eSafetyresearch

Best Practice Framework for Online Safety Education (Stage 1)

July 2023

Australian Government | eSafetyCommissioner

This research was commissioned by the eSafety Commissioner (eSafety), with the report prepared by Queensland University of Technology. The research for the report was conducted in 2019.

Please note that the views and opinions expressed in this publication are those of the participants and not necessarily those of eSafety.

Queensland University of Technology

Best Practice Framework for Online Safety Education

Report for the eSafety Commissioner

Kerryann Walsh, Elizabeth Wallace,

Natasha Ayling and Annette Sondergeld

Faculty of Education

Queensland University of Technology

June 2020

Acknowledgements

This research was commissioned by eSafety and funded through a partnership between eSafety and the Australian Government Department of Education.

The report presents the findings of research to establish a best practice framework for online safety education in Australian schools. The views and findings expressed in this report are those of the author(s) and do not necessarily reflect those of eSafety. Any recommendations and errors are the responsibility of the author(s).

The report was prepared and written by Professor Kerryann Walsh (PhD), Faculty of Education, Queensland University of Technology. Research was conducted from 20 May 2019 – 15 July 2019. Acknowledged as co-authors in this report are research assistants: Elizabeth Wallace (BEd), Natasha Ayling (MPhil, BEd), and Annette Sondergeld (MAppSc, LLB).

The QUT research team gratefully acknowledge the collaboration and practical assistance provided by staff from the eSafety Commissioner: Tarina Mather, Ella Serry, Sharon Trotter, Kellie Britnell, Joseph DiGregorio, Colleen Doyle and Vanessa Mai.

ISBN number: 978-1-925553-20-8

Author contact details

Professor Kerryann Walsh

Faculty of Education

Queensland University of Technology

Victoria Park Road

Kelvin Grove QLD 4059

Phone +61 7 3138 3174

Email k.walsh@qut.edu.au

QUT staff website https://staff.qut.edu.au/staff/k.walsh

Childhood Adversity Research Program website

https://research.qut.edu.au/child-adversity/

Contents

Executive summary

Introduction

Education is an important part of prevention and a powerful tool for behaviour change. eSafety uses a range of strategies to raise awareness and promote online safety for young people, providing resources and training programs for educators, young people and their parents. These education strategies are underpinned by a strong research and evidence base, enhanced by insights from the cyberbullying and image-based abuse complaints scheme, which provide unique insights into the nature of online harms. However, over time, eSafety has identified a gap in clear evidence and overarching information about what a comprehensive approach to online safety education should look like.

This research was commissioned by eSafety in response to the identified online safety education gaps and as part of its strategic leadership role in this area. This in line with recommendations in the Report of the Statutory Review of the Enhancing Online Safety Act 2015 and the Review of Schedules 5 and 7 to the Broadcasting Services Act 1992 (Online Content Scheme) and the Royal Commission into Institutional Responses to Child Sexual Abuse.

Under Section 15 of the Enhancing Online Safety Act 2015 eSafety:

- supports, encourages, conducts and evaluates research about online safety for Australians
- collects, analyses, interprets and disseminates information about online safety
- publishes reports and papers relating to online safety for Australians.

The research program is underpinned by four key themes including:
1. tracking trends
2. supporting the development of eSafety resources and programs
3. inter-agency and international co-operation
4. program and resource evaluation.

Aim

This research was designed to support the development of a best practice framework for online safety education in Australian schools, from Foundation to Year 12.

This framework aims to provide a consistent, overarching national narrative for education including state and territory education departments, Catholic and Independent school systems, and external online safety education providers. It provides a well-defined set of broad components with a subset of meaningful indicators that can be readily applied to online safety education practice. The framework is comprehensive enough to set directions for future online safety education initiatives, and to distinguish specific program quality.

Stage 1 (current) was commissioned by eSafety to investigate what constitutes best practice in online safety education for school-aged children. This involved undertaking a rapid review of the literature to assess current understandings of best practice in online

safety education. To identify framework components we extracted data, analysed and synthesised relevant information.

