Pre-University Cyber Security Education: A Global Comparison of National Curricula

Krysia E. Waldock[1]

Institute of Cyber Security for Society (iCSS) & School of Computing, University of Kent, Canterbury, CT2 7NP, UK School of Social Policy, Sociology and Social Research (SSPSSR), University of Kent, Canterbury, CT2 7NF, UK

Virginia N. L. Franqueira[2]

Institute of Cyber Security for Society (iCSS) & School of Computing, University of Kent, Canterbury, CT2 7NP, UK

Vincent Miller[3]

School of Social Policy, Sociology and Social Research (SSPSSR), University of Kent, Canterbury, CT2 7NF, UK

Shujun Li[4]

Institute of Cyber Security for Society (iCSS) & School of Computing, University of Kent, Canterbury, CT2 7NP, UK

Abstract

Objectives. There is growing recognition of the importance of cyber security education (including online safety and privacy) at pre-university level (i.e., up to age 18). Previous studies have focused on the cyber security curricula of single countries in isolation, or Computer Science when comparing multiple countries. In light of this gap in the literature, the aim of this study was to compare the curricula of 12 countries, in particular focusing on the similarities and differences. The research questions that guided our study were: (1) What are the similarities and differences in cyber security education curricula across countries? (2) What approaches do countries take to including cyber security education in their curricula?

Study Method. We undertook desk research of the education programs of 12 countries, i.e., Australia, Canada, the Netherlands, New Zealand, Norway, Singapore, South Africa, the UK (England, Northern Ireland, Scotland, and Wales) and the USA, in order to compare their cyber security curriculum or framework at the national level. We undertook desk research to source curricula and also undertook a content analysis to discover patterns in the content covered in the curricula.

Findings. The main findings include the following. Four approaches to the coverage and organization of cyber security education were observed: covered in a single technical subject only, covered in a single non-technical subject only, covered in one technical and one non-technical subject, and covered in all or a range of subjects. We also identified three approaches to cyber security education mandates: a lack of mandate, a mandate where regions can opt in or out, and a mandate with prescribed requirements although schools still have the freedom to pick-and-chose the requirements to implement and at what extent, according to local resources and capabilities.

Conclusions. Policymakers can benefit from the findings and recommendations of this study to make decisions towards a more comprehensive coverage of cyber security in pre-university education, including technical and socio-technical aspects along a range of subjects.

Keywords

Cyber security; pre-university; education; curriculum; children.

[1] ORCID: 0000-0001-9631-3930

[2] Corresponding author: v.franqueira@kent.ac.uk – ORCID: 0000-0003-1332-9115

[3] ORCID: 0000-0002-7193-5378

[4] Corresponding author: s.j.li@kent.ac.uk – ORCID: 0000-0001-5628-7328

1 INTRODUCTION

There is an increasing recognition that children need to learn about cyber security, including more technical topics such as online safety and privacy. Two factors contribute prominently to this. First, there is the growing number of children accessing online content and using digital devices and applications from a young age. According to a recent survey by the UK's Office of Communications, 97% of children aged 3-17 went online in 2022, raising concerns regarding online security and safety risks as a result [60]. A 2017 report from the United Nations International Children's Emergency Fund stated that under-18s accounted for one in three internet users globally [78]. Second, there is an increasing demand for cyber security professionals to fulfil the market needs. The cyber security sector is growing worldwide, with 4.1 million cyber security professionals globally in 2021 [71]. A study by the UK Government's Department for Digital, Culture Media & Sport indicated that almost 700,000 private sector businesses surveyed in the UK (51%, n=697,000) experienced a lack of basic technical cyber security skills in the previous year [22]. The report estimated an annual shortage of cyber security professionals in the UK of around 14,100 [22].

One way to tackle the need to build children and young people's capacity and skills for awareness of online risks, and to raise their attention to career paths in cyber security-related roles, is through the provision of cyber security and online safety content in schools at a pre-university level.

Key terms relating to cyber security and online safety are not consistently used and differ across different countries, regions and cultural contexts. We use definitions from the International Telecommunication Union (ITU) and the National Cyber Security Centre (NCSC, UK) to frame this central concept in our paper. Cyber security has been defined by ITU as "the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets" [38]. The UK's NCSC defines cyber security as the "protection of devices, services and personal information" [54], often focusing on more technical aspects. The above two definitions are largely aligned, so we use them to ground our paper. Note that the ITU is a United Nations agency playing an important role in defining international standards on telecommunications and ICT (information and communication technology) in general, therefore their definition is more widely accepted across different countries. Similarly, as the UK's public-facing authority on cyber security, the NCSC's definition is a good example of authoritative definitions provided by a governmental body for the general public. Some other terms related to cyber security include information security, computer security, data security, network security and systems security, describing different sub-areas or aspects of cyber security. The above definitions have a problem of not being able to cover socio-technical aspects completely, especially 'online safety' which refers to an important aspect of cyber security: the online protection of people. To cover online safety more properly, we chose to use the definition from SWGfL, a non-governmental body (NGO) in the UK co-leading the UK Safer Internet Centre[5], which says "online Safety protects the people … from harm by the devices and networks (and therefore third parties) through awareness, education, information and technology" [74]. Other equivalent terms to online safety include internet safety, e-safety, cyber safety, and digital safety. The remainder of the paper refers to both cyber security (narrow sense) and online safety together in curricula through the broader global term of "cyber security".

1.1 Research Problem

Cyber security education continues to attain research interest globally. Many studies focus on other aspects of teaching cyber security within pre-university settings, such as teaching methods [1], the impact of cyber security education or training sessions for pupils [61] or teachers' experiences of teaching cyber security [62]. While attention has been paid to pre-university cyber security education, existing work on the subject has focused primarily on developments in singular countries in isolation, e.g., England [72], Estonia [45], Scotland [43], the UK [62] and the USA [15, 63]. One study compared the maturity of pre-university cyber security education in the UK and South Africa, highlighting differences between countries with diverse cultural and socio-economic backgrounds [42]. Both countries were making efforts to increase awareness of cyber security in schools, but only in the UK cyber security was found to be embedded within the national curricula.

[5] https://saferinternet.org.uk/

Furthermore, studies comparing multiple countries focusing on curricula have also been undertaken in Computer Science more broadly centered both on wider geographical areas e.g., Europe [34]; the USA [36], Africa [76] and globally [37, 59]. These are however not specific to cyber security education. In a global comparison of curricula, case studies were used from 12 countries (Finland, France, Germany, India, Italy, Israel, Korea, Russia, New Zealand, Sweden, UK, USA) [37]. Deductive coding was used to compare the content of Computer Science education, finding different approaches to teaching Computer Science (in a separate subject or embedded into other subjects). The most commonly addressed goal of Computer Science curricula found from coding the case studies was digital literacy (10 countries: Finland, Germany, India, Italy, Korea, New Zealand, Russia, Sweden, UK, USA). One further study compared the Computer Science enacted curriculum (what is taught by teachers in the classroom) of 7 countries (Australia, England, Ireland, Italy, Malta, Scotland and USA) [33]. Information captured on the intended curricula highlighted some countries provided Computer Science content within their curricula (Australia, England, Malta, Scotland), in others it appeared to be either the teacher's decision (Ireland) or dependent on the type of school pupils attend (Italy) [33].

Although there is a lot of discussion on Computer Science curricula, there is a lack of comparative studies focusing on cyber security curricula specifically.

1.2 Study Aims and Research Questions

This study aims to fill the above-mentioned research gap through comparing the curricula of multiple countries. The aim of our work was to explore cyber security education curricula at a pre-university level across multiple countries. Although focusing on one singular country as a case study may allow for in depth exploration of the phenomenon at hand, comparing of curricula allows for similarities and differences to be gleaned. To the best of our knowledge, this is first attempt to compare cyber security curricula specifically across a large number of countries worldwide, across different continents, government systems, and socio-cultural backgrounds.

The following research questions guided this study:

1. What are the similarities and differences in cyber security education curricula across countries?
2. What approaches do countries take to including cyber security education in their curricula?

2 METHODOLOGY

The study involved a 3-steps methodology, described below.

Stage 1. Select sample of countries

Countries were identified for desk research of curricula. They were deemed suitable for inclusion if curricula information was publicly available in English. This could be because English is the official language of the country and therefore documentation is published in English, or because an official translation is accessible online and provided by a governmental organization.

In addition, we also endeavored to cover a wide variety of countries in different continents, and across different cultural and socio-economic contexts. As a result, we included countries with both developed (Australia, Canada, the Netherlands, New Zealand, Norway, the UK (4 countries) and the USA) and developing economies (Singapore and South Africa) [79]. Some degree of geographic diversity is observable from the sample we used, with countries from Asia, North America and Africa as well as Europe and the UK. However, half of the sample (i.e., 6 of the countries studied) are based in Europe and the UK.

There were a range of official languages used by the countries upon which we focus, and some of the countries have multiple official languages (i.e., Canada, Singapore, South Africa and New Zealand); however, only the English curricula and frameworks were considered for this study.

Stage 2. Study educational system for sample of countries

Desk research was undertaken to understand how pre-university cyber security education is structured and delivered in the countries in our sample.

