD%CE%BF%CE%B1%CF%83%CF%86%CE%B1%CC%81%CE%BB%CE%B5%CE%B9%CE%B1%CF%82.pdf (Accessed 17th January 2022)

NCSC-NL (National Cyber Security Centre, The Netherlands), 2021, "National Cybersecurity Agenda". Retrieved from: https://english.ncsc.nl/topics/national-cybersecurity-agenda (Accessed 6th January 2022)

NCSC-NZ (National Cyber Security Centre, New Zealand), nd-a, "Resources". Retrieved from: https://www.ncsc.govt.nz/resources/ (Accessed 6th January 2022)

NCSC-NZ, nd-b, "Charting Your Course: Cyber Security Governance". Retrieved from: https://www.ncsc.govt.nz/guidance/charting-your-course-cyber-security-governance/ (Accessed 6th January 2022)

NCSC-UK (National Cyber Security Centre, UK), 2019, "Cyber security in schools: Practical tips for everyone working in education". Retrieved from:

https://www.ncsc.gov.uk/files/NCSC_NEN%20cards_PRINT-2.pdf (Accessed 6th January 2022)

NCSC-UK, 2021a, "CyberFirst overview". Retrieved from: https://www.ncsc.gov.uk/cyberfirst/overview (Accessed 6th January 2022)

NCSC-UK, 2021b, "Call for Applications (England) – CyberFirst Schools & Colleges". Retrieved from: https://www.ncsc.gov.uk/files/England%20-%20Call%20for%20applications%20CF%20Schools-Colleges.docx (Accessed 6th January 2022)

NCSC-UK, nd-a, "CyberAware". Retrieved from: https://www.ncsc.gov.uk/cyberaware/home (Accessed 6th January 2022)

NCSC-UK, nd-b, "CyberFirst Schools/Colleges". Retrieved from: https://www.ncsc.gov.uk/cyberfirst/cyberfirst-schools (Accessed 6th January 2022)

Netherlands' Ombudsman for Children, nd, "Weet waar je recht op hebt | De Kinderombudsman". Retrieved from: https://www.dekinderombudsman.nl/en/netherlands-ombudsman-for-children (Accessed 6th January 2022)

Netsafe, 2018, "From literacy to fluency to citizenship: Digital Citizenship in Education" [PDF]. Retrieved from: https://www.netsafe.org.nz/the-kit/wp-content/uploads/2018/07/From-literacy-to-fluency-to-citizenship_July-2018.pdf (Accessed 5th January 2022)

Netsafe, 2020, "How to stop online bullying". Retrieved from: https://www.netsafe.org.nz/bullying-abuse-support/ (Accessed 5th January 2022)

Netsafe, 2021, "Managing your digital footprint". Retrieved from: https://www.netsafe.org.nz/managing-your-cv-digital-footprint/ (Accessed 5th January 2022)

Netsafe, nd-a, "Online safety advice & reporting. Netsafe – Providing free online safety advice in New Zealand". Retrieved from: https://www.netsafe.org.nz/ (Accessed 5th January 2022)

Netsafe, nd-b, "Parenting". Retrieved from: https://www.netsafe.org.nz/advice/parenting/ (Accessed 5th January 2022)

Netsafe, nd-c, "Netsafe Schools". Retrieved from: https://www.netsafe.org.nz/the-kit/ (Accessed 5th January 2022)

Netsafe, nd-d, "Netsafe Schools Tiers". Retrieved from: https://www.netsafe.org.nz/the-kit/netsafe-schools/netsafe-schools-tiers/ (Accessed 5th January 2022)

Netsafe, nd-e, "Netsafe Schools: Resources". Retrieved from: https://www.netsafe.org.nz/the-kit/resources/ (Accessed 5th January 2022)

New York State Education Department, 2020, "New York State Computer Science and Digital Fluency Learning Standards, Grades K-12" [PDF]. Retrieved from: http://www.nysed.gov/common/nysed/files/programs/curriculum-instruction/computer-science-digital-fluency-standards-k-12.pdf (Accessed 5th January 2022)

New York State Education Department, nd-a, "Frequently Asked Questions". Retrieved from: http://www.nysed.gov/curriculum-instruction/csdf-frequently-asked-questions (Accessed 6th January 2022)

New York State Education Department, nd-b, "Learning Standards for Health, Physical Education, and Family and Consumer Sciences at Three Levels" [PDF]. Retrieved from: http://www.nysed.gov/common/nysed/files/programs/curriculum-instruction/healthpefacslearningstandards.pdf (Accessed 6th January 2022)

New Zealand Government, 2011, "New Zealand's Cyber Security Strategy" [PDF]. Retrieved from: https://dpmc.govt.nz/sites/default/files/2017-03/nz-cyber-security-strategy-june-2011_0.pdf (Accessed 5th January 2022)

New Zealand Government, 2015, "New Zealand's Cyber Security Strategy 2015" [PDF]. Retrieved from: https://dpmc.govt.nz/sites/default/files/2017-03/nz-cyber-security-strategy-december-2015.pdf (Accessed 5th January 2022)

New Zealand Government, 2019, "New Zealand's Cyber Security Strategy 2019" [PDF]. Retrieved from: https://dpmc.govt.nz/sites/default/files/2019-07/Cyber%20Security%20Strategy.pdf (Accessed 5th January 2022)

NFER (National Foundation for Educational Research), 2014, "Online and at risk: why cyber safeguarding needs to step up". Retrieved from: https://www.nfer.ac.uk/news-events/nfer-blogs/online-and-at-risk-why-cyber-safeguarding-needs-to-step-up/ (Accessed 6th January 2022)

NICCS (National Initiative for Cybersecurity Careers and Studies, US), 2021, "Cybersecurity in the Classroom". Retrieved from: https://niccs.cisa.gov/formal-education/integrating-cybersecurity-classroom (Accessed 6th January 2022)

NICCY (Northern Ireland Commissioner for Children & Young People), nd, "ThinkUKnow parents info and resources". Retrieved from: https://www.niccy.org/parents-and-carers/how-we-can-help-you-parents-and-carers/thinkuknow-parents-info-and-resources/ (Accessed 6th January 2022)

NIST (National Institute of Standards and Technology, US), 2012, "National Initiative for Cybersecurity Education (NICE): Strategic Plan" [PDF]. Retrieved from: https://www.nist.gov/system/files/documents/2020/10/26/2012_NICE-strategic-plan_withcover.pdf (Accessed 5th January 2022)

NIST, 2016, "National Initiative for Cybersecurity Education (NICE): Strategic Plan" [PDF]. Retrieved from:

https://www.nist.gov/system/files/documents/2020/10/26/2016_NICE-strategic-plan_withcover.pdf (Accessed 5th January 2022)

NIST, 2020a, "National Initiative for Cybersecurity Education (NICE): Strategic Plan". Retrieved from: https://www.nist.gov/itl/applied-cybersecurity/nice/about/strategic-plan (Accessed 28th December 2021)

NIST, 2020b, "K12 Cybersecurity Career Awareness for School Counselors and Administrators" [PDF]. Retrieved from: https://www.nist.gov/system/files/documents/2020/04/23/One%20Pager%20Counselors%20FINAL.pdf (Accessed 5th January 2022)

NIST, 2020c, "NICE Interagency Coordinating Council (ICC)". Retrieved from: https://www.nist.gov/itl/applied-cybersecurity/nice/about/interagency-coordinating-council (Accessed 6th January 2022)

NIST, 2021a, "What is Cybersecurity Career Awareness Week?". Retrieved from: https://www.nist.gov/news-events/news/2021/07/join-us-cybersecurity-career-awareness-week-october-18-23 (Accessed 6th January 2022)