Stage 2 (future) may include consulting on and refining the best practice framework as well as exploring ways to customise the framework for specific audiences. Stakeholder consultation would ensure individuals and groups, with relevant expertise and specialist knowledge, provide input and would allow the framework to be tested in the real-world. This would help to determine the feasibility and acceptability of a framework. Consultation can also generate greater engagement, provide insights into different circumstances and needs and typically leads to greater uptake and use.

Method

The project methodology involved a rapid review of eight sources of evidence:

1. Research conducted by eSafety.
2. Research conducted by international bodies similar to eSafety.
3. Systematic reviews assessing evidence of effectiveness and/or implementation of online safety education initiatives for children and young people.
4. Narrative reviews or practice pieces by renowned researchers in the fields of online safety education, cyberbullying, nudes and sexting, exposure to pornography, time online, gaming, unwanted contact, online grooming, sexual exploitation and solicitation.
5. Literature reviews looking at the characteristics of effective school-based prevention initiatives.
6. Existing frameworks, models, guidelines, standards, tools from Australian, government organisations and non-government organisations.
7. Existing frameworks, models, guidelines, standards, tools from international, government organisations and non-government organisations.
8. Australian inquiries, taskforces, expert groups and working parties with findings relevant to children and online safety risks or harms.

Key findings

We used the sources to find existing frameworks, identify key components, and assess their strengths and weaknesses. From this we identified a number of existing frameworks. The most relevant were:

- Education for a Connected World Framework (UK Council for Child Internet Safety, 2018)
- DQ Common Framework for Digital Literacy, Skills and Readiness (DQ Institute, 2019a)
- Digital Citizenship Education Handbook (Council of Europe, 2019)
- Three Digital Citizenship framework documents (Common Sense Education, 2016, 2017, 2018), including one entitled Digital Citizenship and Social and Emotional Learning (Common Sense Education, 2017)
- Nine Elements (Ribble, 2017)
- BEaPRO (US iKeepSafe Coalition, 2015) which focuses mainly on privacy.

We found no publicly available research reports about the development of comprehensive online safety education frameworks, models, guidelines, standards or tools by agencies in Australia.

Frameworks comparison

All the frameworks reviewed have multiple components, some of which are similar. However, many of the frameworks do not address specific online risks and none appears comprehensive enough, nor contains sufficient scope and detail, to be adopted as Australia's online safety education framework. However, some aspects are relevant, and provide detail needed to inform the development of a best practice framework.

Our review revealed that a new online safety education framework should cover the full range of potential issues, risks and harms that children may encounter, as well as consider the issues of greatest parental concern. This is important because there appears to be contextual, cultural and geographic differences in the ways in which children and parents perceive opportunities and challenges of digital technologies, as found in previous research by eSafety.

Framework evaluation

Although the identified frameworks have been in place for some time our review showed there has been no rigorous or reliable evaluation of their success.

Future evaluation on the effectiveness of online safety initiatives, both in Australia and internationally is needed though as high quality prevention initiatives must be underpinned by recent, rigorous and reliable evaluations.

Framework components

Of note was our analysis of findings and recommendations from recent Australian inquiries. Several identified themes remain unaddressed. There were clear calls for greater awareness and management of online risks, and repeated calls for State and Territory educational authorities to pursue coordinated responses. Inquires also highlighted the need for greater efforts to improve the quality of educational programs for children.

Our research pointed toward the need for a multicomponent online safety education framework. This framework would be based on concepts found in digital citizenship and social and emotional learning programs, augmented with content addressing common risk and protective factors. This would be underpinned by evidence, guided by principles of effective prevention and delivered in supportive school systems with strong partnerships with other agencies. The framework's component parts can be used flexibly by eSafety for multiple purposes either together, or separately.

From the material we examined, the following components would be recommended as part of a comprehensive best practice online safety education framework for school-aged children:

- Component 1: big ideas (or principles) — these are unifying principles that connect, organise and direct the framework. For example, that an online safety framework should be based on children's rights and framed positively.
- Component 2: the landscape — there are several features of schools' environments that need to be in place to increase the likelihood of online safety education having desired effects. These include system-wide approaches and a network of policies and procedures.