Stage 3. Analyse and compare curricula for sample of countries

The national curricula or framework covering cyber security was gathered and collated by the first author, and organized by country and source found. A content analysis was undertaken using the documents and sources collated in order to provide a comparison of the content within curricula and frameworks. The first author read the sources and compiled a set of codes with definitions and allocated them as technical or socio-technical according to our operational definition of cyber security (as discussed in Section 1). The second and fourth authors then read over these codes, their definitions and their designation as technical or socio-technical, providing feedback on the codes including suggestions on merging codes, their designation, duplicates or further information in the definition. The documents and sources were then read again, with the occurrence of each code noted. A list of the codes and their definitions can be found in Appendix A.

3 FINDINGS

This study brings together the findings of cyber security national curricula or frameworks for 12 countries: Australia, Canada, the Netherlands, New Zealand, Norway, Singapore, South Africa, the UK (i.e., England, Northern Ireland, Scotland, and Wales) and the USA.

3.1 Education Systems and Terminology for the Countries in this Study

Education systems in different parts of the world vary in education stages, terms of duration, and terminology. One key factor that influences what a country's education system looks like is whether the country has evolved a unitary or federated government system, or other systems such as in the case of the UK – a unitary state with four devolved countries. Within the countries we focus on, five countries (the Netherlands, New Zealand, Norway, Singapore and South Africa) adhere to a unitary system. Unitary countries have a unified education system applied across the entire country, however, this does not necessarily mean there is a national curriculum for all schools to follow.

Federated countries are more complex. Some have potentially small differences between states (or provinces) with a national curriculum each state can follow (e.g., Australia). Other countries, such as the USA and Canada, have no unique central education system and no national curriculum, with each state or province implementing their own education system. This includes the ages pupils attend school and curriculum content. The USA and Canada have frameworks to guide cyber security content to be taught in schools. We shall use these frameworks as a means of comparison against other countries and as an indicative of what curriculum content is taught in those countries. The federated countries in our study are Australia, Canada and the USA.

Each of the four countries part of the UK (England, Wales, Scotland, and Northern Ireland) has its own devolved education system and national curriculum (the English National Curriculum, the Welsh National Curriculum, the Scottish Curriculum for Excellence, and the Northern Ireland Curriculum). Whilst the constitution sits with the UK Parliament, policies informing education and training are made in devolved parliaments (i.e., the Welsh Parliament, the Scottish Parliament, the Northern Irish Assembly) [77].

The ages of compulsory pre-university education differ for each of the countries in our sample, with starting school age ranging between 5 and 7, and ending ranging between 15 and 18[6]. Table 1 provides an overview of the school stages (primary and secondary) and the structure of the education provision, with primary education ending between ages 11 and 15 and secondary education beginning between ages 12 and 16. It is worth noting that the ages reported in the table (and in this paper as a whole) of when pupils reach different education stages are not absolute values. They are affected not only by the year a pupil was born but also the month. In some countries, the academic year follows the calendar year (e.g., Australia and South Africa) but in others they are not synchronized (such as the majority of the countries in our sample) and this has implications on the starting age of pupils.

As it can be observed in Table 1, among unitary countries, differences in the school systems can be observed between countries. The starting age for primary school varies from age 5 (the Netherlands[7]), to age 6 (New Zealand and Singapore) and age 7 (Norway and South Africa). Federated countries within our sample are more uniform, with all countries starting primary education when pupils turn 6 although, in the USA, the length of primary education varies across states [52]. Despite the lack of a unified education system, the stages of education within the federated countries in our sample, for primary and secondary school, follow a similar approach. Within the UK, four different systems exist

[6] Since 11 out of the 12 countries studied finish pre-university education at 18, we consider that as the typical upper bound, although secondary education in Singapore lasts until the year pupils turn 19.

[7] In the Netherlands, attendance at age 4 is possible but not compulsory [64].

due to the devolved nature of education, and Northern Ireland and Scotland's year groups are labelled differently to England and Wales. However, all countries in the UK adopt an aligned start and end for pre-university education.

The diversity in education systems including between and within countries (such as in the UK) demonstrates how fragmented the picture is in relation to overall education systems.

Table 1: Pupils age and organization of pre-university education (i.e., primary and secondary school) in our sample.

Country	**Age 5**	**Age 6**	**Age 7-11**	**Age 12-17**	**Age 18**
Unitary countries					
The Netherlands	Group 1	Group 2	Groups 3-7	Group 8 Groups 1-5*	Group 6*
New Zealand	■	Kindergarten	Years 1-5	Years 6-11	Year 12
Norway	■	■	Years 1-5	Years 6-7 Years 8-10, Year VG1	Year VG2
Singapore	■	Kindergarten	Years P1-P5	Years P6 Years S1-S5	Year S6**
South Africa	■	■	Years 1-5	Years 6-9 Years 10-11	Year 12
Federated countries					
Australia	■	Kindergarten	Years 1-5	Years 6-11	Year 12
Canada	■	Kindergarten	Grades 1-5	Grades 6 Grades 7-11	Grade 12
The USA	■	Kindergarten	Grades 1-5	Grades 6*** Grades 7-11	Grade 12
The UK					
England	Reception	Year 1	Years 2-6	Years 7-12	Year 13
Northern Ireland	Year 1	Year 2	Years 3-7	Years 8-13	Year 14
Scotland	Year P1	Year P2	Years P3-P7	Years S1-S6	Year S6
Wales	Reception	Year 1	Years 2-6	Years 7-12	Year 13

Legend: red font for primary education, blue font for secondary education, and solid grey box to mark ages not part of the mandatory education system.

3.2 Cyber Security Curricula Content

3.2.1 Australia

Although the Australian Curriculum is a national curriculum, it is the choice of each state to implement and follow it. Many Australian states use the Australian Curriculum as it is published [4, 5], with only three territories (New South Wales, Victoria, Western Australia) making any changes. The latest Australian curriculum was released in May 2022 [6] and was reported prior to its release to include significantly more cyber security than previously [66]. Cyber security related content is covered within both the Digital Technologies learning area specifically, and dispersed across a range of subjects within the Australian Curriculum's 'digital literacy'[8] general capability [3]. Four strands exist within the digital literacy capability: 'practicing digital safety and wellbeing'; 'investigating'; 'creating and exchanging'; and 'managing and operating'. Relevant content includes managing digital privacy and wellbeing; respecting intellectual property; managing and protecting content; and selecting and operating tools [3]. Examples are given for teachers on

[8] The terminology from the original source was kept.

how the digital literacy general capability is relevant to their learning area. For example, intellectual property can be discussed in English and Humanities and Social Sciences learning areas; and cyberbullying and ethical online behavior can be covered in Health and Physical Education [3].

The Digital Technologies learning area is compulsory for 5-6-year-old pupils until the age of 13-14 [4] and elective for pupils aged 14-16 years [5]. Topics covered straddle both technical and socio-technical aspects of cyber security, including ethical practices and protocols, security practices, managing intellectual property, and interrogating the quality of digital data. Tangible examples for teachers to follow are not provided, with topic areas given as suggestions for teachers to interpret.

3.2.2 Canada

Canada has developed a framework to guide curriculum content and teaching related to computing, as education is a local and provincial level issue[9]. Within the Pan-Canadian K-12 Computer Science Education Framework [9], two areas are of particular interest for cyber security education: 'Computing and Networks' (includes cyber security), and 'Technology and Society' (includes ethics, safety and the law). Relevant items under 'Computing and Networks' include: defining cyber security, describing types of cyber-attacks and prevention practices, applying encryption and assessing the impacts of cyber-attacks on society [9]. Relevant items under 'Technology and Society' include: identifying strategies to protect personal data and identity, defining basic copyright principles, understanding privacy concerns relating to personal data and assessing policies governing technology [9]. Launched on 31st July 2020 [10], it provides 5 steps from beginner through to proficient learner and extension activities [9], with content to be covered incrementally with pupils able to build on prior knowledge, irrelevant of age group.. Each step is not tied to a particular grade level, however, it is encouraged to begin the steps of the framework in kindergarten [9]. Each competency gives example tasks pupils should be able to complete at the end of each step [9].

3.2.3 England

In England, cyber security is part of the computing curriculum in the English National Curriculum, with Computing as compulsory for pupils aged 5-14 [26, 27]. The focus of content for pupils aged 5-14 is using technology responsibility and respectfully, including knowing where to access help, and keeping personal information safe. For pupils aged 5-7, the specific focus is on being aware of their digital footprint and keeping passwords secure; for pupils aged 8-11, the specific focus is on recognizing inappropriate content; and for pupils aged 12-14 the specific foci are privacy, online identity, and recognizing inappropriate content [27]. No example activities or further specification are given other than an overview of the content e.g., 'recognize common uses of information technology beyond school'; and 'understand how changes in technology affect safety' [27]. Pupils aged 15-18 should be able to access Computing qualifications but this is an optional part of the English National Curriculum. Curriculum guidance outlines specifics of what students should know, e.g., 'show awareness of social opportunities and risks of computing' [2].

Cyber security related content is also present in both Relationships Education (RE) (for pupils aged 5-11) and Relationships and Sex Education (RSE) (for pupils aged 11-16), which have been compulsory since September 2020 [28]. Topics for pupils aged 5-11 include: online relationships [28]; distinguishing between online content [28] how information and data are shared [27]; online safety and boundaries in online relationships [27]; and recognizing harmful content and how to report it [27]. Topics for pupils aged 11-16, in addition to the topics for pupils aged 5-11, include: healthy online relationships; cyberbullying; rights and responsibilities; risks of sharing content online; how information is collected and generated online; and consent in online [27]. Links should also be drawn with the rest of the national curriculum [27].