NIST, 2021b, "K12 Cybersecurity Education Community of Interest". Retrieved from: https://www.nist.gov/itl/applied-cybersecurity/nice/community/community-coordinating-council/k12-cybersecurity-education (Accessed 6th January 2022)

NIST, 2021c, "NICE Strategic Plan: Implementation Plan" [PDF]. Retrieved from: https://www.nist.gov/system/files/documents/2021/09/23/Implementation%20Plan_22Sep2021.pdf (Accessed 5th January 2022)

NIST, 2021d, "National K12 Cybersecurity Education Roadmap" [PDF]. Retrieved from: https://www.nist.gov/system/files/documents/2021/12/07/K12%20Roadmap_07122021.pdf (Accessed 5th January 2022)

NIST, 2021e, "What is Cybersecurity Career Awareness Week?". Retrieved from: https://www.nist.gov/itl/applied-cybersecurity/nice/events/cybersecurity-career-awareness-week/what-cybersecurity-career (Accessed 28th December 2021)

NIST, 2021f, "NICE Community Coordinating Council". Retrieved from: https://www.nist.gov/itl/applied-cybersecurity/nice/community/community-coordinating-council (Accessed 28th December 2021)

NIST, 2021g, "K12 Cybersecurity Education Community of Interest". Retrieved from: https://www.nist.gov/itl/applied-cybersecurity/nice/community/community-coordinating-council/k12-cybersecurity-education (Accessed 28th December 2021)

NIST, 2021h, "Federal Cybersecurity Workforce Summit". Retrieved from: https://www.nist.gov/itl/applied-cybersecurity/nice/events/federal-cybersecurity-workforce-summit (Accessed 5th January 2022)

Northern Ireland Government, 2021, "Keeping children and young people safe: an Online Safety Strategy for Northern Ireland 2020-2025" [PDF]. Retrieved from:

https://www.health-ni.gov.uk/sites/default/files/publications/health/online-safety-strategy.pdf (Accessed 5th January 2022)

Norwegian Ministries, 2019, "National Cyber Security Strategy for Norway" [PDF]. Retrieved from: https://www.regjeringen.no/contentassets/c57a0733652f47688294934ffd93fc53/national-cyber-security-strategy-for-norway.pdf (Accessed 6th January 2022)

Norwegian Ministry of Education and Research, 2012, "Framework for Basic Skills" [PDF]. Retrieved from: https://www.udir.no/contentassets/fd2d6bfbf2364e1c98b73e030119bd38/framework_for_basic_skills.pdf (Accessed 6th January 2022)

Norwegian Ombudsperson for Children, 2019, "Young People's Thoughts on the Digital Environment" [PDF]. Retrieved from: https://www.barneombudet.no/uploads/documents/Publikasjoner/English/Young-Peoples-Thought-on-the-Digital-Environment.pdf (Accessed 6th January 2022)

Norwegian Ombudsperson for Children, nd, "About the Ombudsperson for Children – Barneombudet". Retrieved from: https://www.barneombudet.no/english/ (Accessed 6th January 2022)

NPCC (National Police Cadet Corps, Singapore), nd, "National Police Cadet Corps, NPCC". Retrieved from: https://www.npcc.org.sg/ (Accessed 6th January 2022)

NSA (National Security Agency, US), nd, "About GenCyber". Retrieved from: https://www.gen-cyber.com/about/ (Accessed 6th January 2022)

NSPCC (National Society for the Prevention of Cruelty to Children, UK), nd-a, "Online Safety Training". Retrieved from: https://learning.nspcc.org.uk/training/online-safety (Accessed 6th January 2022)

NSPCC, nd-b, "Talking to your child about online safety". Retrieved from: https://www.nspcc.org.uk/keeping-children-safe/online-safety/talking-child-online-safety/ (Accessed 6th January 2022)

NSPCC, nd-c, "Keeping children safe online". Retrieved from: https://www.nspcc.org.uk/keeping-children-safe/online-safety/ (Accessed 6th January 2022)

NZQA (New Zealand Qualifications Authority), 2021, "Approved subjects for University Entrance". Retrieved from: https://www.nzqa.govt.nz/qualifications-standards/awards/university-entrance/approved-subjects/ (Accessed 6th January 2022)

NZQA, nd-a, "NCEA levels and certificates". Retrieved from:
Retrieved from: https://www.nzqa.govt.nz/ncea/understanding-ncea/how-ncea-works/ncea-levels-and-certificates/ (Accessed 6th January 2022)

NZQA, nd-b, "NCEA literacy and numeracy requirements". Retrieved from: https://www.nzqa.govt.nz/ncea/subjects/literacy-and-numeracy/level-1-requirements/ (Accessed 6th January 2022)

NZQA, nd-c, "Choosing a course or subjects at school". Retrieved from: https://www.nzqa.govt.nz/studying-in-new-zealand/secondary-school-and-ncea/choosing-a-course-or-subjects-at-school/#heading2-0 (Accessed 6th January 2022).

OASDI (Ontario Association of School Districts International), nd, "The Ontario Curriculum". Retrieved from: https://www.oasdi.ca/k-12-education-in-ontario/curriculum/ (Accessed 6th January 2022)

OCR (Oxford, Cambridge and RSA), 2021a, "GCSE (9–1) Specification: Computer Science" [PDF]. Retrieved from: https://www.ocr.org.uk/Images/558027-specification-gcse-computer-science-j277.pdf (Accessed 6th January 2022)

OCR, 2021b, "AS Level Specification: Computer Science" [PDF]. Retrieved from: https://www.ocr.org.uk/images/170845-specification-accredited-as-level-gce-computer-science-h046.pdf (Accessed 6th January 2022)

OCR, 2021c, "A Level Specification: Computer Science" [PDF]. Retrieved from: https://www.ocr.org.uk/Images/170844-specification-accredited-a-level-gce-computer-science-h446.pdf (Accessed 6th January 2022))

OECD (Organisation for Economic Co-operation and Development), nd, "Digital security". Retrieved from: https://www.oecd.org/sti/ieconomy/digital-security/ (Accessed 6th January 2022)

Ofcom (Office of Communications, UK), 2014, "Children's online behaviour: Issues of risk and trust – Qualitative research findings" [PDF]. Retrieved from: https://www.ofcom.org.uk/__data/assets/pdf_file/0028/95068/Childrens-online-behaviour-issues-of-risk-and-trust.pdf (Accessed 5th January 2022)

Ofcom, 2020, "Making Sense of Media Bulletin" [PDF]. Retrieved from: https://www.ofcom.org.uk/__data/assets/pdf_file/0025/207583/making-sense-of-media-bulletin-november.pdf (Accessed 5th January 2022)

Ofcom, 2021, "Children and parents: Media use and attitudes report 2020-21" [PDF]. Retrieved from: https://www.ofcom.org.uk/__data/assets/pdf_file/0025/217825/children-and-parents-media-use-and-attitudes-report-2020-21.pdf (Accessed 5th January 2022)

Office of Governor of California, 2021, "Newsom Administration Announces First Multi-year Cybersecurity Roadmap to Protect Californians' Privacy and Security". Retrieved from: https://www.gov.ca.gov/2021/10/22/newsom-administration-announces-first-multi-year-cybersecurity-roadmap-to-protect-californians-privacy-and-security/ (Accessed 5th January 2022)

Office of the Parliamentary Council, Canberra, 2017, "Enhancing Online Safety Act 2015" [PDF]. Retrieved from:

https://www.ilo.org/dyn/natlex/docs/ELECTRONIC/105255/128681/F249839433/AUS105255%202017.pdf (Accessed 5th January 2022)