- Component 3: ‘the what’ and ‘the how’ — the what refers to the contents of online safety education, including digital citizenship, social and emotional learning, specific risks, and help seeking and the how refers to the methods by which these should be taught.

Limitations

There were a number of limitations identified in our review:

- The rapid review methodology used in Stage 1 is retrospective — the material gathered and examined is from the past and is, to some degree, ‘backward-looking’.
- All the frameworks had strengths and weaknesses.
- There is a strong and growing evidence base highlighting the key elements of effective school-based prevention in general, but there is little literature about specific, comprehensive school-based online safety education.

To strengthen the basis for the framework in Stage 2 it is important to take a prospective approach and to become ‘forward-looking’. This can be done by collecting further experiential and contextual evidence and consulting with a range of stakeholders.

Background

Aim

The aim of this research was to develop a best practice framework for online safety education for Australian schools (F-12).

Method

For this research we used a rapid review of research evidence, which uses the same methods as a traditional systematic review but with concessions (such as restricting searches to only the most relevant databases, excluding unpublished theses and not contacting study authors to supply missing data) to enable completion in a shorter time (Gannan, Ciliska & Thomas, 2010). Rapid evidence review is used to investigate what is already known about a topic by employing explicit, transparent and replicable methods for locating, extracting and synthesising evidence from existing sources. The aim is to summarise the existing knowledge base to provide a balanced, yet high level, perspective that can help inform policy and practice decisions, and strategic directions.

We used a well-established model which offers a way of conceptualising 'evidence' in three overlapping spheres: (i) the best available research evidence (ii) experiential evidence and (iii) contextual evidence, as shown in Figure 1.

Figure 1: Puddy & Wilkins' (2011, p.4) model for thinking about evidence.

Best available research evidence is based on empirical studies in which data has been collected, analysed and documented. It also includes research reviews.

Experiential evidence is based on an expert's long-term engagement in a field, offering insights into what has worked, what seems to work, and other knowledge and expertise that can sometimes be understood, without being stated.

Contextual evidence is based on information about whether a strategy or practice is perceived as useful, relevant, feasible to implement and is acceptable to specific groups. In this research, contextual evidence was identified through consultation with eSafety staff. It could be further honed in stage two of the project through consultation with stakeholders.

For this project the best available research evidence and experiential evidence were identified in rapid reviews of eight evidence sources:

1. Research conducted by eSafety.
2. Research conducted by international bodies similar to eSafety.
3. Systematic reviews assessing evidence of effectiveness and/or implementation of online safety education initiatives for children and young people.
4. Narrative reviews or practice pieces by renowned researchers in the fields of online safety education, cyberbullying, nudes and sexting, exposure to pornography, time online, gaming, unwanted contact, online grooming, sexual exploitation and solicitation.
5. Literature reviews looking at the characteristics of effective school-based prevention initiatives.
6. Existing frameworks, models, guidelines, standards, tools (Australian, government organisations and non-government organisations).
7. Existing frameworks, models, guidelines, standards, tools (international, government organisations and non-government organisations).
8. Australian inquiries/taskforces/expert groups/working parties with findings relevant to children and online safety risks and harm.

Search strategy

We conducted online searches of: (i) internet websites and (ii) academic databases.

Research assistants searched the internet using Google with results documented in an Excel spreadsheet known as a searchtracker. They undertook multiple searches using combinations of predefined search terms (Appendix 1). Searches were both general and targeted, with the latter yielding more relevant results. For each website we systematically recorded the website URL, specific search terms, the total number of records found and their relevance.

Academic database searches were conducted by an information specialist using a standardised search strategy that had been piloted and refined (Appendix 2). We searched nine databases covering the period 2010-2019. Search results were also recorded in the searchtracker.

The project searchtracker record files were provided to eSafety as supplementary files.

Screening and selecting documents

We screened records from searches on: (i) the internet and (ii) databases.

