2022

Cyber security curriculum in Western Australian primary and secondary schools: Interim report: Curriculum mapping

Nicola Johnson
Edith Cowan University

Ahmed Ibrahim
Edith Cowan University

Leslie Sikos
Edith Cowan University

Cheryl Glowrey
Edith Cowan University

10.25958/x9r3-d254
Johnson, N. F., Ibrahim, A., Sikos, L., & Glowrey, C. (2022). Cyber security curriculum in Western Australian primary and secondary schools: Interim report: Curriculum mapping. Report for the Cyber Security Cooperative Research Centre and the Office of Digital Government, WA.
https://doi.org/10.25958/x9r3-d254

CYBER SECURITY
COOPERATIVE
RESEARCH
CENTRE

Cyber security curriculum in Western Australian primary and secondary schools

Interim report: Curriculum Mapping
September 2022

Associate Professor Nicola Johnson
Security Research Institute & School of Education
Edith Cowan University
Cyber Security Cooperative Research Centre

Dr Ahmed Ibrahim; Dr Leslie Sikos
Security Research Institute & School of Science
Edith Cowan University
Cyber Security Cooperative Research Centre

Dr Cheryl Glowrey
School of Education
Edith Cowan University

The work has been supported by the Cyber Security Research Centre Limited whose activities are partially funded by the Australian Government's Cooperative Research Centres Programme.

Executive Summary

Cyber-crime poses a significant threat to Australians—think of, for example, how scams take advantage of vulnerable people and systems. There is a need to educate people from an early age to protect them from cyberthreats.

Consistent with the increasing prevalence of cyberthreats to individuals and organisations in Australia, the national Australian curriculum has been updated (version 9.0) to include specific content for cyber security for primary and secondary students up to Year 10. Endorsed by Education Ministers in April 2022, the Western Australian *School Curriculum and Standards Authority (SCSA)* completed a detailed audit of the endorsed Australian Curriculum version 9.0 against the current Western Australian curriculum. Furthermore, in 2022, SCSA undertook extensive consultation surrounding version 9.0 for all eight K-10 learning areas. This included obtaining stakeholder feedback from teachers, principals, industry professionals, universities, and system/sector representatives as well as engagement with Curriculum Advisory Committees, Steering Committees, and Curriculum and Assessment Committees. SCSA is committed to producing a high-quality curriculum that is suited for Western Australian schools including remote and regional schools.

The introduction of teaching for cyber security in the curriculum will require a cultural shift in how teachers use digital technologies in the classroom. This is vital to keep up with the expectations for teachers nationally and in WA to ensure students learn the know-how and develop all the skills required to work safely in online environments. The consistent introduction of cyber security curriculum requires effective professional learning in addition to the wide range of resources available for individual teachers and teams to access and be integrated into classroom learning. Developing a hybrid model for the delivery of professional learning on cyber security will enable opportunities for teachers to collaborate and master skills across a diverse range of schools, sectors, and geographic locations, including rural and remote locations.

Time is an important factor in ensuring that WA primary and secondary schools are ready to implement all important inclusion of cyber security additions in the revised curriculum. With the impending adoption and adaption of the national Australian curriculum version 9.0 into the WA Curriculum (K-10), WA has a unique opportunity to establish further collaborations with educational sectors, government agencies, and industry with expertise in cyber security.

Introduction

In our modern digital society, cyber security is critical to protect people and organisations from cyber-threats. There is a need to educate people, including young people so that they know how to recognise and mitigate cyber-threats. This research project maps the Australian Curriculum to examine what aspects of cyber security are covered, and to what extent, and where they are integrated in terms of learning areas and year levels. Cyber-criminals have developed practices that enable them to illegally access digital information belonging to individuals and organisations. To fight against cybercrime, people require an ever-expanding set of skills, which helps identify nefarious online behaviour, malicious software, and traits of cyberattacks. There is an opportunity to address how we might teach cyber security knowledge, skills and understanding more proactively to ensure safe, considered use of digital devices and services, and how we best position young people in WA to be cyber-aware and cyber-safe, both now and in the future. Educating young people is an investment in the future.

Computing device users constitute the weakest links in cyberspace, therefore developing the appropriate behavioural patterns early according to best practices is crucial. There are many false assumptions amongst both teachers and parents about how digitally literate children are; in fact, the prevalence of computing device use does not entail thorough theoretical background and hands-on skills in general information technology (IT), nor in cyber security. In addition, the general perception of what some groups of people believe schools teach in relation to cyber security, an increasingly important field that is not yet taught as its own learning area (e.g., Science, Mathematics), varies greatly, and cannot be used as the basis for this project.

Background

This interim report for the project *Cyber security curriculum in WA primary and secondary schools* maps the Australian Curriculum (ACARA, 2021) to ascertain what concepts and fields of cyber security are covered in the learning areas and in which year levels. The report considers the unique features of the senior secondary WA syllabus, the students' educational situation, activity, and progress, unique approaches, and methods to be used by the teacher, and the rationale in the scheme of the current curriculum.

The research partnership includes Dr Nicola Johnson, Deputy Co-Director of the Security Research Institute (SRI), associate professor of digital technologies in education, School of Education, Edith Cowan University (ECU); Dr Leslie Sikos, SRI/School of Science, ECU, who specialises in network forensics and cyber security applications powered by artificial intelligence and data science; Dr Ahmed Ibrahim, SRI/School of Science, ECU, who specialises in critical infrastructure, IT security, and cyber security risks in organisations; and Dr Cheryl Glowrey, School of Education, ECU, research assistant, who is a secondary school curriculum expert and former school principal. Upon release of this interim report, essential and important consultation with stakeholders will occur including the WA Department of Education, and the School Curriculum and Standards Authority (SCSA) alongside other key industry experts and school stakeholders.

The initial curriculum mapping project was to be based on the Western Australian curriculum published in the *Western Australian Curriculum and Assessment Outline* (https://k10outline.scsa.wa.edu.au/) which sets out the mandatory teaching, assessing and reporting on student achievement requirements for all Western Australian schools. However, the endorsement of the Australian Curriculum version 9.0 (ACARA, 2022) by Education Ministers in April 2022 created an opportunity to:

- map cyber security curriculum in preparation for classroom delivery; and
- identify the skills and knowledge that are included in the revised curriculum, potential gaps, and implications for embedding change in classroom teaching.

This was done by comparing the Australian Curriculum version 8.4 with version 9.0. From here, please note the Australian Curriculum refers to the national Australian curriculum released by the Australian Curriculum and Assessment Authority (ACARA). The WA curriculum refers to the adopted and adapted *Western Australian Curriculum and Assessment Outline*. In WA, Year 11 and 12 content is referred to as the syllabus content subject; in Pre-primary to Year 10 the content is referred to as the curriculum.