Ofsted, 2021, "School inspection handbook: section 8". Retrieved from: https://www.gov.uk/government/publications/section-8-school-inspection-handbook-eif/school-inspection-handbook-section-8 (Accessed 5th January 2022)

ONS (Office for National Statistics, UK), 2021a, "Children's online behaviour in England and Wales: year ending March 2020". Retrieved from: https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/childrensonlinebehaviourinenglandandwales/yearendingmarch2020 (Accessed 5th January 2022)

ONS, 2021b, "GDP, UK regions and countries: January to March 2021". Retrieved from: https://www.ons.gov.uk/economy/grossdomesticproductgdp/bulletins/gdpukregionsandcountries/januarytomarch2021 (Accessed 5th January 2022)

ONS, nd-a, "cyber crime - Search - Office for National Statistics". Retrieved from: https://www.ons.gov.uk/search?q=cyber+crime (Accessed 25th January 2022)

ONS, nd-b, "cybercrime - Search - Office for National Statistics". Retrieved from: https://www.ons.gov.uk/search?q=cybercrime (Accessed 25th January 2022)

Ontario Ministry of Education, 2008, "The Ontario Curriculum – Grades 10-12: Computer Studies" [PDF]. Retrieved from: http://www.edu.gov.on.ca/eng/curriculum/secondary/computer10to12_2008.pdf (Accessed 5th January 2022)

Ontario Ministry of Education, 2015, "The Ontario Curriculum – Grades 9-12: Health and Physical Education" [PDF]. Retrieved from: http://www.edu.gov.on.ca/eng/curriculum/secondary/health9to12.pdf (Accessed 5th January 2022)

Ontario Ministry of Education, 2019, "The Ontario Curriculum – Grades 1-8: Health and Physical Education" [PDF]. Retrieved from: http://www.edu.gov.on.ca/eng/curriculum/elementary/2019-health-physical-education-grades-1to8.pdf (Accessed5th January 2022)

Ontario Ministry of Education, 2022, "Health and Physical Education in Ontario". Retrieved from: https://www.ontario.ca/page/health-and-physical-education-ontario (Accessed 5th January 2022)

Ontario Ministry of Government and Consumer Services, 2020, "Cyber Security Centre of Excellence". Retrieved from: https://www.ontario.ca/page/cyber-security-centre-excellence (Accessed 5th January 2022)

Ontario Treasury Board Secretariat, 2021, "Ontario's Digital and Data Strategy". Retrieved from: https://www.ontario.ca/page/building-digital-ontario#section-0 (Accessed 5th January 2022)

Oxford Reference, 2022, “unitary state”. Retrieved from: https://www.oxfordreference.com/view/10.1093/oi/authority.20110803110720298 (Accessed 5th January 2022)

Paloato, nd, “Cyber A.C.E.S. Lessons”. Retrieved from: https://start.paloaltonetworks.com/cyber-aces-program-lessons (Accessed 5th January 2022)

Papadopoulous, G., 1998, “Learning for the twenty-first century: issues”, In *Education for the twenty-first century: issues and prospects. Contributions to the work of the International Commission on Education for the twenty-first century*. Paris: United Nations Educational, Scientific and Cultural Organisation. Retrieved from: http://hdl.voced.edu.au/10707/72831 (Accessed 5th January 2022)

Parliament of Canada, 2009, “Bill C-418”. Retrieved from: https://parl.ca/DocumentViewer/en/40-2/bill/C-418/first-reading/page-30 (Accessed 5th January 2022)

Passey, D., 2017, “Computer science (CS) in the compulsory education curriculum: Implications for future research”. *Education and Information Technologies*, 22(2), pp. 421-443. Retrieved from: https://doi.org/10.1007/s10639-016-9475-z (Accessed 5th January 2022)

Pearson Edexcel, 2010, “Edexcel BTEC Level 2 Certificate, BTEC Level 2 Extended Certificate and BTEC Level 2 Diploma in Information Technology (QCF)” [PDF]. Retrieved from: https://qualifications.pearson.com/content/dam/pdf/BTEC-Firsts/Information-Technology/2010/Specification/BF021880-Firsts-in-Information-Technology-L2-spec-for-web-100810.pdf (Accessed 5th January 2022)

Pearson Edexecel, 2018, “What is a BTEC?” [PDF]. Retrieved from: https://qualifications.pearson.com/content/dam/pdf/btec-brand/what-is-a-btec.pdf (Accessed 5th January 2022)

Pearson Edexcel, 2019, “BTEC Level 1/Level 2 Tech Award in Digital Information Technology” [PDF]. Retrieved from: https://qualifications.pearson.com/content/dam/pdf/btec-tec-awards/information-technology/2017/specification-and-sample-assessments/Spec-BTEC-L1-2TECHAWD-DIT.pdf (Accessed 5th January 2022)

Pearson Edexcel, 2020a, “Pearson BTEC Level 3 National Certificate in Computing Specification” [PDF]. Retrieved from: https://qualifications.pearson.com/content/dam/pdf/BTEC-Nationals/computing/2016/specification-and-sample-assessments/9781446940143-BTEC-nat-l3-cert-comp-spec.pdf (Accessed 5th January 2022)

Pearson Edexcel, 2020b, “GCSE (9-1) Computer Science” [PDF]. Retrieved from: https://qualifications.pearson.com/content/dam/pdf/GCSE/Computer%20Science/2020/specification-and-sample-assessments/GCSE_L1_L2_Computer_Science_2020_Specification.pdf (Accessed 5th January 2022)

PHE BC (Physical & Health Education in British Columbia, Canada), nd, "At Home Resources". Retrieved from: https://phebc.ca/at-home-resources/ (Accessed 5th January 2022)

PSHE Association, 2019, "Exploring Cybercrime: KS3 Lesson plans from the National Crime Agency (NCA)". Retrieved from: https://pshe-association.org.uk/curriculum-and-resources/resources/exploring-cybercrime-ks3-lesson-plans-national (Accessed 5th January 2022)

PSHE Association, nd-a, "Home | pshe-association.org.uk". Retrieved from: https://pshe-association.org.uk/ (Accessed 5th January 2022)

PSHE Association, nd-b, "Health and Wellbeing in Wales – how the PSHE Association can support teachers and schools". Retrieved from: https://www.pshe-association.org.uk/curriculum-and-resources/resources/health-and-wellbeing-wales-how-pshe-association (Accessed 5th January 2022)

PSHE Association, nd-c, "Health and Wellbeing education in Scotland". Retrieved from: https://www.pshe-association.org.uk/curriculum-and-resources/resources/health-and-wellbeing-education-scotland (Accessed 5th January 2022)

PTSIC (Portuguese Safer Internet Centre; Centro Internet Segura in Portuguese), nd-a, "O Centro de Sensibilização". Retrieved from: https://www.internetsegura.pt/cis/centro-de-sensibilizacao (Accessed 6th January 2022)

PTSIC, nd-b, "Recursos". Retrieved from: https://www.internetsegura.pt/recursos/all/all (Accessed 6th January 2022)

Prime Minister's Office (UK), 2003, "Countries within a country". Retrieved from: https://webarchive.nationalarchives.gov.uk/ukgwa/20080909013512/http://www.number10.gov.uk/Page823 (Accessed 5th January 2022)

PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses), nd, "PRISMA". Retrieved from: http://prisma-statement.org/ (Accessed 25th January 2022)

Provedor de Justiça, nd, "Provedoria de Justiça". Retrieved from: https://www.provedor-jus.pt/en/ (Accessed 5th January 2022)