3.2.4 The Netherlands

The stratified nature of the education system in the Netherlands impacts how many years pupils have access have to subjects that may cover cyber security content. Pupils who attend senior general secondary education (HAVO) and university preparatory education (VWO) 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

[9] As mentioned in the methodology section, non-English national curricula or frameworks were not considered for Canada, therefore, the French framework is not reflected in the paper.

[35]. For pupils who attend preparatory vocational secondary education (VMBO), the focus of their studies is on the vocational courses they undertake at school.

3.2.5 New Zealand

Education in New Zealand is guided by the New Zealand Curriculum for English medium schooling[10]. Cyber security education in the New Zealand Curriculum in primary level education is embedded into other subjects or topics and themes which cross multiple subject areas [46]. Digital Technologies, the subject under which cyber security education falls under, has been a compulsory part of the New Zealand Curriculum since January 2020. Digital technologies focuses on computational thinking, and designing and creating (digital) products [46]. Ethics and the impact on stakeholders such as businesses, the government and clients are also a part of Digital Technologies [46]. Pupils can take Digital Technologies as a National Certificate of Educational Achievement (NCEA) at all three levels of achievement [57, 58]. In the New Zealand Curriculum examples of activities are not given [46]

Cyber security is also a part of the key competencies within the primary curriculum under the competency 'using language, symbols, and texts' [47]. The key competencies are to be developed across a range of contexts within the curriculum [47]. As part of this competency, proficient use of ICT and being able to communicate with other ICT users is central [47].

3.2.6 Northern Ireland

ICT is a key part of the cross-curricular statutory requirements within the Northern Irish Curriculum for pupils aged 5-11 and 11-14 [11, 12, 14]. Aspects of cyber security (e.g., staying safe online) are to be taught in across a range of subjects. In particular, staying safe online and acceptable online behavior are featured within the curriculum [12]. Pupils aged 16-18 are able to study Computing or Computing-related subjects, however, much of the content appears to be online safety focused rather than technical aspects of cyber security [14]. Curriculum guidance for these qualifications outlines specifics of what students should know e.g., defining cybercrime, hacking and phishing [13] and explaining how networks and data can be protected [13].

3.2.7 Norway

In Norway, digital skills in a broad sense are embedded into subjects across the curriculum. Digital skills are part of the Framework of Basic Skills along with oral skills, reading and writing skills, and numeracy. Each skill develops continuously throughout their educational journey, and is incorporated into all subjects [81]. All teachers in all subjects have the responsibility for the development of these basic skills, however, some skills may be more emphasized in some subjects than others [81]. Aspects of cyber security are added into digital skills, notably under the action 'digital judgement', which includes understanding privacy online and online behavior, and reflecting on ethics of the internet as a communication tool (56; 81] Teachers interpret the framework independently, with no prescribed activities suggested [81].

3.2.8 Scotland

Digital literacy is described as a core part of a 'broad general education' within the Scottish Curriculum for Excellence [31] and digital literacy outcomes are recommended to be met in all curriculum areas [30]. Cyber security education is also included under the curriculum area 'Technologies' for pupils aged 5-14 [29]. Within digital literacy, relevant content is included under the organizers 'searching, processing and managing information responsibly' and 'cyber resilience and internet safety'. This includes communicating online safely, how to stay safe online, and staying secure online [30]. Pupils in Scotland can take a wide variety of qualifications specializing in cyber security, e.g., National Progression Award (NPA) in Cyber Security [67], as well as Computing qualifications as Nationals [68] Highers [69] and Advanced Highers [70]. Curriculum guidance for these qualifications outlines specifics of what students should know e.g., 'understanding legal and ethical considerations' [67]; and 'understanding the tools and techniques of hackers' [67].

[10] As mentioned before in the methodology, we will not cover non-English national curricula, but we want to highlight that New Zealand does have a Māori national curriculum.

3.2.9 Singapore

In Singapore, ICT, computing or digital skills are not compulsory subjects in primary education [51]. However, cyber security content is embedded within the compulsory subject 'Character and Citizenship Education' (CCE) for pupils aged 10-12, covering online friendships, communicating online and managing online bullying [48]. Pupils aged 12-17 have Cyber Wellness (CW) as a key part of the CCE curriculum, which includes covering the wellbeing of students online, positive online presence, using ICT for positive means, and being safe and responsible users of ICT [49]. An update to the CCE curriculum, valid from 2021, indicates scenarios to be used and an extra 50% allocated time in comparison to the previous curriculum given to CW [50]. Computing is offered for pupil aged 15-19 years by some schools in Singapore [17]. Other than using authentic scenarios, no other examples are given as to how the content should be covered in lessons [48].

3.2.10 South Africa

In the South Africa Curriculum to date, there is no cyber security educational provision, including in computing (only available between the ages of 16 and 18; optional) and within the life skills curriculum (taught at all ages; compulsory) [23, 24, 25]. Informal information and resources exists for pupils up to 18, but this educational content is not compulsory nor centrally administered by the government (e.g., for Grades 4 and 6 [41]).

3.2.11 The USA

A similar approach to Canada's framework exists in the USA, named K–12 Computer Science Framework [40]. It informs the development of state-level curricula, as in the USA national curricula are banned in the Elementary and Secondary Education Act (ESEA) [80]. Content related to cyber security is present in the core concepts of 'networks and the internet' (which includes technical topics) and the 'impacts of computing' (which includes safety, law and ethics). The framework has a suggested starting age of 6, aligning with the beginning of primary school in the USA. The main content recommended includes security measures, harmful behaviors, and law. The USA also has further recommendations regarding standards and the topics taught; notably the Common Core State Standards Initiative [18] and the ISTEs National Educational Technology Standards (NETS) [53]. Standards and the K–12 Computer Science Framework indicate progression levels, much like the Pan-Canadian K-12 Computer Science Education Framework, with levels not attached to set grade levels. This allows content to be covered incrementally with pupils able to build on prior knowledge, irrelevant of age group. Example activities are given for some concepts on the K–12 Computer Science Framework [40].

3.2.12 Wales

The latest Curriculum for Wales started implementation from September 2022, with 'digital competence' (being a confident user of digital technology) as one of the core cross-curricular skills within it [84]. Furthermore, one of the four purposes of the Curriculum for Wales specifically encapsulates digital technologies with: 'ambitious, capable learners who: use digital technologies creatively to communicate, find and analyze information' [85]. A central part of the Curriculum for Wales is the flexibility for schools to design their own curriculum, whilst developing prescribed cross-curricular skills.

Computer science features as part of the 'Science and Technology Area of Learning and Experience' [83] with cyber security content focused on storing and securing data, and networks. Online relationships are also a component of the 'relationships and identity' strand – prescribed content of the curriculum for ages 5-16+ [85] ICT remains a key component of the Welsh Baccalaureate [21]. Qualifications are available for pupils aged 14-18 as an optional part of the Curriculum for Wales [87, 88, 89]. The new GCSE Digital Technologies [86] qualification contains cyber security specific content such as securing systems and was designed to provide cyber security skills for pupils who did not take the GCSE Computer Science.

Within RSE[11] for pupils aged 5-16, the following topics are prescribed: effective communication and decision making in online relationships [86]; respect in online relationships [86]; bodily privacy online [86]; understand how behavior is perceived online; steps to stay safe from harm in online relationships [86]; understand how consent can be given within online relationships [86]; benefits and dangers of the internet and social media in forming friendships [86]; and understanding how to stay safe online [86].

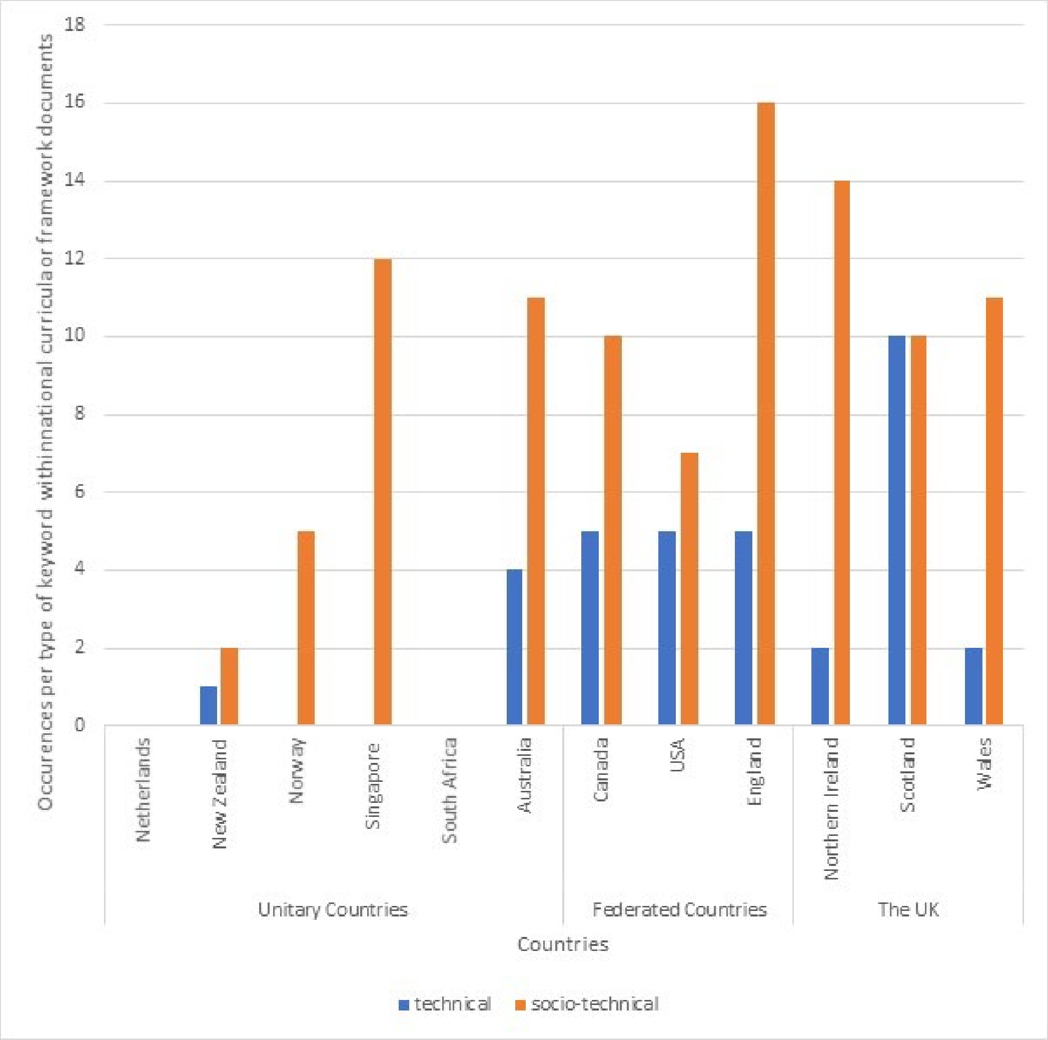
[11] Wales uses RSE for pupils of all ages.