Rationale for cyber security in school curriculum

Cyber security supports Australian businesses and citizens to prosper by enabling people to manage and remove threats to interactions using digital technologies more confidently. The Alice Springs (Mparntwe) Education Declaration (COAG, 2019) sets out the vision for education for young Australians by state and territory Ministers for Education. The first goal is for the Australian education system to promote excellence and equity; the second is for all young Australians to become confident and creative individuals, lifelong learners, and active and informed members of the community (COAG, 2019). Consistent with these two goals, the Australian Curriculum aims to enable all young Australians to become successful learners, confident and creative individuals, and active and informed citizens (ACARA, 2022).

Three critical roles of cyber security curriculum

The three aspects underpinning additions to cyber security teaching and learning in the Australian Curriculum version 9.0 are developing the knowledge and skills for individuals, as members of contemporary digital society and as potential participants in the cyber security workforce (see Table 1). These revised curriculum documents consider ethical and safe online behaviour, resilience and wellbeing, the capacity to manage and protect digital data, ongoing learning about future cyberthreats and the pre-requisite skills and knowledge for seeking further training and education in cyber security.

In terms of the critical shortfall in an emerging skilled cyber security workforce, the Australian Government acknowledges that cyber security is one of the fastest growing employment sectors with an estimated generation of 17,000 new jobs by 2026 (Commonwealth of Australia, 2020). The school curriculum has a role in developing skills and knowledge that engage students in thinking about working in the industry in the same way that the curriculum enables students to make choices about potential career opportunities in a wide range of nationally important industries.

Table 1: Three critical purposes of cyber security curriculum

	Curriculum focus
Cyber security & digital citizenship: *Cyber security actions & responsibilities for individuals*	• Ethical and safe online behaviours • Resilience and wellbeing
Cyber security in an interconnected digital world: *Digital connections to others at home, school & work*	• Recognising & responding to cyber security threats to shared data • Capacity for ongoing learning about cyber security
Cyber security expertise for the workforce: *Developing aspirations & capacity to seek further training and education in cyber security*	• Pre-requisite skills and knowledge for future training, education & work • Understanding systems, networks & threats

Scope of curriculum mapping for this report

This curriculum mapping project examined documents where teaching knowledge and skills specific to cyber security are the focus. The analysis considered learning areas, the developmental continuum for learning knowledge and skills, prerequisites to understand the relevant concepts in the Australian Curriculum Foundation to Year 10 (F–10) version 9.0, and the WA SCSA Senior Secondary syllabuses of *Computer Science* and *Applied Information Technology*. These curriculum documents articulate the content and standards for teachers to implement in all primary and secondary schools from kindergarten through until the completion of Year 12. The curriculum mapping for this report focuses specifically on the Australian Curriculum (F–10) Version 9.0 as it will inform what SCSA adapts, adopts, and stamps as the approved WA curriculum (Pre-primary to Year 10) and the syllabus (11-12).

It should be noted that each state and territory has its own interpretation and version of the curriculum. Specific to WA, children start school at age 5 at the beginning of the year in pre-primary. Kindergartens are for 3-4-year-olds and can be located on school sites. In other states, the first year is foundation (F) and kindergartens are typically located on separate sites. Each state has its own curriculum authority which has the right to interpret and determine what aspects of a national curriculum version will be approved to be taught in that state. One example is from the Victorian Curriculum and Assessment Authority who excluded *information and communication skills* as a *general capability*.

Developing knowledge and skills in cyber security are best learned within the context of the broader applications of digital technologies in schools. The knowledge and skills developed in other learning areas and particularly, in other strands of the Digital Technologies subject, contribute to student confidence in connecting digitally and identifying cyber security threats and being able to take actions to mitigate risks. The wide range of informal digital learning experiences students engage in as they progress through school are important, but beyond the scope of this report. In the school context, teachers bring diverse perspectives, knowledge, and skills to this wider application of digital technologies across the curriculum. Interactions within a school and classroom, planned or unplanned, between teachers and their students contribute to what is learned in ways that mediate the written curriculum. Extra-curricular activities, such as competitions, or presentations by experts in cyber security are also valuable experiences for students. In addition, digital knowledge and skills that are learned out of school through interactions with family and friends, or self-learned mean that

many students bring their own lived experiences to classroom learning. However, assumptions that *all* students acquire sufficient knowledge and skills about cyber security to respond to diverse and changing threats outside of school risk increasing the proportion of future Australians who are vulnerable to the activities of cyber-criminals.

The consultation for an Australian senior secondary curriculum continues to take place. The curriculum for the Digital Technologies subject has only been endorsed from K-10, hence there is no Australian wide year 11 and 12 curriculum included in this report, other than the two subjects endorsed by SCSA WA as the syllabus, i.e., *Computer Science* and *Applied Information Technology*. In WA, the finalised units published on the SCSA website state the new Year 11 Computer Science ATAR syllabus will be implemented in 2023 and Year 12 Computer Science ATAR syllabus in 2024.

The structure of the Australian curriculum

The Australian Curriculum (F–10) is the national curriculum written under the authority of the Australian Curriculum and Assessment Authority (ACARA) and agreed upon by the State and Territory Ministers for Education in 2015. The Australian Curriculum (F–10) describes what is to be taught and the quality of learning expected for all young people regardless of where they live. It is designed to help all young Australians to become successful learners, confident and creative individuals, and active and informed citizens. The Australian Curriculum (F–10) was recently reviewed according to the agreed six-year timeline and endorsed by all state Ministers of Education at the beginning of April 2022 (ACARA, 2016).

The Australian Curriculum (F–10) is structured into three components:

- **learning areas** (n=8)**:** English, Mathematics, Science, Health and Physical Education, Humanities and Social Sciences, The Arts, Technologies, and Languages.
- **general capabilities** (n=7)**:** literacy, numeracy, information, and communication technology capability (digital literacy in version 9.0), critical and creative thinking, personal and social capability, ethical understanding, intercultural understanding.
- **cross-curricula priorities** (n=3)**:** Aboriginal and Torres Strait Islander Histories and Cultures, Asia and Australia's Engagement with Asia, and Sustainability.

The Technologies learning area includes two subjects: digital technologies and design technologies. General capabilities and cross-curricula priorities are designed to be taught across all subjects to add depth to teaching and learning. They are intended to play a significant role in equipping young Australians to live and work successfully in the twenty-first century. In the Australian Curriculum, the general capabilities encompass knowledge, skills, behaviours, and dispositions which are developed when they apply knowledge and skills confidently, effectively, and appropriately in complex and changing circumstances, in their learning at school and in their lives outside school.