Internet searches were conducted in June 2019. The first five pages of results for each search were screened and records that were identified as potentially relevant were entered into a source file. The full text of these records was then further screened using several criteria which were consistently applied (Appendix 3).

Database searches were also conducted in June 2019. Search results were imported to EndNote reference manager software, then transferred into Covidence — an online software platform used to streamline screening processes. Duplicate records were removed. Titles and abstracts were screened by two reviewers working independently who resolved any conflicts through discussion. The full text of potentially relevant records was also screened.

Table 1 shows search and screening results for each of the eight evidence sources.

Table 1: Search results

	Number of records screened	**Number of records included in thematic analysis**
1. Primary research eSafety	17	9
2. Primary research international*	31	22
3. Academic databases	1229	79
4. Australian government organisations	194	32
5. Australian non-government organisations**	17	4
6. International organisations	168	31
7. Australian inquiries	15	11
8. Favourites (selected by eSafety staff)	21	11
Totals	1692	199

*Primary research was sourced from worldwide agencies with similar functions to eSafety.
**Searches of Australian non-government organisations were limited eSafety's list of Certified Training Providers (CTPs).

Extracting relevant information from documents

The next step was to extract relevant information from 199 documents into a matrix for each evidence source. We looked for the key findings, recommendations, principles, elements, features, fundamentals, foundations, specifications and basics that are applicable to teaching online safety education in schools.

In this material we asked:

- What should be taught in online safety education for primary and secondary school students (topics/contents/subject matter/information/knowledge/skills/dispositions)?
- How should it be taught (pedagogies/teaching methods/strategies/approaches)?
- By whom (who delivers key messages, their qualifications, training, expertise, experience)?

- In what ways? (delivery modes used such as face-to-face or online, single class/year or whole school)?
- When, how often, and how much (session/lesson timing, sequence, number, duration, intensity)?
- What information should be provided to participants (students, parents, teachers, schools)?
- What training should be provided to deliver it (professional development content and methods)?
- Where is it taught (location, infrastructure, resources required)?

The project matrices data files were provided to eSafety as supplementary files.

Data analysis and synthesis

Our approach to data analysis and synthesis was two-fold. First, we looked across the document dataset to identify promising existing frameworks and for any other papers with relevance to Australian education contexts. Several promising sources were identified.

Second, we looked inside frameworks and other documents to understand their component parts with a view to combining information from various sources. We used qualitative thematic analysis (Braun & Clarke, 2006) to organise the extracted information. We coded and categorised information and looked for patterns, regularities, and irregularities. We did not begin with preconceived ideas about how the data should be organised or pre-defined themes. Themes emerged very clearly from the data set.

Results: existing frameworks

This section draws on the eight sources of evidence and looks across the documents to examine existing frameworks used in Australia and worldwide. Where possible, it identifies the key elements of these initiatives and their strengths and weaknesses.

Evidence source 1: primary research by eSafety

We searched the eSafety website for research to inform the development of a best practice framework for online safety education. We looked at: (i) research on children's digital practices, issues and concerns (ii) research on parents' digital practices, issues and concerns and (iii) research on children's exposure, risk and harm.

Nine documents were included and while the study reports were highly relevant, no existing frameworks were identified.

Notably, much of the identified eSafety research involved data collection with children — an approach that is widely supported in the literature as crucial for intervention design. eSafety research assists in understanding online safety issues as experienced by Australian children and their parents/carers. This is important because an online safety education framework should cover the full range of potential issues, risks and harms that children may encounter, and the issues of greatest parental concern.

Evidence source 2: primary research by international agencies

As part of our research we searched the websites of international agencies with similar functions to eSafety, specifically looking for research reports that would help inform the development of a best practice framework for online safety education.

In total, 22 documents were examined. No existing frameworks were identified.