Public Policy Institute of California, 2018, "Prioritizing Computer Science in California Schools". Retrieved from: https://www.ppic.org/blog/making-computer-science-priority-california-schools/ (Accessed 5th January 2022)

Public Safety Canada, 2018a, "National Cyber Security Strategy" [PDF]. Retrieved from: https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/ntnl-cbr-scrt-strtg-en.pdf (Accessed 5th January 2022)

Public Safety Canada, 2018b, "National Cyber Security Action Plan (2019-2024)". Retrieved from:

https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg-2019/ (Accessed 5th January 2022

República Portuguesa Educação, 2018a, "5.º ANO | 2.º CICLO DO ENSINO BÁSICOTECNOLOGIAS DA INFORMAÇÃO E COMUNICAÇÃO" [PDF]. Retrieved from: http://www.dge.mec.pt/sites/default/files/Curriculo/Aprendizagens_Essenciais/2_ciclo/5_tic.pdf (Accessed 5th January 2022)

República Portuguesa Educação, 2018b, "6.º ANO | 2.º CICLO DO ENSINO BÁSICOTECNOLOGIAS DA INFORMAÇÃO E COMUNICAÇÃO" [PDF]. Retrieved from: http://www.dge.mec.pt/sites/default/files/Curriculo/Aprendizagens_Essenciais/2_ciclo/6_tic.pdf (Accessed 5th January 2022)

República Portuguesa Educação, 2018c, "7.º ANO | 3.º CICLO DO ENSINO BÁSICOTECNOLOGIAS DA INFORMAÇÃO E COMUNICAÇÃO" [PDF]. Retrieved from: http://www.dge.mec.pt/sites/default/files/Curriculo/Aprendizagens_Essenciais/3_ciclo/tic_3c_7a_ff.pdf (Accessed 5th January 2022)

República Portuguesa Educação, 2018d, "8.º ANO | 3.º CICLO DO ENSINO BÁSICOTECNOLOGIAS DA INFORMAÇÃO E COMUNICAÇÃO" [PDF]. Retrieved from: http://www.dge.mec.pt/sites/default/files/Curriculo/Aprendizagens_Essenciais/3_ciclo/tic_3c_8a_ff.pdf (Accessed 5th January 2022)

República Portuguesa Educação, 2018e, "9.º ANO | 3.º CICLO DO ENSINO BÁSICOTECNOLOGIAS DA INFORMAÇÃO E COMUNICAÇÃO" [PDF]. Retrieved from: http://www.dge.mec.pt/sites/default/files/Curriculo/Aprendizagens_Essenciais/3_ciclo/tic_3c_9a_ff.pdf (Accessed 5th January 2022)

RT.com, 2021, "Australia proposes teaching five year-olds about cybersecurity, while culling 20% of existing curriculum". Retrieved from: https://www.rt.com/news/522736-australia-cybersecurity-primary-education/ (Accessed 5th January 2022)

Safe4Me, nd, "Resources". Retrieved from: https://www.safe4me.co.uk/resources/ (Accessed 5th January 2022)

Safer Internet Day, 2021a, "An Internet Young People Can Trust: How young people are managing reliability and misleading content online" [PDF]. Retrieved from: https://d1xsi6mgo67kia.cloudfront.net/uploads/2021/10/An-Internet-Young-People-Can-Trust-Full-report.pdf (Accessed 5th January 2022)

Safer Internet Day, 2021b, "European Commission". Retrieved from: https://www.saferinternetday.org/en-GB/supporters/european-commission (Accessed 5th January 2022)

SaferInternet4Kids.gr, 2020, "Φυλλάδιο YouTube Kids". Retrieved from: https://saferinternet4kids.gr/fylladia/youtubekids-2/ (Accessed 5th January 2022)

SaferInternet4Kids.gr, 2021, "Φυλλάδιο για την ασφάλεια στο διαδίκτυο για γονείς από το υλικό SID 2021". Retrieved from: https://saferinternet4kids.gr/fylladia/goneis-sid-2021/ (Accessed 5th January 2022)

SaferInternet4Kids.gr, nd, "Webinars". Retrieved from: https://saferinternet4kids.gr/all-webinars/?by-type[]=webinars&submit=%CE%91%CE%BD%CE%B1%CE%B6%CE%AE%CF%84%CE%B7%CF%83%CE%B7 (Accessed 5th January 2022))

Sağlam, R.B., Miller, V. and Franqueira, V.N.L., 2021, "A Systematic Literature Review on Pre-University Cyber Security Education: What to Teach, How to Teach, and Who Should Teach". (Available upon request to the corresponding author via v.franqueira@kent.ac.uk)

SANS Institute, 2022, "SANS Internet Storm Center". Retrieved from: https://isc.sans.edu/ (Accessed 5th January 2022)

SANS Institute, nd, "SANS Cyber Camp for Teens". Retrieved from: https://www.sans.org/cyber-camp/ (Accessed 5th January 2022)

Scholaro Pro, nd, "Education System in South Africa". Retrieved from: https://www.scholaro.com/pro/Countries/South-Africa/Education-System (Accessed 5th January 2022)

Scottish Government, 2017, "Curriculum for Excellence" [PDF]. Retrieved from: https://education.gov.scot/Documents/All-experiencesoutcomes18.pdf (Accessed 5th January 2022)

Scottish Government, 2021a, "Cyber Resilient Scotland: strategic framework – Understanding the Framework". Retrieved from: https://www.gov.scot/publications/strategic-framework-cyber-resilient-scotland/pages/4/ (Accessed 5th January 2022)

Scottish Government, 2021b, "Cyber Resilient Scotland: strategic framework – Annex C: Action Plans 2021-23". Retrieved from: https://www.gov.scot/publications/strategic-framework-cyber-resilient-scotland/pages/7/ (Accessed 5th January 2022)

Scottish Government, nd, "Health and wellbeing in schools". Retrieved from: https://www.gov.scot/policies/schools/wellbeing-in-schools/ (Accessed 5th January 2022)

Sewell, K. and Newman, S., 2014, "What is education?". In *Education Studies: An issues based approach*, pp. 3-11. London: SAGE. Retrieved from: http://dx.doi.org/10.4135/9781526435705.n2 (Accessed 5th January 2022)

SFC (Scottish Funding Council), 2020a, The Financial Sustainability of Colleges and Universities in Scotland. Retrieved from: https://www.sfc.ac.uk/publications-statistics/corporate-publications/2020/SFCCP022020.aspx (Accessed 13th January 2022)

SFC, 2020b, "Review of Regional Strategic Bodies – Overview Report" [PDF]. Retrieved from: http://www.sfc.ac.uk/web/FILES/corporatepublications_sfccp052020/Overarching_RSB_Review_report.pdf (Accessed 13th January 2022)

Sharwood, S., 2021, "Australia proposes teaching cyber-security to five-year-old kids". Retrieved from:

https://www.theregister.com/2021/04/30/eaching_cybersecurity_to_five_year_olds/ (Accessed 5th January 2022)

Six Nations Rugby Ltd, 2022, "Six Nations Rugby | Home". Retrieved from: https://www.sixnationsrugby.com/ (Accessed 5th January 2022)

Smahel, D., MacHackova, H., Mascheroni, G., Dedkova, L., Staksrud, E., Olafsson, K., Livingstone, S. and Hasebrink, U., 2020, "EU Kids Online 2020: Survey results from 19 countries". London School of Economics and Political Science, UK. Retrieved from: https://doi.org/10.21953/lse.47fdeqj01ofo (Accessed 5th January 2022)