Table 2: Example of Structure of Australian Curriculum, Level 4 (Years 5–6)

Learning Area	Strand	Sub-Strand	Curriculum Content Descriptions	Content Elaborations	General Capabilities
Technologies - Digital Technologies (subject)	*Processing & production skills*	• Privacy & data security	Access multiple personal accounts using unique passphrases and explain the risks of password re-use (AC9TDI6P09)	Using multiple accounts each with different passwords, to access each website account or app used for school or home, for example having a different username and password combination for school, gaming and music accounts. Explaining why re-using a password is risky when one of them is found out, for example how a compromised password from one social media account might be able to be used to access their bank or school account if their password is the same and other details are compromised.	**Digital Literacy** *Managing & operating* • Protect content

The Australian Curriculum (F–10) is a framework written as a developmental continuum of knowledge and skills where achievements are expressed as outcomes. In other words, what students will be able to know and do at the completion of a level. Apart from the first Foundation year, the curriculum is divided into bands of two years; Years 1 & 2 are called Level 2; Years 3 & 4 are Level 3, etc. Australian Curriculum elaborations have never been used in the Western Australian Curriculum. This is because Western Australia unbanded ACARA's curriculum into year level syllabuses, and instead of elaborations, provided exemplifications of students' work.

The seven general capabilities in both the Australian Curriculum and Western Australian curriculum are:

- Information and Communication Technology capability (retitled as Digital Literacy capability in the Australian Curriculum version 9.0)
- Critical and Creative Thinking capability
- Personal and Social capability
- Ethical Understanding capability
- Intercultural Understanding capability
- Literacy capability
- Numeracy capability
- Critical and creative thinking capability

These capabilities complement curriculum content but are not assessed in Western Australian schools.

State and territory implementation of the Australian Curriculum

The Australian Curriculum can be implemented flexibly by relevant state and territory authorities, according to jurisdictional and system policies, to develop programs that meet the educational needs of their students and that extend and challenge students. States and territories make decisions about the extent and timing of take-up and translation of the intended Australian Curriculum (F–10) into the curriculum that is experienced by students (ACARA, 2016). They implement the Australian Curriculum (F–10) in ways that value teachers' professional knowledge, reflect local contexts and consider individual students' family, cultural and community backgrounds.

Progress with implementation of the full scope of the Australian Curriculum in each state and territory level is informed by, amongst other things:

- the readiness of their systems, schools, and teachers
- the extent of change from current curriculum provision
- available resources
- existing curriculum development cycles and processes.

Currently, states and territories are teaching the Australian Curriculum (F–10) version 8.4. In April 2022, the revised Australian Curriculum (F–10) Version 9.0 was endorsed by Education Ministers, for implementation in 2023, although each state and territory can set an appropriate timeline for implementation. In WA, this first must be revised and approved by SCSA as the curriculum authority. The interpretations of Version 9.0 SCSA make, establish, and sign off on through extensive processes of consultation, reporting and accountability will eventually become the WA Pre-primary – Year 10 curriculum and senior secondary syllabuses.

Teaching, assessment, and reporting

Teachers are expected to teach and assess general capabilities to the extent that they are incorporated within each learning area. State and territory school authorities will determine whether and how student learning of the general capabilities will be further assessed and reported (ACARA, 2016).

In schools, teachers are responsible for preparing resources and materials that will engage students in learning the knowledge and skills described in curriculum documents at an appropriate cognitive level for the individual. It is expected that students will be achieving at various levels in each classroom. Teachers are accountable for the evidence of learning that takes place in their classrooms, and they do this through assessment. Learning can only effectively be assessed based on what students write, say, do or make. As a result, teachers are required to plan for learning, teach students in such a way that students can demonstrate their learning and then assess the ability that is evidenced. This is a complex and highly skilled process, the results of which are formally reported to parents twice each year.

Summary of key points

Australian state and territory governments agreed to a national school curriculum in 2015, known as the Australian Curriculum (F-10). State and territory education authorities can adapt and implement the Australian Curriculum (F-10) in keeping with system and teacher readiness, established procedures for curriculum review and the availability of resources. Agreed standards for student achievement are included in the Australian Curriculum (F-10). Assessment and reporting requirements are tied to Commonwealth funding arrangements to ensure a common national standard.

Cyber security curriculum in WA primary and secondary schools

The WA School Curriculum and Standards Authority (SCSA) is responsible for the curriculum, assessment standards and reporting processes for all primary and secondary schools in the state. SCSA determines changes to curriculum, syllabuses, and resource materials, both in terms of adopting and/or adapting the Australian Curriculum for the Western Australian context, and for updating Year 11 and 12 syllabuses based upon curriculum development cycles and processes. In WA, schools and teachers have been advised by SCSA that they should continue teaching the current *Western Australian Curriculum and Assessment Outline* until advised otherwise.

In terms of cyber security in the curriculum, while it is appropriate to follow established processes for curriculum revision in WA, these are inherently time-consuming, particularly given the number of stakeholders within the state likely to be involved in consultation processes. The School Curriculum and Standards Authority has well-established consultation processes with the schools systems and sector, schools and other stakeholders, such as universities and professional associations. As was evident during the recent COVID pandemic and the need for remote learning by school children, cyber security is a current issue if students are to be equipped to deal with threats such as phishing, malware, and scams.

WA Kindergarten – Year 10 (K–10) Curriculum

The structure of the WA curriculum (K–10) differs from the Australian Curriculum (F-10). Content and assessment are divided into single year levels, unbanding the levels of the Australian curriculum. That is, in WA, teachers have a clear set of curriculum points they are required to teach at each year level rather than an expectation that they will teach and assess a broader content over a two-year band. Teachers in Western Australia are required to teach all the year-level content and assess a representative sample of year-level content to report student progress against the Achievement Standard. The Western Australian Curriculum was adapted and adopted from the Australian Curriculum and while it contains content from the Australian Curriculum, content was adapted and written to meet the needs of Western Australian students and teachers. The initial scoping analysis of references to cyber security

and the language used in the Australian and Western Australian curriculum documents suggest that cyber security is a consistent, but minor point in terms of ethical and safe behaviour. We do acknowledge the F-10 Health and Physical Education Australian curriculum version 9.0 does include a focus on online safety, avoidance of risk, and the evaluation of digital sources.