3.3 Comparison of Cyber Security Curricula

3.3.1 Overall Trends Based on Content Analysis

An analysis of content was undertaken based on two categories: technical and socio-technical. The aim was to have an overview of the type of content where cyber security topics were mentioned in the national curricula and frameworks studied. Figure 2 provides an overview of the number of times cyber security content occurs within each curriculum, and whether it is technical or socio-technical in nature. Of countries that had a national curriculum including cyber security content, it can be observed that – overall – socio-technical content is mentioned more in the curricula (n=107) than technical content (n=37). The only country with a curriculum that included an equal number of technical keywords (n=10) and socio-technical keywords (n=10) was Scotland. The other extreme was Norway since only socio-technical keywords were identified (n=5) in their curriculum.

Figure 2: A bar chart of technical and socio-technical keywords related to cyber security in the national curricula or frameworks covered in our sample.



A closer examination of the educational content, via content analysis, revealed the most often mentioned topics in national curricula/frameworks of the studied countries. The keyword 'online ethics' was found across all countries except Scotland, with 'inappropriate online behavior', and 'Cyber Law and Legislation' found in the documentation of 9 countries. Overall, socio-technical keywords were found across more documents, with technical content occurring less frequently (e.g., 'authentication'; 'network security'; 'privacy configuration').

3.3.2 Age Range Coverage

One dimension relevant for comparing curricula is school age when cyber security content should be covered. Compiled from the previous section, Table 2 summarizes cyber security content coverage within the existing national curricula or framework for the 12 countries in our sample.

Table 2: Cyber security coverage in national curricula and frameworks per age group in our sample.

		Age reached at school													
Government	**Country**	5	6	7	8	9	10	11	12	13	14	15	16	17	18
Unitary	The Netherlands*	-	-	-	-	-	-	-	-	-	-	-	-	-	-
	New Zealand		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	o	o	o
	Norway**			✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	Singapore		-	-	-	-	✓	✓	✓	✓	✓	✓	✓	✓	✓
	South Africa*			-	-	-	-	-	-	-	-	-	-	-	-
Federated	Australia		✓	✓	✓	✓	✓	✓	✓	✓	✓	o	o	-	-
	Canada**		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	The USA**		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
The UK	England	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	o	o
	Northern Ireland	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	o	o
	Scotland	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	o	o	o	o
	Wales	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	o	o

Legend: ✓ Prescribed requirement for coverage of cyber security per age group

- No requirement for coverage of cyber security per age group

o Optional coverage of cyber security per age group depending of choice of qualification

* Countries where the national curriculum or framework does not mention cyber security at all

** Countries where the national curriculum or framework operate no age bounds on expectations of cyber security coverage, whereby pupils can go faster or slower through the levels.

Some patterns can be observed from Table 3. The age that the cyber security provision starts differs across the countries, with the majority starting at 5-6 (9 out of 12 countries), and 1 starting at 10 (Singapore). 9 of the 12 countries within our sample (Australia, Canada, New Zealand, Norway, all the four UK countries and the USA) are teaching cyber security content to younger children (i.e., aged 5-6). Furthermore, Australia is teaching cyber security to children as young as 5 years old. Although this occurs prior to the start of their primary education age (as shown in Table 1), this forward-thinking initiative is of note [66].

It also appears that the federated countries within our sample have similar coverage in regards to cyber security content. However, there is a great diversity to unitary countries. For example, Norway conducts cyber security education from the ages of 7-15 (a large coverage), while Singapore has the narrowest range at 8-10 years, and the Netherlands and South Africa have no cyber security coverage at all within their national curriculum.

All countries within the UK operationalize choice within the qualifications pupils can take toward the end of their secondary education, choosing which subjects to specialize into. Notably, England, Northern Ireland and Wales all follow the same pattern of when this choice exists in relation to cyber security coverage (age 16-18). This is perhaps indicative of England, Northern Ireland and Wales having very similar age bounds for levels of content (e.g., ISCED levels 2-4 all align). However, Scotland differs from England, Northern Ireland and Wales in regards to when choice occurs. Two other countries outside the UK where pupil choice exist are Australia and New Zealand. Both of these countries follow a different pattern to both Scotland, and England, Northern Ireland and Wales.

Also of note is the nature of the frameworks used within Canada, Norway and the USA. The frameworks include cyber security content for all age groups, however set content is not prescribed per age group. This is to allow pupils to work faster or slower as per their ability incrementally, with pupils able to build on prior knowledge.

3.3.3 Organization of Content

The nature of how cyber security content is embedded into the national curriculum or framework appears to follow four main approaches, as can be seen in Table 3.

Table 3: How cyber security content is embedded into the national curricula or frameworks in our sample.

Country	**One technical subject only (e.g., Computing, ICT)**	**One non-technical subject only (e.g., RSE, CCE*)**	**One technical & one non-technical subject**	**Across all or a range of subjects**
Unitary countries				
The Netherlands**				
New Zealand	✓ (ages 12-18)			✓ (ages 6-11)
Norway				✓
Singapore		✓		
South Africa**				
Federated countries				
Australia				✓
Canada	✓			
The USA			✓	
The UK				
England			✓	
Northern Ireland				✓
Scotland				✓
Wales				✓

** RSE: Relationships and Sexual Education; CCE: Character and Citizenship Education.*

*** Countries where there is no national curriculum or framework.*

The first approach is where cyber security is covered in a single technical subject only. This means cyber security content is only present within a technical subject such as Computing or ICT. Within our sample, Canada follows this approach, as does New Zealand for pupils aged 12-18 (secondary school).

The second approach is where cyber security is covered only in a single non-technical subject only. Non-technical subjects include RSE and CCE. Singapore is the only country within our sample that follows this approach.

The third approach is where cyber security is covered in both technical and non-technical subjects. One example of this could be where some cyber security content is taught within Computing, and some within RSE. England and the USA are the countries within our sample that follow this approach.

The final approach is where cyber security is covered across all or a range of subjects. In this case, cyber security content is taught within subjects not traditionally associated with cyber security, such as Literature and History (e.g., copyright and intellectual property, communicate using text messages and understanding the content), as well as those that may be perceived to have stronger links, such as Mathematics (e.g., cryptography) and Science (e.g., selecting appropriate online content for a research project). Through cyber security content being covered across a range of subjects, links can be provided across disciplines. Therefore, pupils might be able to see how subjects and content interlink. The countries within our sample that follow this approach are: Australia, New Zealand (for ages 6-11; primary school), Northern Ireland, Norway, Scotland and Wales. This final approach is the most popular approach within our sample.

3.3.4 Approaches to Curricula Mandate

Of the countries that did have cyber security content within their curricula, we identified three approaches to mandates within our sample. These are: no mandate for cyber security education; a mandate exists and states can opt in or out; a mandate exists with prescribed requirements.

Within our sample, the Netherlands and South Africa do not have a mandate for cyber security education at pre-university level. Due to the lack of a national curricula or framework that covers cyber security, it becomes completely up to individual schools to recognize the importance of the subject, and seek independent guidance on whether or what and when to deliver cyber security content. In the Netherlands, organizations such as Kennisnet may assist with cyber security content in schools, even though there is no mention of cyber security content within their national curriculum.

Canada and the USA have frameworks regarding cyber security education, however it is up to states to opt in to the framework. Whereas a curriculum may provide expectations of what should be taught, a framework provides guidance as to what cyber security content should be covered. This is an important distinction for federated countries that have frameworks (Canada and the USA) to organize matters of education at state level rather than country level due to government system. With these frameworks being implemented at the state level, it appears that a level of unity is aspired to, but huge discrepancies may remain due to the nature of such frameworks. Nevertheless, expectations are also not compulsory and remain at requirements level, i.e., they “should” be implemented rather than “must” be implemented. Schools still have the freedom to pick-and-choose the requirements to implement and at what extent, according to local resources and capabilities.