SQA (Scottish Qualifications Authority), 2015a, 'National Unit specification: General information, Unit title: Cyber Security Fundamentals (SCQF level 4), Unit code: H9T5 44' [PDF]. Retrieved from: https://www.sqa.org.uk/sqa/files/nq/H9T544.pdf (Accessed 12th January 2022)

SQA, 2015b, 'Group Award Specification for: National Progression Award (NPA) in Cyber Security at SCQF level 4, Group Award Code: GK7W 44. National Progression Award (NPA) in Cyber Security at SCQF level 5, Group Award Code: GK7X 45. National Progression Award (NPA) in Cyber Security at SCQF level 6, Group Award Code: GK7Y 46' [PDF]. Retrieved from: https://www.sqa.org.uk/sqa/files_ccc/GK7W44_GK7X45_GK7Y46.pdf (Accessed 12th January 2022)

SQA, 2015c, 'National Unit specification, General information, Unit title: Data Security (SCQF level 4), Unit code: H9E2 44' [PDF]. Retrieved from: https://www.sqa.org.uk/files/nq/H9E244.pdf (Accessed 12th January 2022)

SQA, 2015d, 'National Unit specification, General information Unit, title: Digital Forensics (SCQF level 4), Unit code: H9J0 44' [PDF]. Retrieved from: https://www.sqa.org.uk/files/nq/H9J044.pdf (Accessed 12th January 2022)

SQA, 2015e, 'National Unit specification General information Unit title: Ethical Hacking (SCQF level 4) Unit code: H9HY 44' [PDF]. Retrieved from: https://www.sqa.org.uk/files/nq/H9HY44.pdf (Accessed 12th January 2022)

SQA, 2015f, 'National Unit specification, General information, Unit title: Data Security (SCQF level 5), Unit code: H9E2 45' [PDF]. Retrieved from: https://www.sqa.org.uk/sqa/files/nq/H9E245.pdf (Accessed 12th January 2022)

SQA, 2015g, 'National Unit specification, General information Unit title: Digital Forensics (SCQF level 5), Unit code: H9J0 45' [PDF]. Retrieved from: https://www.sqa.org.uk/files/nq/H9J045.pdf (Accessed 12th January 2022)

SQA, 2015h, 'National Unit specification, General information, Unit title: Ethical Hacking (SCQF level 5), Unit code: H9HY 45' [PDF]. Retrieved from: https://www.sqa.org.uk/files/nu/H9HY45.pdf (Accessed 12th January 2022)

SQA, 2015i, 'National Unit specification, General information, Unit title: Data Security (SCQF level 6), Unit code: H9E2 46' [PDF]. Retrieved from: https://www.sqa.org.uk/sqa/files/nq/H9E246.pdf (Accessed 12th January 2022)

SQA, 2015j, 'National Unit specification General information Unit title: Digital Forensics (SCQF level 6) Unit code: H9J0 46' [PDF]. Retrieved from: https://www.sqa.org.uk/files/nq/H9J046.pdf (Accessed 12th January 2022)

SQA, 2015k, 'National Unit specification, General information, Unit title: Ethical Hacking (SCQF level 6), Unit code: H9HY 46' [PDF]. Retrieved from: https://www.sqa.org.uk/sqa/files/nu/H9HY46.pdf (Accessed 12th January 2022)

SQA, 2019, "Advanced Higher Computing Science" [PDF]. Retrieved from: https://www.sqa.org.uk/files_ccc/AHCourseSpecComputingScience.pdf (Accessed 5th January 2022)

SQA, 2021a, "National 5 Computing Science" [PDF]. Retrieved from: https://www.sqa.org.uk/files_ccc/ComputingScienceCourseSpecN5.pdf (Accessed 5th January 2022)

SQA, 2021b, "Higher Computing Science" [PDF]. Retrieved from: https://www.sqa.org.uk/files_ccc/HigherCourseSpecComputingScience.pdf (Accessed 5th January 2022)

State Security Agency (South Africa), 2015, "National Cybersecurity Policy Framework for South Africa" [PDF]. Retrieved from: https://www.gov.za/sites/default/files/gcis_document/201512/39475gon609.pdf (Accessed 5th January 2022)

Stop Online Abuse, nd, "Resources". Retrieved from: https://www.stoponlineabuse.org.uk/resources (Accessed 5th January 2022)

STOP. THINK. CONNECT., nd, "About STOP. THINK. CONNECT.". Retrieved from: https://www.stopthinkconnect.org/about (Accessed 5th January 2022)

Student Wellbeing Hub, 2020a, "Resources to build safe, inclusive and connected school communities". Retrieved from: https://studentwellbeinghub.edu.au/ (Accessed 5th January 2022)

Student Wellbeing Hub, 2020b, "Cyber A.C.E.S. Program (5-15 years)". Retrieved from: https://studentwellbeinghub.edu.au/educators/resources/cyber-aces-program-5-15-years/ (Accessed 5th January 2022)

SWGfL (South West Grid for Learning, UK), nd-a, "SWGfL - Safety & Security Online". Retrieved from: https://swgfl.org.uk/ (Accessed 5th January 2022)

SWGfL, nd-b, "Quick Start Guide: How to use 360safe". Retrieved from: https://360safe.org.uk/overview/start-guide/ (Accessed 5th January 2022)

SWGfL, nd-c, "Online Safety Self-Review Tool for Schools | 360safe". Retrieved from: http://www.360safe.org.uk/ (Accessed 7th February 2022)

SWGfL, nd-d, "Online Safety Self-Review Tool | 360 Early Years". Retrieved from: https://360earlyyears.org.uk/ (Accessed 7th February 2022)

SWGfL, nd-e, "What is ProjectEVOLVE?". Retrieved from: https://projectevolve.co.uk/about/ (Accessed 5th January 2022)

Texas Higher Education Coordinating Board, nd, "Texas College and Career Readiness Standards". Retrieved from: https://www.highered.texas.gov/institutional-resources-programs/public-community-technical-state-colleges/texas-college-and-career-readiness-standards/ (Accessed 5th January 2022)

TEA (Texas Education Agency), 2012a, "Chapter 126. Texas Essential Knowledge and Skills for Technology Applications: Subchapter A. Elementary" [PDF]. Retrieved from: https://tea.texas.gov/sites/default/files/ch126a.pdf (Accessed 5th January 2022)

TEA, 2012b, "Chapter 126. Texas Essential Knowledge and Skills for Technology Applications: Subchapter B. Middle School" [PDF]. Retrieved from: https://tea.texas.gov/sites/default/files/ch126b.pdf (Accessed 5th January 2022)

TEA, 2021, "Chapter 74. Curriculum Requirements: Subchapter A. Required Curriculum" [PDF]. Retrieved from: https://tea.texas.gov/sites/default/files/ch074a.pdf (Accessed 5th January 2022)

TheSchoolRun.com, nd-a, "An overview of the Welsh education system". Retrieved from: https://www.theschoolrun.com/overview-welsh-education-system (Accessed 5th January 2022)

TheSchoolRun.com, nd-b, "What are national curriculum levels?". Retrieved from: https://www.theschoolrun.com/what-are-national-curriculum-levels (Accessed 6th January 2022)

ThinkUKnow, nd-a, "Welcome to ThinkUKnow". Retrieved from: https://www.thinkuknow.co.uk/ (Accessed 5th January 2022)

ThinkUKnow, nd-b, "4-7s Homepage". Retrieved from: https://www.thinkuknow.co.uk/4_7/ (Accessed 5th January 2022)