Access to cyber security curriculum

SCSA provides recommendations to schools for the time allocation of curriculum disciplines (SCSA, 2016). The notional time allocations provide schools with guidelines for student learning across all learning areas until the completion of Year 8. To illustrate, mathematics and English are allocated much more time per week in each state across Australia compared to health and physical education for example, which may only be taught for 1-2 hours per week. In Years 9 and 10, the learning areas of Languages, Technologies (including Design and Technologies, and Digital Technologies), and The Arts are optional. As a result, many students will not have the opportunity to experience the cyber security curriculum within Digital Technologies intended for this stage. In effect,

- Students who elect the Digital Technologies subject from Year 9 might be regarded as having a higher level of interest and/or a future career in ICT.
- Teachers from all subject areas in Years 9 and 10 share the responsibility for cyber security curriculum through the General Capability of Digital Literacy. Some teachers of Year 9 and 10 will be required to teach the General Capability of Digital Literacy in other learning areas.
- There are no teacher assessment requirements for General Capabilities.

Western Australian Senior Secondary Curriculum (Years 11 and 12)

SCSA is responsible for all curriculum in the Western Australian Certificate of Education (WACE) and the two subjects that provide the key teaching for cyber security in Years 11 and 12 are:

- Computer Science
- Applied Information Technology

It should be noted that the current Western Australian senior secondary school curriculum includes consideration of the general capabilities in ICT (Australian Curriculum 8.4).

In the high stakes learning and assessment environment of Years 11 and 12, the emphasis in the classroom will, in most cases, be focused on content which is most likely to be examined. Individual teachers may teach about cyber security based on their own knowledge and skills. The lack of direct assessment requirements related to cyber security in the current curricula for these two senior secondary subjects suggests that this would be *ad hoc* in nature across the school system. It should be noted WA is the only jurisdiction to include cyber security in its senior secondary syllabus.

Summary of key points

SCSA are responsible for the WA Curriculum (K-10) and the senior secondary syllabus. The WA Curriculum (K-10) differs from the Australian Curriculum (F-10) with single year level content and therefore includes unique WA content descriptions to facilitate the additional number of levels. SCSA have advised schools and teachers in WA that they should continue to teach the current curriculum, based on the Australian Curriculum (F-10) version 8.4 until they have been able to undertake the adaption and adoption processes of version 9.0 for the WA curriculum and assessment outline. Design and consultation procedures suggest that the WA curriculum and assessment outline version of 9.0 will have a staggered implementation over 2024 – 2027 in WA. Western Australia has a long standing history of 'adopting and/or adapting' the Australian Curriculum and this will continue. The Authority will coordinate the collaboration between the school systems and sectors, as it has in the past, to ensure that any changes to the mandated Western Australian curriculum are well considered and consulted before being finalised.

Access to cyber security content in the WA Curriculum (P-10) is primarily through Digital Technologies and the General Capability: Information and Communications Technology Capability. All students in WA experience Digital Technologies curriculum from Pre-primary to Year 8, after which it becomes an elective subject. The General Capability is embedded in all learning areas, including the Years 11 and 12 (ATAR) courses of Computer Science and Applied Information Technology.

Cyber security in Australian Curriculum version 9.0

In terms of cyber security curriculum, significant changes have been made in version 9.0 to reflect the need to better prepare young people to participate confidently in a changing digital world.

Revisions to the Australian Curriculum were open to a public consultation via a survey and email feedback for education stakeholders over 10 weeks between 29 April and 8 July 2021. Responses were received from a wide range of educators and education peak bodies, social groups, government, and industry groups.

The following comments reflect responses from the Western Australian peak body invited to provide feedback to ACARA. In response to the revised (F–10) Digital Technologies curriculum, the Western Australian response made overall comments, noting that several aspects of the Digital Technologies curriculum required further revision. In particular, the new sub-strand for Privacy and security was supported at (F–6) but should be incorporated into the Digital Literacy General Capability for Years (7-10). Western Australia also indicated that some terminology used in the Digital Technologies curriculum was too specialised for general primary school teachers (ACARA, 2021b).

The General Capability of information and communication technology has been renamed Digital Literacy in version 9 to align with international developments and the findings of recent national reports, while the curriculum has been embedded in the Digital Technologies content (ACARA, 2021a). Generally, the consultation process for Digital Literacy showed that respondents believed the changes to be more relevant to the 21st century but generally thought there needed to be more content covering information sharing (ACARA, 2021a). The Western Australian response agreed the curriculum structure had improved for the new Digital Literacy capability, but that there was too much content and that in places, it created confusion with the curriculum for Digital Technologies (ACARA 2021a).

Developmental structure of the Australian Curriculum 9.0

The Australian Curriculum 9.0 reflects the need to focus on cyber security as a visible set of skills and knowledge for students to achieve as shown in the comparative tables provided by ACARA (see separate documents). This is evident in the new sub-element to the Digital Technologies curriculum, Manage Digital Privacy and Identity. It is also evident in the new title for the former General Capability in Information and Communications Technology to Digital Literacy.

The curriculum is developmental and begins with clarity of language for skills and knowledge to be learned from Foundation, which is the equivalent to pre-primary in WA.

The language of cyber security in the curriculum

A significant difference between the revised Australian Curriculum (F–10) and the current P-10 and senior secondary curriculum is in the language used to reflect knowledge and skills which we would now recognise as cyber security curriculum. The language in version 9.0 is more specific than in the previous version. This presents an ideal opportunity to clarify the skills and knowledge for students to learn by using the specialised language associated with cyber security.

Table 3: Inclusion of relevant skills and knowledge to teach common cyber security threats in the Australian Curriculum 9.0: Curriculum Area, Strand & Band

Common Cyber security Threats	Learning Area/General Capability, Strand & sub-strand	Content Description	Band
Crypto (currency) mining	**Digital Technologies** *Processing and production skills: Privacy and data security*	develop cybersecurity threat models, and explore a software, user or software supply chain vulnerability	Band 9-10
Data Spill/data breach	**Digital Literacy** *Practising Digital safety and wellbeing: 2. Manage digital privacy and identity*	recognise that their digital footprint is valuable, used by online tools for targeting, and that data shared online is no longer under their control	Level 5 (Years 7 & 8)
Denial of Service (DDoS attack)	**Digital Technologies** *Processing and production skills: Privacy and data security*	develop cybersecurity threat models, and explore a software, user or software supply chain vulnerability	Band 9-10
Hacking	**Digital Literacy** *Practising Digital safety and wellbeing: 2. Manage digital privacy and identity*	protect content when sharing by selecting appropriate access controls for individuals and shared links for wider groups	Level 5 (Years 7 & 8)
Identity Theft	**Digital Technologies** *Processing and production skills: Privacy and data security*	access multiple personal accounts using unique passphrases and explain the risks of password re-use	Band 5-6
Malicious Insiders	**Digital Technologies** *Processing and production skills: Privacy and data security*	develop cybersecurity threat models, and explore a software, user or software supply chain vulnerability	Band 9-10
Malware	**Digital Technologies** *Processing and production skills: Privacy and data security*	develop cybersecurity threat models, and explore a software, user or software supply chain vulnerability	Band 9-10
Phishing – scam emails	**Digital Technologies** *Processing and production skills: Privacy and data security*	explain how multi-factor authentication protects an account when the password is compromised and identify phishing and other cybersecurity threats	Band 7-8
Ransomware	**Digital Technologies** *Processing and production skills: Privacy and data security*	develop cybersecurity threat models, and explore a software, user or software supply chain vulnerability	Band 9-10
Scams	**Digital Technologies** *Processing and production skills: Privacy and data security*	explain how multi-factor authentication protects an account when the password is compromised and identify phishing and other cybersecurity threats	Band 7-8
Web shell malware	**Digital Technologies** *Processing and production skills: Privacy and data security*	develop cybersecurity threat models, and explore a software, user or software supply chain vulnerability	Band 9-10