Seven countries in our sample (Australia, England, Northern Ireland, New Zealand, Scotland, Singapore and Wales) have a national curriculum that prescribes requirements to be followed by schools.

3.3.5 Teacher Discretion on Content Delivery

Within the national curricula or framework of some countries in our sample, schools and teachers are allowed to decide what is taught and how. Countries such as England, are more prescriptive with the topics that need to be covered [26, 27] but even in these cases, it appears that teacher discretion remains with the activities or length of teaching time that is devoted to each topic. Notably, Canada’s K-12 framework suggests following it from age 6, yet there are no prescribed activities or guidance for it to happen. Furthermore, the steps not having a set age to cover the content at allows for the content to be covered incrementally with pupils able to build on prior knowledge, irrelevant of age group. This increases the flexibility within teacher choice. Additionally, cyber security content may not only be taught by teachers (for example, stakeholders external to schools may deliver such content, as in Singapore with the Go Safe Online Drama Skit [20]). Although having multiple stakeholders (e.g., who visit schools for cyber security activities and talks) involved in the teaching of cyber security has benefits – potentially enhancing cyber security education, it becomes hard to ensure consistency of content coverage and alignment to avoid fragmentation.

4 DISCUSSION

This study aimed to explore the cyber security curricula of multiple countries through the following 2 research questions: (1) What are the similarities and differences in cyber security education curricula across countries? (2) What approaches do countries take to including cyber security education in their curricula? We have structured our discussion into how each of our research questions have been answered, strengths and limitations, and implications for the future.

4.1 Research question 1: What are the similarities and differences in cyber security education curricula across countries?

One similarity found across the intended curricula and frameworks of the countries included in our study was cyber security content that is socio-technical generally appears to be more mentioned in intended curricula. Scotland was the only country in our study that appeared to feature more technical content in its intended curriculum. In addition, more socio-technical cyber security content was present in intended curricula in our study, irrespective of if the country has a unitary, federated or devolved government. Reasons for this focus within cyber security curricula and frameworks may be numerous, however the increasing time children are spending online [60], and the perceived risks [60], may partially account for this. Another similarity exists for 9 of 12 countries (Australia, Canada, New Zealand, Norway, all the four UK countries and the USA), who have cyber security curricula content for children age 5-6. However, there appeared to be no one set way for cyber security content to be covered in intended curricula, echoing previous studies comparing intended and enacted Computer Science curricula [33, 37].

Socio-economic status also appeared to be a dimension that impacted the provision of cyber security content within the school curriculum. This finding is unsurprising given many of the countries in our sample rank highly on the Global Cybersecurity Index (GCI) (e.g., the USA has a GCI of 1 out of 182 countries [39]). Among the two countries not having cyber security educational provision within their curriculum in our sample – the Netherlands and South Africa, only the latter has a lower socio-economic status. Where there are highly limited resources, other subjects are prioritized [76, 90]. On the inverse, countries with a higher socio-economic status within our sample did appear to be making efforts to target 'non-traditional' pupils notably girls (e.g., in Singapore, the UK and the USA). The difference in socio-economic backgrounds seems to contribute to the digital divide in regard to access to devices, education on cyber security, and opportunities to take part in cyber security-related activities. Although cyber security careers exist worldwide, the majority of job openings appear to be located in countries with a higher socio-economic status [71].

4.2 Research question 2: What approaches do countries take to including cyber security education in their curricula?

Four main approaches were identified in regards to the coverage and organization of cyber security education in a pre-university context at schools and colleges were: (1) covered in a single technical subject (Canada, New Zealand (ages 12-18)), (2) covered in a single non-technical subject (Singapore), (3) covered in both one technical and one non-technical subject (the USA), and (4) covered in all or a range of subjects (Australia, New Zealand (ages 5-11), Northern Ireland, Norway, Scotland, Wales). In addition, three approaches to mandates were identified: (1) no mandate regarding cyber security education, (2) a mandate exists and states can opt in or out, (3) a mandate exists with prescribed requirements. Cyber security content within the national curriculum was found across a variety of age groups, with some countries starting teaching cyber security content from 5-6 years old (Australia, Canada, New Zealand, all four UK countries and the USA) to as late as 10 years old (Singapore). Countries that use frameworks (Canada, Norway and the USA) do not have specific content attached to specific age groups, rather they suggest content to be covered incrementally with pupils able to build on prior knowledge.

With the growing use of digital technologies and the internet, pre-university cyber security education becomes ever more vital for children (up to 18) across the globe. Past literature has indicated that ICT and Computer Science competencies may be taught within specific subjects [37, 82], echoing approaches found within this study where cyber security education may only be covered in a single technical subject, or a single non-technical subject. However, countries such as Australia and Scotland, that embed cyber security content into their curriculum across a range of subjects, in addition to specific in-subject content, allow for cyber security content to be taught 'in context'. This approach was recommended by the OECD on improving children's online safety [8], stating that learning about e-safety should not be isolated in nature. This recommendation from the OECD echoes other findings from research exploring how Computer Science should be taught [37, 75). This type of approach ensures that all pupils are targeted with at least some cyber security content. This approach to embed key skills into the curriculum (regarding embedding ICT and Computer Science across subjects [73]) is perhaps indicative of pedagogy (ideas of teaching and learning) [32] at a policy level. Given the disparities in the diversity of pupil that may wish to study cyber security (e.g., pupils from 'non-traditional' backgrounds such as ethnic minorities, disabled pupils and from lower socio-economic backgrounds [7, 16, 19], not all pupils may opt to study technical subjects that are more traditionally associated with cyber security. Therefore, an approach covering cyber security across a range of subjects would allow for all pupils to access key skills associated with it.

The different approaches to curriculum mandates are crucial to consider for the implementation of cyber security education in pre-university settings. In particular, the difference in nature between national curricula and national frameworks is central. National-level frameworks can inform regional curricula. Within federated countries, it may be hard to mandate curricula uniformly across multiple states, or in the case of the USA, where a national curriculum is illegal. Frameworks may be seen as an attempt to unify what is taught across states.

4.3 Strengths and Limitations

Twelve countries were covered in this study. Through comparing the curricula of 12 countries, similarities and differences between the curricula could elicited. Although our sample may not be representative, including for English speaking countries, we were limited to countries with available knowledgeable contacts that were available at the time of our research, and availability of national curricula or frameworks in English. This meant we had more unitary countries within our sample at this time than federated countries. Future research should explore further federated countries and their curricula, as well as other English-speaking and non-English speaking countries. It is also important to note that not all countries will have their curricula available publicly in English. As the research team are English-speaking, this shaped our inclusion criteria which required online information to be available in English.

Our study also only included one country from Africa and one from Asia, therefore, it would be inappropriate to assume the findings from these countries could be generalizable without further exploration of cyber security pre-university education of more countries in these two continents. In addition, we did not include any countries from Latin America, mainly due to the lack of English material in relation to their national curricula. We were also unable to include countries that are defined as 'the least developed countries' [79].

4.4 Conclusion and Implications for the Future

In this study, we have sought to explore and compare the cyber security curricula from multiple countries. A primary finding from our research is that most of the countries in our study concentrated their school-age cyber security teaching curricula or frameworks on socio-technical content (such as digital literacy, ethical behavior and online safety) as opposed to more computer-focused technical content (such as password protection, or tools and techniques of hackers). Of our sample, only the Scottish curriculum was seen to be providing robust technical education on cyber security to pupils.

We have also found a great variety of time and approaches to cyber security education among our sample. In terms of age ranges, with Canada and the US providing framework curricula for 10 years of school-age education, several countries providing between 12 and 9 years, and two countries (The Netherlands and South Africa) providing no required cyber security education within their national curriculum. In terms of approach, we identified four approaches to including cyber security within the curriculum: included within a single technical subject; included in a single non-technical subject; included in a single technical and non-technical subject; and included within a variety of subjects. This demonstrates a lack of consistency across countries in terms of the implementation of cyber security implementation.

Lastly, we identified that within federated countries (where the education system is not nationally prescribed, but is coordinated at the provincial or state level) national frameworks for cyber security education can be important tools to help maintain a coherent and consistent basic cyber security education across a federation.

In light of our findings, we suggest some key recommendations. Some of the countries that had more cyber security coverage within their national curricula or frameworks embedded cyber security skills across their national curriculum, including across a range of subjects. These findings echo previous findings which suggested that competencies should not be linked to one academic subject only (e.g., Computing or ICT) [82]. We recommend that governments setting pre-university curricula should follow such approach as it allows for a wider range of pupils to be exposed to cyber security education. This is important due to the nature of cyber security skills, which are not only relevant to technological careers.

In a similar manner, both technical and socio-technical aspects of cyber security need to be covered. Cyber security includes not only technical aspects [55] and, as emphasized above, some cyber security skills are relevant to a diverse range of careers. A recent systematic review recommended six categories of cyber security (broad sense) awareness for teachers and policy makers to follow (technological awareness, procedural awareness, data awareness, identity awareness, sociocultural awareness, and consumer awareness) that may assist ensuring the required breadth of cyber security content coverage [65]. We therefore recommend that countries follow the approach of teaching cyber security content in both technical and non-technical subjects, along with teaching cyber security as a key skill across multiple of subjects to show its relevance across disciplines. Future studies should evaluate the efficacy of curricula in relation to teaching outcomes and teachers' confidence in teaching the topics mandated to investigate the policy-to-practice gap.