ThinkUKnow, nd-c, "Jessie & Friends: online safety education for 4-7s". Retrieved from: https://www.thinkuknow.co.uk/parents/jessie-and-friends/ (Accessed 5th January 2022)

ThinkUKnow, nd-d, "Jessie & Friends: online safety education for 4-7s". Retrieved from: https://www.thinkuknow.co.uk/professionals/resources/jessie-and-friends/ (Accessed 5th January 2022)

ThinkUKnow, nd-e, "Think Know 8-10s". Retrieved from: https://www.thinkuknow.co.uk/8_10/ (Accessed 5th January 2022)

ThinkUKnow, nd-f, "Band Runner for 8-10 year olds". Retrieved from: https://www.thinkuknow.co.uk/parents/articles/band-runner/ (Accessed 5th January 2022)

ThinkUKnow, nd-g, "Band Runner game and website". Retrieved from: https://www.thinkuknow.co.uk/professionals/resources/band-runner/ (Accessed 5th January 2022)

ThinkUKnow, nd-h, "ThinkUKnow – home". Retrieved from: https://www.thinkuknow.co.uk/11_13/ (Accessed 5th January 2022)

ThinkUKnow, nd-i, "ThinkUKnow – home". Retrieved from: https://www.thinkuknow.co.uk/14_plus/ (Accessed 5th January 2022)

Trevallion, D., 2014, "Connecting to Australia's first digital technology curriculum". *The Conversation*. Retrieved from: https://theconversation.com/connecting-to-australias-first-digital-technology-curriculum-23507 (Accessed 5th January 2022)

UCAS.com, nd, "BTEC Diplomas". Retrieved from: https://www.ucas.com/further-education/post-16-qualifications/qualifications-you-can-take/btec-diplomas (Accessed 5th January 2022)

UK Government, 2011, "Cyber Security Strategy". Retrieved from: https://www.gov.uk/government/publications/cyber-security-strategy (Accessed 5th January 2022)

UK Government, 2016a, "The UK Cyber Security Strategy 2011-2016: annual report". Retrieved from: https://www.gov.uk/government/publications/the-uk-cyber-security-strategy-2011-2016-annual-report (Accessed 5th January 2022)

UK Government, 2016b, "National Cyber Security Strategy 2016 to 2021". Last updated 11th September 2017. Retrieved from: https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021 (Accessed 5th January 2022)

UK Government, 2021a, "Landmark laws to keep children safe, stop racial hate and protect democracy online published". Retrieved from: https://www.gov.uk/government/news/landmark-laws-to-keep-children-safe-stop-racial-hate-and-protect-democracy-online-published (Accessed 5th January 2022)

UK Government, 2021b, "Online media literacy resources". Retrieved from: https://www.gov.uk/guidance/online-media-literacy-resources (Accessed 7th February 2022)

UK Government, nd-a, "The national curriculum". Retrieved from: https://www.gov.uk/national-curriculum (Accessed 5th January 2022)

UK Government, nd-b, "UK Council for Child Internet Safety (UKCCIS)". Retrieved from: https://www.gov.uk/government/groups/uk-council-for-child-internet-safety-ukccis (Accessed 5th January 2022)

UK Government, nd-c, "School leaving age". Retrieved from: https://www.gov.uk/know-when-you-can-leave-school (Accessed 5th January 2022)

UK Government, nd-d "Digital Production, Design and Development". Retrieved from: https://www.tlevels.gov.uk/students/subjects/digital-production-design-development (Accessed 5th January 2022)

UK Government, nd-e, "Digital Support Services". Retrieved from: https://www.tlevels.gov.uk/students/subjects/digital-support-services (Accessed 5th January 2022)

UK Parliament, 2000, "Learning and Skills Act 2000". Retrieved from: https://www.legislation.gov.uk/ukpga/2000/21/contents (Accessed 5th January 2022)

UK Parliament, 2010, "Academies Act 2010". Retrieved from: https://www.legislation.gov.uk/ukpga/2010/32/contents (Accessed 5th January 2022)

UK Parliament, 2018, "Data Protection Act 2018". Available at: https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted (Accessed 5th January 2022)

UK Safer Internet Centre, 2018, "Education for a Connected World". Retrieved from: https://www.saferinternet.org.uk/blog/education-connected-world (Accessed 5th January 2022)

UK Safer Internet Centre, 2021d, "Safer Internet Day officially breaks GUINNESS WORLD RECORD™". Retrieved from: https://www.saferinternet.org.uk/blog/safer-internet-day-officially-breaks-guinness-world-record%E2%84%A2 (Accessed on 5th January 2022)

UK Safer Internet Centre, 2021b, "Young People's Charter". Retrieved from: https://www.saferinternet.org.uk/safer-internet-day/safer-internet-day-2021/young-peoples-charter (Accessed 5th January 2022)

UK Safer Internet Centre, nd-a, "Resources for 3-11s". Retrieved from: https://www.saferinternet.org.uk/advice-centre/young-people/resources-3-11s (Accessed 5th January 2022)

UK Safer Internet Centre, nd-b, "Resources for 11-19s". Retrieved from: https://www.saferinternet.org.uk/advice-centre/young-people/resources-11-19s (Accessed 5th January 2022)

UK Safer Internet Centre, nd-c, "About - UK Safer Internet Centre". Retrived from: https://saferinternet.org.uk/about (Accessed 8th Febuary 2022)

UKCCIS (UK Council for Child Internet Safety), 2017, "Tackling race and faith targeted bullying face to face and online: A short guide for schools" [PDF]. Retrieved from: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/759004/Tackling_race_and_faith_targeted_bullying_face_to_face_and_online_-_a_guide.pdf (Accessed 5th January 2022)

UKCIS (UK Council for Internet Safety), 2019a, "Digital Resilience Framework: A framework and tool for organisations, communities and groups to help people build resilience in their digital life" [PDF]. Retrieved from: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/831217/UKCIS_Digital_Resilience_Framework.pdf (Accessed 24th January 2022)

UKCIS, 2019b, "Digital Resilience Working Group Policy Paper" [PDF]. Retrieved from: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/831218/UKCIS_Digital_Resilience_Working_Group_Policy_Paper.pdf (Accessed 24th January 2022)

UKCIS, 2020, "Education for a Connected World – 2020 edition" [PDF]. Retrieved from: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/896323/UKCIS_Education_for_a_Connected_World_.pdf (Accessed 5th January 2022)

UKCIS, nd, "About us". Retrieved from: https://www.gov.uk/government/organisations/uk-council-for-internet-safety/about (Accessed 5th January 2022)

UKCIS Digital Resilience Working Group, nd, "The digital resilience framework". Retrieved from: https://www.drwg.org.uk/the-framework (Accessed 24th January 2022)

UNESCO (United Nations Educational, Scientific and Cultural Organization), 2011, "International Standard Classification of Education ISCED 2011" [PDF]. Retrieved from: http://uis.unesco.org/sites/default/files/documents/international-standard-classification-of-education-isced-2011-en.pdf (Accessed 5th January 2022)

UNICEF, nd-a, "About UNICEF". Retrieved from: https://www.unicef.org/about-unicef (Accessed 7th February 2022)

UNICEF, nd-b, "Protecting children online". Retrieved from: https://www.unicef.org/protection/violence-against-children-online (Accessed 7th February 2022)

UNICEF, nd-c, "Global Kids Online | Children's rights in the digital age". Retrieved from: http://globalkidsonline.net/ (Accessed 8th February 2022)

UNICEF, nd-d, "Disrupting harm". Retrieved from: https://www.unicef-irc.org/research/disrupting-harm (Accessed 8th February 2022)