Summary of key points

In accordance with the agreed schedule, the Australian Curriculum (F-10) was reviewed in 2020–2021 to examine where changes might be required to continue to meet the goals for educating young Australians in a changing global and national society. The revised Australian Curriculum version 9.0 was launched in April 2022 with advice that it could be implemented by state and territory education authorities from the beginning of the 2023 school year.

Consistent with the increasing prevalence of cyber security threats to individuals and organisations in Australia, the curriculum has been updated to include specific knowledge and skills to better prepare young Australians. The General Capability: Information and Communications Technology Capability is now the General Capability: Digital Literacy with a stronger emphasis on teaching online safety. The learning area of Digital Technologies has a new sub-strand, *Privacy and data security*, which is aimed at teaching a continuum of knowledge and skills from the pre-requisite ability to protect personal data to systems analysis for cyber security threats.

A significant feature of the revised Australian Curriculum version 9.0 is the increased specificity of language related to cyber security, which clarifies to teachers that these are skills and knowledges (content) that must be taught. Not all content needs to be assessed, only that which is in the achievement standards.

Revisions to the WA senior secondary syllabus

In WA senior secondary subjects are regularly reviewed and updated following consultation with schools, teachers, and assessors. In 2022, the syllabus for Computer Science (ATAR) was revised through extensive consultation and has been finalised on the SCSA website. Reviews of courses typically occur over a five-year-cycle.

In recognition of the increasing importance of cyber security, the content for Unit 2 has been updated and renamed *Design and development of database solutions and cyber security considerations*. In their consultation notes, SCSA explain strengthening the content on cyber security as aligning with university expectations. The content covered includes ethics and law, understanding privacy; network security, distinguishing between the different methods used to compromise the security of a system; and, cryptography, recognising common cyphers, their substitutes, and breaking substitutes (Table 4).

The inclusion of cyber security content is further prioritised in the assessment guidelines for Year 11 Computer Science, which explicitly require teachers to grade on a student ability to explain network threats and security solutions. A deeper understanding then simply the explanation is required and incorporated in the syllabus. Grading is not based on one section of the syllabus, rather at the end of the Year or unit based on the collective suite of student work. Grading cannot be completed based on one element of the syllabus.

Table 4: Western Australian Senior Secondary Curriculum: Examples of skills and knowledge for cyber security in revised Computer Science (ATAR) curriculum

Year 11 Unit 2: Design and development and cyber security considerations	
Cyber security **Ethics and Law** **Knowledge** · role of ethical hacking in network security purpose (improving security) penetration testing comparison with unethical hacking · role of the Privacy Act 1988 · the concept of the Australian privacy principles · Australian Privacy Principles in relation to keeping data secure **Network security** **Knowledge** · authentication characteristics of strong passwords organisational approach to password policies password policies impact on data security two-factor authentication · encryption purpose of encryption public vs private key encryption	**Network threats** **Knowledge** • distinguish between the different methods used to compromise the security of a system: social engineering (phishing)* denial of service back door IP spoofing SQL Injection man-in-the-middle cross-site scripting types of malware physical security threats ** zero-day vulnerabilities **Cryptography** **Knowledge** • purpose of cryptography • plain text vs cipher text • common ciphers substitution rotation cipher random substitution polyalphabetic cipher (e.g. Vigenère) methods for cracking substitution ciphers brute force frequency analysis **Skills** • use common ciphers

The content in Table 4 is taken directly from the source. We note the following under 'network threats'. The list is quite convoluted. For example, some of the words are listed as nouns, others as adjectives—see denial of service listed (as opposed to denial-of-service attacks) vs man-in-the-middle (as listed, incorrectly), which should be either "man-in-the-middle-attacks" or "man in the middle", but considering the bullet point under which these are, the first one would be the only correct way of writing this. * Phishing is just one type of social engineering, but the two concepts are not interchangeable. ** A physical security threat is not a method of compromise.

Summary of key points

The WA consultation process for revisions to the senior secondary subject, Computer Science (ATAR) has closed and the syllabus has been finalised. A significant change in the new curriculum is the inclusion of cyber security in Unit 2, traditionally semester 2 of Year 11, named *Design and development and cyber security considerations*. The curriculum mandates teaching in specific aspects of cyber security knowledge and assessment of student learning about network threats and security solutions.

Cyber security skills and knowledge required by students and teachers

The digital environment is constantly changing as new technology is released for consumers and in the world of work. For this reason, the skills and knowledge required by students *now* will be superseded within a short space of time. Therefore, cyber security curriculum skills and knowledge are required to provide both a set of skills which will equip students with key skills to manage and protect their own data, understand the risks associated with cyber security threats and be prepared for ongoing learning. In addition, senior secondary curriculum has a key role to play in developing skills and knowledge for students studying with the aim of working in ICT industries, including emerging careers in cyber security.

Cyber security skills and knowledge required by students

The actions that individuals and families might take to protect themselves from common cyberthreats are included on the Australian Cyber Security Centre (ACSC) website, and for the basis of a series of educational resources for young people (ACSC, 2022). When mapped against the Australian Curriculum (F-10) version 9, it is evident that these skills, which might be considered pre-requisite skills for all young Australians to learn are only partly explicit in the content descriptions. By implication, the opportunity to learn a broader set of skills will be dependent on the knowledge and skills of individual teachers, the resources made available or the professional learning experiences associated with cyber security curriculum. Table 5 (below) lists the actions to take for individuals and families to protect themselves against common cyber security threats. The second column points to where evidence of these actions being taught are included (or not) in the Australian Curriculum version 9.