Working with children and young people, their parents, carers and teachers using a participatory approach is of central importance and allows their views to shape any subsequent curriculum [62], allowing it to be culturally and socio-economically sensitive. Teachers in particular have discretion and influence over the content they teach to their pupils and how they implement curricula [44]. Governments (either those at the national level in the case of unitary countries or those at the state level for federated countries) and other relevant organizations responsible for guiding curricular content should seek to prioritize cyber security, including any resulting output or policy targeting all ethnic and cultural groups within their country.

In regards to future research, researchers can build on the findings of this study by enlarging the sample of countries, considering national curricula and frameworks in languages beyond English, and aiming for further cultural diversity across geographic locations and socio-economic status. More researchers, and especially those who speak non-English languages, should replicate this study on more countries to validate results and enrich the evidence base on cyber security content in national curricula worldwide.

ACKNOWLEDGMENTS

This article is built on a research project commissioned by the *Global Forum on Cyber Expertise* and specifically its Working Group D on "cyber security culture and skills", funded by Global Affairs Canada. To learn more about the GFCE, visit www.thegfce.org.

REFERENCES

[1] Eric Amankwa. 2021. Relevance of Cybersecurity Education at Pedagogy Levels in Schools. J. Information Security 12, 4, (September 2021), pp. 233–249. https://doi.org/10.4236/jis.2021.124013

[2] AQA (Assessment and Qualifications Alliance) (UK). 2023. AS and A-Level Computer Science, AS (7516) A-level (7517). Retrieved December 18, 2023 from https://www.aqa.org.uk/subjects/computer-science-and-it/as-and-a-level/computer-science-7516-7517/subject-content-a-level/consequences-of-uses-of-computing

[3] Australian Curriculum. 2023. Digital Literacy. Retrieved December 18, 2023 from https://v9.australiancurriculum.edu.au/f-10-curriculum/general-capabilities/digital-literacy

[4] ACARA (Australian Curriculum, Assessment and Reporting Authority). n.d.-a. Foundation – Year 10 curriculum (Version 8.4). Retrieved December 18, 2023 from https://www.acara.edu.au/curriculum/foundation-year-10

[5] ACARA. n.d.-b. Structure. Retrieved December 18, 2023 from https://www.australiancurriculum.edu.au/f-10-curriculum/structure/

[6] Australian Government. 2022.. Australian Curriculum. Retrieved December 18, 2023 from https://www.education.gov.au/australian-curriculum

[7] Amanda Babbs. 2022. Why we need more women in cyber security. Computer Fraud & Security, 2022, 2, (February 2022). https://doi.org/10.12968/s1361-3723(22)70020-6

[8] Tracey Burns and Francesca Gottschalk, F. 2019. What do we know about children and technology? Organisation for Economic Co-operation and Development. Retrieved December 18, 2023 from https://web-archive.oecd.org/2019-03-13/510634-booklet-21st-century-children.pdf

[9] Canada Learning Code. 2020a. Learning in the Digital World: A Pan-Canadian K-12 Computer Science Education Framework. Retrieved December 18, 2023 from https://k12csframework.ca/wp-content/uploads/Learning-for-the-Digital- Future_Framework_Final.pdf

[10] Canada Learning Code. 2020b. A Pan-Canadian K-12 Computer Science Education Framework. Retrieved December 18, 2023 from https://www.canadalearningcode.ca/bringing-the-k-12-computer-science-education-framework-to-life/

[11] CCEA (Council for the Curriculum, Examinations and Assessment) (UK). 2007a. The Northern Ireland Curriculum: Primary. Retrieved December 18, 2023 from https://ccea.org.uk/document/924

[12] CCEA. 2007b. Statutory Curriculum at Key Stage 3. Retrieved December 18, 2023 from https://ccea.org.uk/downloads/docs/ccea-asset/Curriculum/The%20Statutory%20Curriculum%20at%20Key%20Stage%203.pdf

[13] CCEA. 2017. CCEA GCSE Specification in Digital Technology. Retrieved December 18, 2023 from https://ccea.org.uk/downloads/docs/Specifications/GCSE/GCSE%20Digital%20Technology%20%282017%29/GCSE%20Digital%20Technology%20%282017%29-specification-Standard_1.pdf

[14] CCEA. 2019. GCE Digital Technology. Retrieved December 18, 2023 from https://ccea.org.uk/downloads/docs/Specifications/GCE/GCE%20Digital%20Technology%20%282016%29/GCE%20Digital%20Technology%20%282016%29-specificationStandard_1.pdf

[15] Weiru Chen, Yuming. He, Xin Tian, and Wu He. 2021. Exploring Cybersecurity Education at the K-12 Level. In Proceedings of the SITE Interactive Conference. Association for the Advancement of Computing in Education (AACE), Online, United States, 108-114. https://www.learntechlib.org/p/220175/

[16] Michelle J. Cobb. 2018. Plugging the skills gap: the vital role that women should play in cyber-security. Computer Fraud & Security 2018, 1, (January 2018), 5–8. https://doi.org/10.1016/S1361-3723(18)30004-6

[17] Coding Lab. 2020. Schools in Singapore offering IB Computer Science, O-Level and A-Level Computing. Retrieved December 18, 2023 from https://www.codinglab.com.sg/schools-singapore-offering-ib-o-level-a-level-computing/

[18] Council of Chief State School Officers and National Governors Association Center for Best Practices. n.d.. Common Core State Standards Initiative. Retrieved December 18, 2023 from http://www.corestandards.org/

[19] Rowena Cullen. 2001. Addressing the digital divide," Online Information Review 25, 5, (October 2001), 311–320. doi: https://doi.org/10.1108/14684520110410517

[20] Cyber Security Agency of Singapore. n.d.. Go Safe Online Awareness Skit. Retrieved December 18, 2023 from https://www.csa.gov.sg/our-programmes/cybersecurity-outreach/sg-cyber-safe-students/events-and-activities/go-safe-online-awareness-skit

[21] DCELLS (Department for Children, Education, Lifelong Learning and Skills, Welsh Assembly Government). 2009. Information and communication technology at Key Stage 4: Guidance for schools. Retrieved December 18, 2023 from https://hwb.gov.wales/api/storage/b83b9ca6-8bd6-475e-a2ec-6e65cecbb7cd/information-and-communication-technology-at-key-stage-4.pdf

[22] DCMS (Department for Digital, Culture Media & Sports) (UK). 2022. Cyber security skills in the UK labour market 2022: findings report. Retrieved December 18, 2023 from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1072767/Cyber_security_skills_in_the_UK_labour_market_2022_-_findings_report.pdf

[23] Department of Basic Education (South Africa). 2011a. Curriculum and Assessment Policy Statement Grades R-3: Life Skills. Retrieved December 18, 2023 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

[24] Department of Basic Education (South Africa). 2011b. Curriculum and Assessment Policy Statement Grades 7-9: Life Skills. Retrieved December 18, 2023 from https://www.education.gov.za/Portals/0/Documents/CSE%20Scripted%20lessons/CAPS%20SP%20%20LIFE%20ORIENTATION%20%20WEB.pdf

[25] Department of Basic Education (South Africa). 2018. Curriculum and Assessment Policy Statement Grades 4-6: Life Skills. Retrieved December 18, 2023 from https://www.education.gov.za/Portals/0/Documents/Publications/CAPS%20Commnets/GET/LIFE%20SKILLS%20IP%20GRADES%204%20-%206%20EDITED.PDF

[26] Department for Education (UK). 2013. National curriculum in England: computing programmes of study. Retrieved December 18, 2023 from https://www.gov.uk/government/publications/national-curriculum-in-england-computing-programmes-of-study

[27] Department for Education (UK). 2014. National curriculum. Retrieved December 18, 2023 from https://www.gov.uk/government/collections/national-curriculum

[28] Department for Education (UK). 2022. Relationships Education, Relationships and Sex Education (RSE), and Health Education. Retrieved December 18, 2023 from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1090195/Relationships_Education_RSE_and_Health_Education.pdf

[29] Education Scotland. 2017. Benchmarks: Technologies. Retrieved December 18, 2023 from https://education.gov.scot/improvement/documents/technologiesbenchmarkspdf.pdf

[30] Education Scotland. 2018. Curriculum for Excellence: Technologies. Experiences and Outcomes. Retrieved December 18, 2023 from https://education.gov.scot/Documents/Technologies-es-os.pdf

[31] Education Scotland. n.d.. About the 3-18 curriculum. Retrieved December 18, 2023 from https://education.gov.scot/parentzone/learning-in-scotland/about-the-3-18-curriculum/

[32] Per-Olof Erixon. 2010. School subject paradigms and teaching practice in lower secondary Swedish schools influenced by ICT and media. Computers & Education 54, 4 (May 2010), 1212–1221. https://doi.org/10.1016/j.compedu.2009.11.007

[33] Katrina. Falkner, Sue Sentance, Rebecca Vivian, Sarah Barksdale, Leonard Busuttil, Elizabeth Cole, Christine Liebe, Francesco Mariorana, Monica M. McGill and Keith Quille. 2019. An International Comparison of K-12 Computer Science Education Intended and Enacted Curricula. In Proceedings of the 19th Koli Calling International Conference on Computing Education Research. Association for Computing Machinery, New York, NY, USA, Article 4, 1–10. https://doi.org/10.1145/3364510.3364517