United States Congress, 1965, "An act to strengthen and improve educational quality and educational opportunities in the United States of American's elementary and secondary schools" [PDF]. Retrieved from: https://www.govinfo.gov/content/pkg/STATUTE-79/pdf/STATUTE-79-Pg27.pdf (Accessed 5th January 2022)

United States Congress, 2015, "Every Student Succeeds Act 2015" [PDF]. Retrieved from: https://www.congress.gov/114/plaws/publ95/PLAW-114publ95.pdf (Accessed 5th January 2022)

U.S. Department of Defense, 2018, "Department of Defense Cyber Strategy" [PDF]. Retrieved from: https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF (Accessed 5th January 2022)

U.S. Department of Education. 2008a, “Structure of the U.S. Education System: Curriculum and Content Standards”. Retrieved from: https://www2.ed.gov/about/offices/list/ous/international/usnei/us/standards.doc (Accessed 5th January 2022)

U.S. Department of Education. 2008b, “Organization of U.S. Education: The School Level”. Retrieved from: https://www2.ed.gov/about/offices/list/ous/international/usnei/us/schoollevel.doc (Accessed 5th January 2022)

U.S. Department of Education, 2021, “The Federal Role in Education”. Retrieved from: https://www2.ed.gov/about/overview/fed/role.html (Accessed 5th January 2022)

U.S. Department for Education, nd, “Structure of U.S. Education”. Retrieved from: https://www.ed.gov/about/offices/list/ous/international/usnei/us/edlite-structure-us.html (Accessed 5th January 2022)

U.S. Department for Homeland Security, 2018, “Cybersecurity Strategy” [PDF]. Retrieved from: https://www.dhs.gov/sites/default/files/publications/DHS-Cybersecurity-Strategy_1.pdf (Accessed 5th January 2022)

Utah Department of Human Services, nd, “Care Concerns”. Retrieved from: https://hs.utah.gov/services/care-concerns (Accessed 5th January 2022)

U.S. Department of State, nd, “About Us – Office of the Coordinator for Cyber Issues”. Retrieved from: https://2017-2021.state.gov/about-us-office-of-the-coordinator-for-cyber-issues/ (Accessed 5th January 2022)

Utah Education Network, 2019a, “K-5 Computer Science”. Retrieved from: https://www.uen.org/core/core.do?courseNum=512 (Accessed 5th January 2022)

Utah Education Network, 2019b, “6-12 Computer Science”. Retrieved from: https://www.uen.org/core/core.do?courseNum=612 (Accessed 5th January 2022)

Utdanningsdirektoratet, nd, “Core Curriculum: The Basic Skills”. Retrieved from: https://www.udir.no/lk20/overordnet-del/prinsipper-for-laring-utvikling-og-danning/grunnleggende-ferdigheter/?lang=eng (Accessed 7th February 2022)

Vuorikari, R., Punie, Y., Carretero, S., and Van den Brande, L., 2017, “DigComp 2.0: The Digital Competence Framework for Citizens”. JRC (Joint Research Centre) Science for Policy Report EUR 27948 EN. Luxembourg Publication Office of the European Union. Retrieved from: https://doi.org/10.2791/11517 (Accessed 5th January 2022)

Welsh Assembly Government, 2008, “Information and communication technology in the National Curriculum for Wales” [PDF]. Retrieved from: https://hwb.gov.wales/api/storage/4edae1df-9feb-4a44-95be-8060f7916cde/ict-in-the-national-curriculum-for-wales.pdf (Accessed 5th January 2022)

Welsh Assembly Government, 2009, "Information and communication technology at Key Stage 4: Guidance for schools" [PDF]. Retrieved from: https://hwb.gov.wales/api/storage/b83b9ca6-8bd6-475e-a2ec-6e65cecbb7cd/information-and-communication-technology-at-key-stage-4.pdf (Accessed 5th January 2022)

Welsh Government, 2015, "Curriculum for Wales: Foundation Phase Framework (Revised 2015)" [PDF]. Retrieved from: https://hwb.gov.wales/api/storage/d5d8e39c-b534-40cb-a3f5-7e2e126d8077/foundation-phase-framework.pdf (Accessed 5th January 2022)

Welsh Government, 2020a, "Health and Well-being". Retrieved from: https://hwb.gov.wales/curriculum-for-wales/health-and-well-being/ (Accessed 5th January 2022)

Welsh Government, 2020b, "Health and Well-being: 4. Descriptions of learning". Retrieved from: https://hwb.gov.wales/curriculum-for-wales/health-and-well-being/descriptions-of-learning/ (Accessed 5th January 2022)

Welsh Government, 2020c, "International strategy for Wales". Retrieved from: https://gov.wales/international-strategy-for-wales (Accessed 12th Jan 2022)

Western Cape Government, nd, "Commissioner for Children | Western Cape". Retrieved from: https://www.westerncape.gov.za/childrens-commissioner/ (Accessed 5th January 2022)

WeTeach, 2020, "An Introductory High School Computer Science Curriculum" [PDF]. Retrieved from: https://utexas.box.com/shared/static/uhboah5l23jgfonxtmxmoor2agu8dfpe.pdf (Accessed 5th January 2022)

The White House, 2018, "National Cyber Strategy of the United States of America" [PDF]. Retrieved from: https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf (Accessed 5th January 2022)

Wikipedia, nd-a, "Countries of the United Kingdom". Retrieved from: https://en.wikipedia.org/wiki/Countries_of_the_United_Kingdom#Acts_of_Parliament (Accessed 5th January 2022)

Wikipedia, nd-b, "National Police Cadet Corps – Wikipedia". Retrieved from: https://en.wikipedia.org/wiki/National_Police_Cadet_Corps (Accessed 5th January 2022)

Wikipedia, nd-c, "Children's ombudsman: 1.18 Greece". Retrieved from: https://en.wikipedia.org/wiki/Children's_ombudsman#Greece (Accessed 16th January 2022)

Wikipedia, nd-d, Ministry of Citizen Protection (Greece). Retrieved from: https://en.wikipedia.org/wiki/Ministry_of_Citizen_Protection_(Greece) (Accessed 16th January 2022)

Wikipedia, nd-e, Ministry of Interior (Greece). Retrieved from: https://en.wikipedia.org/wiki/Ministry_of_the_Interior_(Greece) (Accessed 16th January 2022)

Wise.com, 2017, "The Mexican education system: An overview". Retrieved from: https://wise.com/gb/blog/mexican-education-overview (Accessed 5th January 2022)

WJEC (Welsh Joint Education Committee), 2019a, "WJEC GCSE in Computer Science" [PDF]. Retrieved from: https://www.wjec.co.uk/media/jymdzl0a/wjec-gcse-comp-science-spec-2017-e-04-05-2020.pdf (Accessed 5th January 2022)

WJEC, 2019b, "WJEC GCE AS/A LEVEL in Computer Science" [PDF]. Version 2. Retrieved from: https://www.wjec.co.uk/media/wl4kj5l1/wjec-gce-computer-science-spec-from-2015.pdf (Accessed 5th January 2022)

Appendix A: List of Interviewees

Stage 3 of the reported research is based on 21 interviews with 24 interviewees. For the following three interviews, more than one interviewee was involved:

1. An interview with three interviewees from the ITU
    - Yasmine Idrissi Azouzzi, Cybersecurity Policy Officer, ITU
    - Fanny Rotino, Child Online Protection Officer, ITU
    - Caroline Troein, Lead Cyber Security Researcher, ITU
2. An interview with three interviewees from Estonia
    - Kristjan Kaskman, Cyber Security Research and Development Advisor, Department of National Cyber Security, Estonia
    - Birgy Lorenz, Researcher at Tallinn University of Technology, School of Information Technologies, Department of Software Science and Development manager (IT) at Pelgulinna Gymnasium, Estonia
    - Tiina Pau, Curriculum Specialist, Ministry of Education and Research, Estonia
3. An interview with two interviewees from the CyberFirst team, HM Government, UK