Table 5: Australian Cyber Security Centre (ACSC): actions suggested to individuals and families to protect against common cyber security threats

ACSA recommended actions to protect against common cyber security threats	Evidence of teaching in Australian Curriculum 9.0
Use strong passwords	**Digital Technologies:** Processing and production skills: Privacy and data security
Avoid re-using passwords	**Digital Technologies:** Processing and production skills: Privacy and data security
Use two factor or multi factor authentication	**Digital Technologies:** Processing and production skills: Privacy and data security
Practising safe online browsing	**Digital Literacy:** Practising Digital safety and wellbeing: Manage online safety
Limit information shared online	**Digital Literacy:** Manage digital privacy and identity; Protect content
Only click on trusted or recognised links (email, social media, SMS …)	**Digital Technologies:** Processing and production skills: Collaborating and Managing
Backing up important information	Not explicit in content descriptions
Set social media settings to 'private'	Not explicit in content descriptions
Use anti-virus software	Not explicit in content descriptions
Install software updates	Not explicit in content descriptions
Communicate concerns and seek help	Not explicit in content descriptions

All students experience General Capability: Digital Literacy curriculum to Foundation to Year 10. In Western Australia, the General Capabilities continue into Years 11 and 12. The knowledge and skills learned through the General Capability in Digital Literacy are focused on ethical behaviours and personal resilience and wellbeing.

The Digital Technologies curriculum discipline becomes an elective at Years 9 and 10, with the implication that many students who choose to specialise in other curriculum areas will gain only a basic level of skills and knowledge in cyber security curriculum as shown in Table 1.

Students who continue to specialise in senior secondary subjects of Computer Science and Applied Information Technology will continue to enhance their skills and knowledge at a level that may prepare them to apply for emerging careers in the cyber security industry. Additional programs and curriculum are already present as an opportunity for Western Australian schools. As part of the Western Australian Certificate in Education (WACE), Years 11 and 12 students with an interest in cyber security can select to study ATAR and/or General courses or pursue a VET qualification. Certificate courses, up to and including a Certificate 4, are delivered in many schools with a focus on information and digital media technologies. Other programs endorsed by the Authority as part of students achieving a WACE include CISCO

networking and cyber security courses and Codemaster institutes web development courses. This range of courses provides a broad choice for student engagement with all aspects of digital technology, including cyber security.

Cyber security skills and knowledge required by teachers

Schools and teachers work within a curriculum environment that is crowded with priorities to meet accountability requirements such as the National Assessment Program – Literacy and Numeracy (NAPLAN), senior secondary external examinations and teacher assessments across a broad curriculum. This is especially true at the middle school level. They are also required to engage students in learning.

The introduction of new curriculum material for cyber security requires information about how students might demonstrate their learning for assessment. Suggestions for teachers are currently provided in the curriculum elaborations for each curriculum point in the Australian curriculum.

All school teachers require the appropriate levels of skills and knowledge to confidently teach cyber security curriculum in the classroom. In primary schools, in most cases, the generalist classroom teacher will be required to teach and assess student ability in Digital Technologies as a subject and to also embed the General Capability of Digital Literacy. Secondary school teachers of Years 7 and 8 will require the appropriate skills and knowledge to confidently teach and assess student ability if they are teaching in the specialist subject of Digital Technologies. For example, the Australian Curriculum 9.0 suggests that this capability might be taught in subjects like Mathematics and Health and Physical Education. The knowledge and skills required by secondary teachers to enrich the curriculum/syllabus through the General Capability of Digital Literacy continues throughout Years 9 to 12.

Teachers of students who elect to enrol in Digital Technologies subjects in Years 9 and 10 will be required to confidently teach and assess increasingly specialised knowledge and skills appropriate to cyber security. Where students continue into the WA syllabus - Computer Science and Applied Information Technology - the teachers will require high level ability to teach and assess student ability.

Implications are:

- all primary school teachers will require a confident knowledge of cyber security elements in the subject of Digital Technologies.
- all primary school teachers and secondary school teachers when they are delivering subject content that addresses the General Capability of Digital Literacy will require the knowledge and skills to confidently teach and assess students in cyber security curriculum.
- WA secondary school teachers in the subject of Digital Technologies and the senior secondary syllabuses of Computer Science and Applied Information Technology will require high level skills and knowledge to teach and assess the cyber security content in the curriculum.

In the dynamic digital environment of cyber security, teachers may be expected to regularly update their skills and knowledge. Access to engaging teaching resources and professional learning will be an essential part of ensuring teachers are able to meet the need for new knowledge and skills.

Summary of key points

The common actions individuals and families can take to protect from cyberthreats include pre-requisite skills such as multi factor authentication, strong passwords, backing-up data, 'private' social media settings, etc. Many of these are listed in the Australian Curriculum (F-10) version 9.0 to be taught explicitly across Levels 4–5 (Years 5–8) in the Digital Technologies subject. A focus on these skills and the fact that continuing efforts by criminals and others to threaten cyber security means there will a need for ongoing learning to protect data will ensure all young Australians can continue to connect safely, collaboratively, and creatively in the future.

Teachers across all curriculum areas where Digital Technologies is a classroom resource will require the same levels of pre-requisite skills. In addition, teachers should be able to explain why these are important skills for students when asked and therefore will require a deeper understanding of the roles these pre-requisite skills play in cyber security. Teachers have a preeminent role to play in reinforcing messages about ongoing learning for young people.

WA teachers of Digital Technologies at Years 9–10 and senior secondary Computer Science, who have students electing to study with a potential career in mind, work with an increasingly sophisticated understanding of cyber security as curricula revisions respond to changing digital environment. It is imperative that teachers can access the skills and knowledge to implement these changed aspects of the curriculum for their subjects.

Implementing cyber security curriculum in schools

Schools throughout Australia respond to complex and at times competing policy and procedural requirements for teaching and learning. Cyber security skills and knowledge are widely recognised as important to the development of confident Australian citizens and the future Australian economy. Curriculum changes to strengthen the focus on cyber security skills and knowledge for students is a critical step in achieving better outcomes for young people, however embedding new learning and teaching in the curriculum also requires:

- Developing teacher capacity to deliver cyber security skills and knowledge
- Resources for teachers

Resources for schools

The Australian Curriculum includes guidelines for teachers for each curriculum point listed. These dot points 'elaborate' the possibilities for teachers, however, are not mandatory.

Digital learning resources aligned with the Australian Curriculum are provided through *Scootle*, a website managed by Education Services Australia and supported by the Australian

Government Department of Education. *Scootle* is free for all school educators, including pre-service teachers.

Resources for online safety provided through the Australian government eSafety Commissioner website are provided for teachers and schools to access. The ACSC was established by the Federal Government in 2020 in response to the government's commitment to a revised cyber security strategy (2020). The ACSC website provides advice to Australian businesses, families, and individuals. Mapping the common cyber security threats to families and individuals listed on the ACSC website against the Australian Curriculum 9.0 (F – 10) indicates that the General Capability Digital Literacy and the Digital Technologies curriculum area develop a range of skills and knowledge that will enable students to be aware of and manage cyber security threats. However, the level at which students will be able to identify cyber security threats varies and is limited by the lack of specific examples and language included in the curriculum documentation. It should be noted teachers use the mandated curriculum to plan for teaching and learning. Teachers make decisions about learning strategies and contexts and/or examples to use, allowing for school and students' needs.