[34] W Gander, A Petit, G Berry, B Demo, J Vahrenhold, A McGettrick, R Boyle, M Drechsler, A Mendelson, C Stephenson, C Ghezzi, and B Meyer. 2013. Informatics Education: Europe Cannot Afford to Miss the Boat. Technical Report. Association for Computing Machinery &, Joint Informatics Europe ACM Europe Working Group on Informatics Education, New York. 1--21 pages. https://www.informatics-europe.org/news/382-informatics-education-in-europe-are-we-on-the-same-boat.html

[35] Government of the Netherlands. 2021. Senior general secondary education (HAVO) and pre university education (VWO). Retrieved December 18, 2023 from https://www.government.nl/topics/secondary-education/different-types-of-secondary-education/senior-general-secondary-education-havo-and-pre-university-education-vwo

[36] Hai Hong, Jennifer Wang, and Sepehr Hejazi Moghadam. 2016. K-12 computer science education across the U.S. In Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics). https://doi.org/10.1007/978-3-319-46747-4_12

[37] Peter Hubwieser, Michail N. Giannakos, Marc Berges, Torsten Brinda, Ira Diethelm, Johannes Magenheim, Yogendra Pal, Jana Jackova, and Egle Jasute. 2015. A Global Snapshot of Computer Science Education in K-12 Schools. In Proceedings of the 2015 ITiCSE on Working Group Reports (ITICSE-WGR '15). Association for Computing Machinery, New York, NY, USA, 65–83. https://doi.org/10.1145/2858796.2858799

[38] ITU (International Telecommunication Union). (2023). Definition of cybersecurity. Retrieved December 18, 2023 from https://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx

[39] ITU. n.d.. Global Cybersecurity Index. Retrieved December 18, 2023 from https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx

[40] K–12 Computer Science Framework Steering Committee. 2016. K–12 Computer Science Framework. Retrieved December 18, 2023 from https://k12cs.org/wp-content/uploads/2016/09/K%E2%80%9312-Computer-Science-Framework.pdf

[41] Elmarie Kritzinger. 2017. Cyber Safety Educator Workbook, Grade 4 & Grade 6. (Received from the author via email on 9th August 2021)

[42] Elmarie Kritzinger, Maria Bada, and Jason R. C. Nurse. 2017. A study into the cybersecurity awareness initiatives for school learners in South Africa and the UK. In IFIP World Conference on Information Security Education, Springer, Cham, 110-120. https://doi.org/10.1007/978-3-319-58553-6_10

[43] Maria Lamond, Karen Renaud, Lara Wood and Suzanne Prior. 2022. SOK: young children's cybersecurity knowledge, skills & practice: a systematic literature review. In Proceedings of the 2022 European Symposium on Usable Security. Association for Computing Machinery, New York, NY, USA, 14–27. https://doi.org/10.1145/3549015.3554207

[44] Laura R. Larke. 2019. Agentic neglect: Teachers as gatekeepers of England's national computing curriculum. British Journal of Educational Technology 50, 3 (February 2019), 1137-1150. https://doi.org/10.1111/bjet.12744

[45] Birgy Lorenz, Kaido Kikkas and Kairi Osula 2018. Development of children's cyber security competencies in Estonia. In Proceeding of the Learning and Collaboration Technologies. Learning and Teaching: 5th International Conference, LCT 2018, Held as Part of HCI International 2018, Las Vegas,

NV, USA, July 15-20, 2018, Proceedings, Part II 5, Springer International Publishing, 473-482. https://doi.org/10.1007/978-3-319-91152-6_36

[46] Ministry of Education (New Zealand). 2019a. Technology in the New Zealand Curriculum. Retrieved December 18, 2023 from https://nzcurriculum.tki.org.nz/content/download/168478/1244184/file/NZC-Technology%20in%20the%20New%20Zealand%20Curriculum-Insert%20Web.pdf

[47] Ministry of Education (New Zealand). 2019b. The New Zealand Curriculum. Retrieved December 18, 2023 from https://nzcurriculum.tki.org.nz/content/download/1108/11989/file/NZ%20Curriculum%20Web.pdf

[48] Ministry of Education (Singapore). 2012. Character and Citizenship Education Syllabus – Primary. Retrieved December 18, 2023 from https://www.moe.gov.sg/-/media/files/primary/characterandcitizenshipeducationprimarysyllabusenglish.pdf

[49] Ministry of Education (Singapore). 2020a. Character and Citizenship Education Syllabus – Secondary. Retrieved December 18, 2023 from https://www.moe.gov.sg/-/media/files/secondary/syllabuses/cce/2021-character-and-citizenship-education-syllabus-secondary.pdf

[50] Ministry of Education (Singapore). 2020b. Character and Citizenship Education (CCE 2021). Retrieved December 18, 2023 from https://www.moe.gov.sg/microsites/cos2020/refreshing-our-curriculum/cce2021.html

[51] Ministry of Education (Singapore). n.d. Primary school subjects and syllabuses.: Retrieved December 18, 2023 from https://www.moe.gov.sg/primary/curriculum/syllabus

[52] NCES (National Center for Education Statistics) (USA). 2001. Digest of Education Statistics 2001. Retrieved December 18, 2023 from https://nces.ed.gov/pubs2002/2002130.pdf

[53] NCES. 2002. Technology Integration. In Technology in Schools: Suggestions, Tools, and Guidelines for Assessing Technology in Elementary and Secondary Education. Retrieved December 18, 2023 from https://nces.ed.gov/pubs2003/tech_schools/chapter7.asp

[54] NCSC (National Cyber Security Centre) (UK). n.d.-a. About the NCSC: What is cyber security? Retrieved December 18, 2023 from https://www.ncsc.gov.uk/section/about-ncsc/what-is-cyber-security

[55] NCSC. n.d.-b CyBOK – The Cyber Security Body of Knowledge. Retrieved December 18, 2023 from https://www.cybok.org/

[56] Norwegian Ministry of Education and Research. (2012). Framework for Basic Skills. Retrieved December 18, 2023 from https://www.udir.no/contentassets/fd2d6bfbf2364e1c98b73e030119bd38/framework_for_basic_skills.pdf

[57] NZQA (New Zealand Qualifications Authority). 2021a. Approved subjects for University Entrance. Retrieved December 18, 2023 from https://www.nzqa.govt.nz/qualifications-standards/awards/university-entrance/approved-subjects/

[58] NZQA. 2021b. NCEA levels and certificates. Retrieved December 18, 2023 from https://www.nzqa.govt.nz/ncea/understanding-ncea/how-ncea-works/ncea-levels-and-certificates/

[59] Michiyo Oda, Yoko Noborimoto & Tatsuya Horita. 2023. Implications for Computer Science Curricula in Primary School: A Comparative Study of Sequences in England, South Korea, and New Zealand. In Proceedings of Towards a Collaborative Society Through Creative Learning. IFIP Advances in Information and Communication Technology, vol 685. Springer, Cham. https://doi.org/10.1007/978-3-031-43393-1_57

[60] Ofcom (Office of Communications) (UK). 2023. Children and Parents: Media Use and Attitudes. Retrieved December 18, 2023 from https://www.ofcom.org.uk/research-and-data/media-literacy-research/childrens/children-and-parents-media-use-and-attitudes-report-2023

[61] Dana Ondrušková and Richard Pospíšil. 2023. The good practices for implementation of cyber security education for school children. Contemporary Educational Technology 15, 3, (2022), ep435. https://doi.org/10.30935/cedtech/13253

[62] Denny Pencheva, Joseph Hallett and Awais Rashid. 2020. Bringing cyber to school: Integrating cybersecurity into secondary school education. IEEE Security & Privacy 18, 2 (March-April 2020), 68-74. https://doi.org/10.1109/MSEC.2020.2969409

[63] Michael D, Richardson, Pamela A. Lemoine, Walter E. Stephens and Robert E. Waller. 2020. Planning for Cyber Security in Schools: The Human Factor. Educational Planning, 27, 2 (2020), 23-39. https://eric.ed.gov/?id=EJ1252710

[64] Rijksoverheid. n.d. When can my child go to primary school? Retrieved December 18, 2023 from https://www.rijksoverheid.nl/onderwerpen/leerplicht/vraag-en-antwoord/wanneer-mag-mijn-kind-naar-de-basisschool

[65] Rahime B. Sağlam, Vincent Miller, V. and Virginia N. L. Franqueira. 2023. A Systematic Literature Review on Cyber Security Education for Children. IEEE Transactions on Education, 66, 3 (June 2023), 274-286. https://doi.org/10.1109/TE.2022.3231019

[66] Sharwood, S. (2021). Australia proposes teaching cyber-security to five-year-old kids. Retrieved December 18, 2023 from https://www.theregister.com/2021/04/30/eaching_cybersecurity_to_five_year_olds/

[67] SQA (Scottish Qualifications Authority). 2015. 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. Retrieved December 18, 2023 from https://www.sqa.org.uk/sqa/files_ccc/GK7W44_GK7X45_GK7Y46.pdf

[68] SQA. 2021a. National 5 Computing Science. Retrieved December 18, 2023 from https://www.sqa.org.uk/files_ccc/ComputingScienceCourseSpecN5.pdf

[69] SQA. 2021b. Higher Computing Science. Retrieved December 18, 2023 from https://www.sqa.org.uk/files_ccc/HigherCourseSpecComputingScience.pdf