For the other 16 interviews, only one interviewee was involved. All those interviewees are listed below:

4. Julia Adamson, Director of Education, BCS, The Chartered Institute for IT, UK
5. Ken Corish, Online Safety Director and SMT member, South West Grid for Learning (SWGfL), UK
6. A technologies curriculum specialist, Australian Curriculum, Assessment and Reporting Authority (ACARA), Australia
7. Joe Dolan, Head of NI Cyber Security Centre, Northern Ireland, UK
8. Anahiby Anyel Becerril Gil, Specialist Professor in Digital Law and Cybersecurity, Mexico
9. A Head of Department, HM Government, UK
10. Elmarie Kritzinger, Professor, University of South Africa, South Africa
11. Shin Yi Lim, Senior Assistant Director, Ecosystem Development, Cyber Security Agency of Singapore, Singapore
12. Cliff Manning, Research and Development Director, Parent Zone, UK
13. Neil Melhuish, Director of Research and Policy, Netsafe, New Zealand
14. Pedro Mendonça, Cybersecurity Observatory Coordinator; Trainer and content developer for Awareness and Training (Development and Innovation Unit), CNCS (Portuguese National Cybersecurity Center), Portugal
15. Georgios Papaprodromou, Police General (ret) Hellenic Police and Expert in Cyber crime, Greece
16. Remco Pijpers, Strategic Advisor Digital Literacy: Ethics, Kennisnet, the Netherlands
17. Daniel Sellers, Cyber Resilience Learning and Skills Coordinator, Scottish Government, UK
18. Karoline Hultman Tømte, Head of Partnership and Government Relations, Norwegian Centre for Information Security, Norway
19. Rich Williams, Assistant Headteacher and Specialism Lead for Cyber & Digital, Berkley Green UTC, UK

Appendix B: Interview Questions

1. Can you confirm your role, affiliation, and country you represent?
2. How does your country's strategies, policies and initiatives recognise and promote cyber security skill development for pre-university education at schools and colleges?
3. How was/is your country's current national curricula (being) developed to include cyber security related content for different pre-university age groups? (For interviewees representing private schools and colleges who do not follow the curricula, the word "national" will be removed or changed.)
4. How are cyber security-related extracurricular activities delivered at schools/colleges, or delivered via other educational programmes targeted at young people in your country?
5. How are cyber security educational content and activities received by teachers, pupils and parents in your country?
6. What are the main challenges faced by the government, schools, teachers and parents in your country to improve cyber security skills among school children and young people?
7. How do schools work with other organisations (e.g., universities, national authorities, and cyber security industry) to complement their own cyber security educational activities and capacity building?
8. How can current national curricula and cyber security educational activities be further improved in the future in your country?

Appendix C: The Coding Scheme Used in Stage 3

Theme	Code name	Description/code includes
I = Implementation and organisation of cyber education	Fragmentation	Policies or initiatives or strategies which are implemented piecemeal, either per state or by third parties e.g., charities and sometimes with little ongoing support
	Idiosyncrasy	The uneven application of opportunities across schools and districts due to teacher choice
	Responsibility	Questions around who is responsible, or directive about who is responsible.
	Ad-hoc nature of input and initiatives	Little events vs solid and consistent curricula and initiatives
	Lack of continuity	A distinct lack of ongoing support for a scheme, policy or programme, or changes to provision across time.
	Practice not following policy	Where there is policy directing action and input, however the reality is somewhat different to this.
	Accessibility	Including different access to provision due to reasons outside teacher choice – for example different access between private and public schools, provision across rural schools compared to city schools, access to devices and Wi-Fi.
	Collaboration and engagement of multiple stakeholders	Including: industry and schools working together, necessity of including multiple stakeholders and voices in guidance and frameworks.
	How we measure outcomes	How outcomes are measured, if they are
	Standardisation	Including: the need for a centralised education, where things are done the same across a context or country and the need for standardisation
	Dissemination	How we get the information about cyber security programmes and initiatives, and broader information about cyber, to the students
P = Professional. Cyber-security professional development and industry needs	Culture and nature of cyber security	Describing the culture of industry, the changing nature of industry and the speed at which is changes
	Awareness of cyber security	Awareness of pupils, teachers and teachers of cyber careers and skills, or lack of (including non-cyber specific careers)
	Relationships with industry	Industry giving talks in schools, industry sponsoring schools, industry involvement
	Industry standards	Certifications, standards and demands from industry
	Issues with CompSci focus	Including over focus on coding/computational thinking as opposed to developing practical skills, stopping ICT GCSE for Computer Science GCSE (one example in UK context), lack of focus on broader ICT issues in education.
	Paths into cyber careers	The variety of ways students can enter cyber careers and what works in different contexts
	Gaps between industry need and taught skills	Marked gaps between what industry needs and the skills taught in schools
	Competitive edge in the market	Where having a cyber offer is seen as a draw in terms of helping the cyber pipeline, especially in comparison to other countries

B = Barriers to effective cyber education (Skills, Cultural, financial)	Priorities	Priorities in regards to creation and actioning of policy related to cyber, including government, educational and competing
	Perceived tech savviness	Understanding of technology by parents, understanding of online safety by children and young people
	Lack of teacher training and skills	The reported lack of skills teachers have in regards to cyber, and the lack of training and CPD they receive.
	Funding/monetary support	Where funding or money supports a scheme, initiative or programme and the impact on it
	Lack of technology skills in schools.	Where students do not have technological skills.
	Student demand	Including student interest and how oversubscribed activities are
	Parent and teacher reception	How the initiatives and programmes are received by parents and teachers
	Diversity (girls/gender)	A note on the lack of women, girls and other marginalised genders in cyber and efforts to change this.
	Diversity (other)	A note on the lack of other marginalised groups in cyber (e.g. disabled people, neurodivergent people, people from poorer socio-economic backgrounds) and efforts to change this.
	Stereotypes	Stereotypes which inform who we think cyber is for and how cyber looks
C = Content taught in cyber education	Resources	Including teaching plans, specialist teachers, labs, and communities of practice for teachers (e.g. computing at school)
	Curriculum provision	Provision on the curriculum on cyber content
	Extra-curricular provision	Extra-curricular provision of cyber content
	Complementing provision	Where extra-curricular content supports curricular content, including external links or events or support from clubs or brigade groups (e.g., scouts, guides, boy's brigade)
	Not targeting under 18s	Strategy, initiative or policy not targeting under 18s
	Higher/further education content/curriculum	Initiatives for those over 18, higher/further education content
	Training provision	Where training for staff and/or parents is provided (ITT and CPD included) on cyber or online safety.
	Flexible and broad curriculum required	This includes problems with fixed narrow curricula across cultural contexts, and the provision of loose curricula or guidance which can be adapted to schools within their contexts.
	How we teach	Pedagogical and teaching methods including gamifying activities
	How we include cyber	Including how it is embedded into the curriculum
	What we teach	Curricula content and what we teach in regards to cyber security/online safety
	What has worked	Where a programme or initiative has had positive outcomes and continues to work well
	Risks for young people and children	Including: risks of using the internet, risks of using devices.
	Non-mandatory nature of Cyber education	Where cyber security education is not mandatory for qualifications or to be taught.

[END]