Organisations and associations providing curriculum support for teachers, such as the Educational Computing Association of Western Australia (ECAWA), the Australian Council for Computers in Education (ACCE) and the Australian Computer Society (ACS), are valued by teachers who become members. Commercial providers of learning resources, both digital and in the form of traditional textbooks are responsive to changes in the curriculum at a national and state level.

Professional learning for teachers

The Alice Springs (Mparntwe) Education Declaration (COAG, 2019) acknowledges the role of teachers in shaping the lives of young Australians and calls for a commitment by Australian Governments, the education community, and universities to work in partnership to foster high quality teaching, including through the provision of ongoing professional learning. Making reference to an information technology rich society, the declaration calls for opportunities for educators to "continually develop their own skills, in order to teach young Australians the essential skills and core knowledge needed for a modern society and economy" (COAG, 2019).

Successfully introducing and embedding significant curriculum change in schools to address student learning in cyber security relies on effective professional learning for curriculum leaders and classroom teachers in diverse settings in primary and secondary schools in Western Australia. The imperative to address professional learning as a priority for educators is stated in in the policy document *Students Online in Public Schools Procedures Version 3.2*, Point: 3.3.1 Personal information, privacy, and confidentiality: "Site Managers must confirm that staff have educated students of the risks associated with any online activities and how to adopt protective online behaviour to avoid exposure to inappropriate online material or activities" (WA DET, 2019). It should be noted this policy only applies to Department of Education schools. Registered teachers in Western Australian are required to complete 100 hours, or pro rata, of professional learning to maintain their status. The Australian

Professional Standards for teachers require teachers to "use ICT safely, responsibly and ethically" with students (AITSL, 2017, Standard 4.5).

The relationship between effective professional development and improved student outcomes is well known (Loughland & Nguyen, 2020; Timperley, 2008). Earlier iterations of systemic change initiatives that relied on mandated and/or event based professional development to introduce new teacher practices had a limited impact on student outcomes. Such formats for professional learning failed to take account of the social, relational, and contextual sites for teacher learning and practice (Forde & McMahon, 2019). Parr and Timperley (2010) found that a whole school focus resulted in coherence for professional learning, and that a process of developing shared goals and agreed evidence of student learning to measure improvement with participants was more effective. Therefore, a single program delivered by facilitators was less effective than engaging participants in a dialogic approach about the purpose and outcomes of their learning (Parr & Timperley, 2010). Effective professional learning occurs within groups of teachers working together on changing practices. Professional learning should be relevant, collaborative, and future focused (AITSL, 2014).

Factors that contribute towards effective professional learning include developing an explicit theory of action, the integration of theory and practice, and collaboration (Timperley, 2008; Loughland & Nguyen, 2020). When designing professional learning for teachers, the teacher's perceived sense of their collective efficacy measured an effect size of 1.57 through meta-analysis (Hattie, 2015). The gaining of mastery of new learning by teachers who are successful in active learning experiences increases collective self-efficacy most effectively and enables vicarious learning that occurs through participation in the collective. Research indicates that teachers may engage with professional learning across multiple dimensions: sources internal to the confines of the classroom; sources external to the classroom; research and theory; and collaborative experiences (Pedder & Opfer, 2013 cited by Forde & McMahon, 2019).

The complexity of the ways in which teachers engage with professional learning and the diversity of schools suggests that there can be no single approach to professional learning. Timperley (2015b) refers to *adaptive expertise* as the disposition required for teachers to navigate ongoing complex and constantly changing technological and societal contexts. Adaptive expertise recognises the need for teachers to take agency for their own professional learning to improve outcomes for students both as individuals and collaboratively, reflecting on practice and challenging existing assumptions about teaching and learning. Leadership of effective professional learning involves engaging the curiosity of teachers (Timperley, 2015a). Timperley (2015a) frames professional learning within spiral of inquiry, learning and action with two key questions: "what's going on for learners?" and "How do we know?". Timperley's research identified a sense of competency, relevance and clear purpose within a collaborative context underpinned effective professional learning for teachers, noting that "learning opportunities need to be differentiated according to the prior knowledge and skills of the learner" (Timperley, 2015a, p. 7).

Regional, rural, and remote schools

In Western Australia, the diversity of school contexts includes schools located in regional, rural, and remote (RRR) settings where access to quality professional learning is limited. Technology enables personalisation, collaboration, access, efficiency and learning designs (AITSL, 2014). Creating a school-based learning community to engage collectively with new skills and knowledge is made more challenging, particularly when the availability of digital technologies is itself an issue (DESE, 2018). A survey of emerging global trends in professional learning offers a framework for developing hybrid models of delivery to enable opportunities for collaboration, mastery and immersion in future focused learning tailored for diverse school contexts:

- *Integrated: Professional learning and performance and development are closely connected and are embedded within organisational culture and practice.*
- *Immersive: Intensive, holistic experiences that challenge beliefs and values and radically alter practice.*
- *Design-Led: Disciplined, problem-solving processes that require deep understanding of and engagement with users.*
- *Market-Led: New providers stimulate demand and grow the market for new products and services.*
- *Open: Ideas and resources are freely exchanged in unregulated online environments. (AITSL, 2014, p. 27)*

These global trends are relevant to the provision of effective professional learning to the diverse settings for schools in WA, particularly those in RRR locations. A designed approach to a hybrid model of professional learning that enables collective learning, mastery of teaching to build confidence and opportunities for teachers to reflect on their achievements will be in keeping with these trends.

Summary of key points

Teachers play an important role in shaping the lives of young Australians. In an increasingly digital modern society and economy, teachers will need to continually develop essential skills and knowledge, including threats to cyber security. A wide range of resources to support teaching new curriculum are available for teachers but rely on individuals and teams to access and integrate them into classroom learning.

Effective professional learning for teachers will lead to improved student learning outcomes and provide a consistent approach to state-wide responses to cyber security curriculum change. Development of a hybrid model for the delivery of professional learning on cyber security will enable opportunities for teachers to collaborate and gain mastery of skills across a diverse range of schools, sectors, and geographic locations, including rural and remote locations.