[70] SQA. 2023. Advanced Higher Computing Science. Retrieved December 18, 2023 from https://www.sqa.org.uk/sqa/files_ccc/ah-course-spec-computing-science.pdf

[71] Statista. 2021. Size of cybersecurity workforce worldwide in 2021, by country. Retrieved December 18, 2023 from https://www.statista.com/statistics/1172449/worldwide-cybersecurity-workforce/

[72] Ollie Stepney and Jordan Allison. 2023. Cyber Security in English Secondary Education Curricula: A Preliminary Study. In Proceedings of the 54th ACM Technical Symposium on Computer Science Education V. 1 (SIGCSE 2023). Association for Computing Machinery, New York, NY, USA, 193–199. https://doi.org/10.1145/3545945.3569758

[73] R. Sutherland, V. Armstrong, S. Barnes, R. Brawn, N. Breeze, M. Gall, and P. John, . 2004. Transforming teaching and learning: embedding ICT into everyday classroom practices. Journal of Computer Assisted Learning, 20, 6 (2004), 413-425. https://doi.org/10.1111/j.1365-2729.2004.00104.x

[74] SWGfL (South West Grid for Learning). n.d. What is online safety? Retrieved December 18, 2023 from https://swgfl.org.uk/online-safety/what-is-online-safety/

[75] Lucy Tsado. 2019. Cybersecurity Education: The need for a top-driven, multidisciplinary, school-wide approach. Journal of Cybersecurity Education, Research and Practice, 2019, 1 (June 2019), 4. https://digitalcommons.kennesaw.edu/jcerp/vol2019/iss1/4/

[76] Ethel Tshukudu, Sue Sentance, Oluwatoyin Adelakun-Adeyemo, Brenda Nyaringita, Keith Quille, and Ziling Zhong. 2023. Investigating K-12 Computing Education in Four African Countries (Botswana, Kenya, Nigeria, and Uganda). ACM Trans. Comput. Educ. 23, 1, Article 9 (March 2023), 29 pages. https://doi.org/10.1145/3554924

[77] UK Parliament. 2023. Devolved Parliaments and Assemblies. Retrieved December 18, 2023 from https://www.parliament.uk/about/how/role/relations-with-other-institutions/devolved/

[78] UNICEF (United Nations International Children's Emergency Fund). 2017. The State of the World's Children 2017. Children in a Digital World.

Retrieved December 18, 2023 from https://www.unicef.org/media/48601/file

[79] United Nations. 2021. World Economic Situation and Prospects 2022. Retrieved December 18, 2023 from https://www.un.org/development/desa/dpad/wp-content/uploads/sites/45/WESP2022_ANNEX.pdf

[80] 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”. Retrieved December 18, 2023 from https://www.govinfo.gov/content/pkg/STATUTE-79/pdf/STATUTE-79-Pg27.pdf

[81] Utdanningsdirektoratet, (n.d.). Core Curriculum: The Basic Skills. Retrieved December 18, 2023 from https://www.udir.no/lk20/overordnet-del/prinsipper-for-laring-utvikling-og-danning/grunnleggende-ferdigheter/?lang=eng

[82] Joke Voogt and Natalie P. Roblin. 2012. A comparative analysis of international frameworks for 21st century competences: Implications for national curriculum policies. Journal of Curriculum Studies 44, 3 (2012), 299-321. https://doi.org/10.1080/00220272.2012.668938

[83] Welsh Government. 2020. Science and Technology. Retrieved December 18, 2023 from https://hwb.gov.wales/curriculum-for-wales/science-and-technology

[84] Welsh Government. 2021. Curriculum and Assessment Act. Retrieved December 18, 2023 from https://www.gov.wales/sites/default/files/publications/2021-04/curriculum-and-assessment-act-explanatory-memorandum.pdf

[85] Welsh Government. 2022a. Developing a vision for curriculum design. Retrieved December 18, 2023 from https://hwb.gov.wales/curriculum-for-wales/designing-your-curriculum/developing-a-vision-for-curriculum-design/#curriculum-design-and-the-four-purposes

[86] Welsh Government. 2022b. The Curriculum for Wales – Relationships and Sexuality Education Code. Retrieved December 18, 2023 from https://www.gov.wales/sites/default/files/publications/2022-01/curriculum-for-wales-relationships-sexuality-education-code.pdf

[87] WJEC (Welsh Joint Education Committee). 2019a. WJEC GCSE in Computer Science. Retrieved December 18, 2023 from https://www.wjec.co.uk/media/jymdzl0a/wjec-gcse-comp-science-spec-2017-e-04-05-2020.pdf

[88] WJEC. 2019b. WJEC GCE AS/A LEVEL in Computer Science. Version 2. Retrieved December 18, 2023 from https://www.wjec.co.uk/media/wl4kj5l1/wjec-gce-computer-science-spec-from-2015.pdf

[89] WJEC. 2020. WJEC GCSE in Digital Technology. Retrieved December 18, 2023 from https://www.wjec.co.uk/umbraco/surface/blobstorage/download?nodeId=30232

[90] R. B. Sağlam, V. Miller and V. N. L. Franqueira, 2023, A Systematic Literature Review on Cyber Security Education for Children, IEEE Transactions on Education 66(3), 274-286, https://doi.org/10.1109/TE.2022.323101

A APPENDICES

A.1 Appendix A

Table A.1: A table of the codes used in the content analysis, their labelling as technical or socio-technical, and their description.

Code	Technical or socio-technical	Description of the code
Age appropriate content	socio-technical	Online safety content that is suitable for the age of the pupil.
Applying safety features	technical	Applying technical features to protect a device from harm.
Authentication	technical	Technical verification of data.
Consent in online relationships	socio-technical	An understanding of the need to agree for something to happen or give permission within online relationships.
Copyright	socio-technical	An understanding of exclusive legal ownership of material and implications of intellectual property infringement.
Cyber crime	socio-technical	An understanding of criminal activities occurring online.
Cyber law and legislation	socio-technical	Awareness of laws/legislation regulating personal data, misuse of data, illegal activities, etc.
Cyber threats	socio-technical	Threat of a malicious attempts to damage a network or device through unauthorized access to a network or device, This can be via destruction, denial of service or modifying information.
Data security	technical	Technical means to protect digital information from unauthorized access. This includes an understanding of how data is sent from one device to another, and how data is stored (including in binary form.
Device disposal	technical	Disposing of or getting rid of an old device, and the technical steps that need to be taken to clear it from personal data.
Device security	technical	Settings to keep computing devices secure from cyber-attacks.
Digital footprint	socio-technical	An understanding that all individuals' actions online leave digital traces and they cannot be erased.
Digital forensics	technical	A branch of Forensic Science; relates to how data can be recovered, identified and analyzed if stored electronically.
Encryption	technical	Transforming sensitive data into a form that cannot be recovered without the presence of a decryption key
Ethical data handling	socio-technical	Being transparent and respectful in handling personal data, and considering how we should handle such data.
Getting support in relation to inappropriate content	socio-technical	Pupils' knowledge of who to turn to (teacher, parent, sibling, trusted adult) when they see inappropriate content online.
Hacking	technical	Technical actions to gain unauthorized access to a device or system.
Impact of online behaviors on others	socio-technical	An understanding of how an individual's online behaviors may impact other individuals and organizations, e.g., causing online risks to them.
Inappropriate online behaviors	socio-technical	Understanding and avoiding inappropriate online behaviors in relation to their online activity and communication (e.g., in regards to avoiding discrimination of other online users because of their personal characteristics such as age, gender, disability, sexuality, and ethnicity).
Managing data threats	technical	Technical means to protect data from action that could threaten its confidentiality or integrity.
Network security	technical	How a network can be configured to protect it against attacks and to keep data confidential of users connected to it.
Online bullying	socio-technical	Awareness of forms of bullying, harassment or other similar behavior occurring online (email, social media, apps).
Online ethics	socio-technical	Morals and values in relation to online activities.

Online identity	socio-technical	Best practices on how an individual should present themselves online.
Online mis-information and dis-information	socio-technical	Awareness of the existence of false and inaccurate information (both accidental and deliberate) shared online.
Online risks	socio-technical	Awareness of risks posed online.
Online risk assessment	socio-technical	Objective consideration of a situation occurring online (e.g., in terms of risks involved), and evaluating available facts.
Online privacy	socio-technical	Awareness of the necessity of online privacy protection.
Online safety	socio-technical	Best practices on staying safe (out of harm) online, for example not over-sharing personal data.
Peer pressure	socio-technical	Danger of the influence from a friendship group or group of peers to pressure not appropriate or illegal behave online.
Privacy configuration	technical	Privacy settings and configuration of devices.
Reporting inappropriate content	socio-technical	Knowledge of how a pupil should report content which is not appropriate for their age group, that is illegal or that makes them uncomfortable.
Security breach	technical	Technical understanding of unauthorized access to a device or data.
Security threats	technical	Technical understanding of security threats.
Sexting	socio-technical	Awareness of impact of sharing sexually explicit photographs or messages.
Spam messages	socio-technical	Understanding of the concept of "spam" as unsolicited and/or irrelevant messages sent over the internet.
Password security	socio-technical	Understanding the need for setting a strong password and the importance of not sharing passwords.
Targeting vulnerable individuals	socio-technical	Awareness of unfair behavior online by targeting internet users who are less confident and/or knowledgeable using their devices.