Considerations

It is suggested …

1. That education systems further consult with agencies such as ACSC and industry providers to ensure all students in WA have access to pre-requisite skills and knowledge about cyber security before the end of Year 8.
2. That the language of cyber security is included in curriculum materials, support resources, and professional learning materials in any future adaption and adoption of the Australian curriculum version 9.0 within the Western Australian Curriculum.
3. That teacher support resources for all learning areas, subjects and year-levels Pre-primary to Year 10 are updated to include cyber security skills and concepts.
4. That in-service and pre-service teachers are funded and provided with professional learning to develop the skills and knowledge to teach with confidence and competence about cyber security.
5. That the incorporation of additional Year 6 and Year 10 assessments to measure cyber security skills and knowledge may lead to these skills and knowledge being taught.
6. That Western Australian universities (or at least one) offer a major in digital technologies in their Bachelor of Education (Secondary) degrees.

Conclusion

Cyberthreats are a concern for all Australians. For young people, the ability to become confident and engaged citizens will include the ability to work and connect socially in a digital world. The purpose of this report based on curriculum mapping for aspects of cyber security in the WA school curriculum is to identify the extent to which cyber security knowledge and skills are currently included and the opportunities for increasing the engagement of young people in learning how to navigate the digital environment safely in the future.

Is it enough to teach school children to be aware of cyber security threats and to be able to protect themselves and their digital footprint through fundamental skills and knowledge such as multifaceted passwords and considering how they share information? The Australian Curriculum 9.0 will enable this.

Do we want Australian citizens to develop a deeper level of skills and understanding of the ways in which threats to cyber security might specifically cause harm in the ways that are outlined by ACSC? The Australian Curriculum 9.0 does not introduce the level required. However, in a classroom context, individual teachers might use particular cyber security threats as an opportunity to teach how best to respond to and mitigate risks, but this would be highly dependent on the personal confidence and competence in cyber security of the individual teacher.

In pursuance of teachers having the confidence and competence in knowledge and skill surrounding teaching cyber security, multiple models of professional learning ought to be provided to both in-service and pre-service teachers. It is not enough to *just* change the curriculum; teacher capacity needs to increase for the sake of achieving better outcomes for young people in terms of developing their knowledge and skills surrounding cyber security and being able to detect new and developing cyberthreats and risks throughout the lifespan.

Abbreviations

ACCE	Australian Council of Computers in Education
ACS	Australian Computer Society
ACARA	Australian Curriculum and Assessment Authority
ACSC	Australian Cyber Security Centre
AITSL	Australian Institute of Teaching and School Leadership
ATAR	Australian Tertiary Admission Rank
ECAWA	Educational Computing Association of Western Australia
ECU	Edith Cowan University
F – 10	Foundation to Year 10
ICT	Information and Communications Technology
K – 10	Kindergarten to Year 10
NAPLAN	National Assessment Program - Literacy and Numeracy
OECD	Organisation for Economic Cooperation and Development
PL	Professional Learning
RRR	Regional, Rural and Remote
SCSA	School Curriculum and Standards Authority, Western Australia
SRI	Security Research Institute
WA	Western Australia/ Western Australian
WACE	Western Australian Certificate of Education

Tables

References

Australian Computer Society (ACS) (2021), *ICT Educators*, accessed 24/08/2022 at ICT Educators (acs.org.au)

Australian Curriculum, Assessment and Reporting Authority (ACARA) (2016) accessed 12/05/2022 www.australiancurriculum.edu.au

Australian Curriculum, Assessment and Reporting Authority (ACARA) (2021a). Final Report – General Capabilities. Accessed online 8/8/2022 at Final Report - General Capabilities (acara.edu.au)

Australian Curriculum, Assessment and Reporting Authority (ACARA) (2021b). *Final Report – Technologies*, Accessed online 8/8/2022 at Final Report - Technologies (acara.edu.au)

Australian Curriculum version 9.0 (2022). Accessed online 12/9/2022 at https://v9.australiancurriculum.edu.au/

Department of Education, Skills, and Employment (DESE) (2018). Independent Review into regional, rural and remote education, final report. accessed 14/06/2022 at www.dese.gov.au/quality-schools-package/resources/independent-review-regional-rural-and-remote-education-final-report

Australian Institute for Teaching and School Leadership (AITSL) (2014). *Designing Professional Learning*, accessed 16/06/2022 at designing_professional_learning_report.pdf (aitsl.edu.au)

Australian Institute for Teaching and School Leadership (AITSL) (2017). *Australian Professional Standards for Teachers*, accessed 17/06/2022 at Teacher Standards (aitsl.edu.au)

Commonwealth of Australia (2022). *Australian Cyber Security Centre (ACSC)* accessed on 07/08/2022 at ACSC Homepage | Cyber.gov.au

Commonwealth of Australia (2020). *Australia's Cyber Security Strategy*, Department of Home Affairs, accessed online 07/08/2022 at Australia's Cyber Security Strategy 2020 (homeaffairs.gov.au)

Commonwealth of Australia (2015). *eSafety Commissioner*, accessed 24/08/2022 at Homepage | eSafety Commissioner

Council of Australian Governments (COAG). Education Council (2019). *Alice Springs (Mparntwe) Education Declaration*. accessed online 14/06/2022 at The Alice Springs (Mparntwe) Education Declaration - Department of Education, Skills and Employment, Australian Government (dese.gov.au)

Education Services Australia, *Scootle: digital resources for Australian teachers*, accessed 23/08/2022 at Home - Scootle

Government of Western Australia Department of Education (WA DET) (2019). *Students Online in Public Schools Procedures, Version: 3.2*, accessed 14/06/2022 at www.education.wa.edu.au/o/article/pdf/web/policies/-/students-online-in-public-schools-procedures

Organization for Economic Cooperation and Development (2021). OECD Digital Education Outlook 2021: *Pushing the frontiers with Artificial Intelligence, Blockchain and Robots*, accessed 18/05/2022 at OECD Digital Education Outlook 2021 : Pushing the Frontiers with Artificial Intelligence, Blockchain and Robots | OECD Digital Education Outlook | OECD iLibrary (oecd-ilibrary.org)

Teacher Registration Board of Western Australia, *Professional Standards for Teachers in Western Australia*, accessed 14/06/2022 at PublishedDoc.aspx (trb.wa.gov.au)

Western Australia Schools Curriculum and Standards Authority (SCSA) (2022). Kindergarten to Year 10 Curriculum: Technologies accessed 18/05/2022 at k10outline - Technologies (scsa.wa.edu.au)

Western Australia Schools Curriculum and Standards Authority (SCSA) (2016). Policy Standards for Pre-primary to Year 10: Teaching, Assessing and Reporting accessed on 15/07/2022 at SECTION 1: (scsa.wa.edu.au)

Edith Cowan University
School of Education
Mt Lawley Campus
2 Bradford St
Mt Lawley WA 6050

www.ecu.edu.au/schools/education