The most relevant reports were:

- United Kingdom Council for Child Internet Safety (UKCCIS) Evidence Group's Children's Online Activities, Risks and Safety: A Literature Review (Livingstone et al., 2017)
- New Zealand (NZ) Ministry for Women and Netsafe's Insights into Digital Harm: The Online Lives of New Zealand Girls and Boys (Ministry for Women & Netsafe, 2017)
- Common Sense Census: Inside the 21st Century Classroom (Vega & Robb, 2019) which reports on the state of educational technology in U.S. classrooms, and
- PREVNet's Mobilising Canada to Promote Healthy Relationships and Prevent Bullying among Children and Youth (Pepler, Craig, Cummings, Petrunka, & Garwood, 2017).

Many of these reports were affiliated with studies from the Global Kids Online initiative which aims to collect comparative and complementary data on children's online rights,

opportunities and risks from countries around the world*. Findings of these studies generally align with eSafety's research, although there are important contextual, cultural and geographical differences in how children and parents perceive opportunities and challenges for digital technologies. This reinforces the ongoing need for Australian-specific research.

We did not find any publicly available research reports on agencies' development of online safety education frameworks, models, guidelines, standards or tools. Nor did we find any evaluations of frameworks of this nature.

*globalkidsonline.net

Evidence source 3: primary research identified in academic databases

For our third evidence source we searched academic databases for systematic reviews, reviews of relevant literature, research syntheses or policy/practice pieces by renowned researchers which assessed the effectiveness and/or implementation of online safety education initiatives for children and young people. This included research reviews of interventions for online safety education broadly and also for specific issues such as cyberbullying, nudes and sexting, exposure to pornography, time online, gaming, unwanted contact, online grooming, exploitation or solicitation (see Appendix 2). We also searched for reviews of literature on the characteristics of effective school-based prevention initiatives.

In total, 79 reviews were examined. All were relevant, to a greater or lesser extent. No existing frameworks were identified.

Through this process we identified a small number of research reviews specifically addressing children's online safety. These reviews included information on the potential components of a best practice framework for online safety education. All were conducted by a research team at the Crimes against Children Research Centre (CCRC) at the University of New Hampshire and were commissioned by the US National Institute of Justice (Finkelhor, 2014; Jones, 2010; Jones, Mitchell, & Walsh, 2013, 2014a, 2014b; Jones & Mitchell, 2016).

We identified systematic reviews of interventions for specific online safety issues, as well as other review types. By far the greatest number of systematic reviews looked at the effectiveness of school-based cyberbullying prevention interventions — with very clear findings across multiple reviews. From these reviews we were able to determine the teaching methods and approaches that appear to characterise effective interventions for cyberbullying prevention. The second largest group of reviews related, broadly, to sexual violence prevention interventions (including child sexual abuse prevention, adolescent intimate partner violence prevention and prevention of technology-assisted harmful sexual behaviour). These reviews had less explicit detail on the characteristics of effective prevention interventions. There were few systematic reviews providing information about what, and how, to teach about exposure to inappropriate content online, dealing with nastiness online, responding to negative incidents online, dealing with digital distraction, being left out/excluded and peer aggression online (as distinct from cyberbullying).

We identified one review detailing characteristics of effective school-based prevention initiatives, broadly (e.g PSHE Association, 2016), conducted on behalf of the UK Child Exploitation and Online Protection command (CEOP) and ThinkUKnow. After hand searching reference lists, four further documents were identified with detail sufficient to inform development of a set of overarching principles for effective school-based prevention initiatives. The additional four documents are: What Works in Prevention: Principles of Effective Prevention Programs (Nation et al., 2003), a Cochrane review on the WHO Health Promoting School Framework (Langford et al., 2014), Implementation in Education: Findings from a Scoping Review (Centre for Evidence and Implementation, 2017), and INSPIRE: Seven Strategies for Ending Violence against Children (World Health Organisation, 2016).

Evidence source 4: Australian government organisations

Another source of material for our research was the existing frameworks on websites of Australian government organisations.

In all, 32 documents were examined. Some wider frameworks relating to child wellbeing, welfare and safety were identified, but none were specifically focused on online safety education.

The most relevant were:

- Australian Student Wellbeing Framework (Education Services Australia, 2018)
- National Principles for Child Safe Organisations (Australian Human Rights Commission, 2018)
- PROTECT: A Guide to Support Victorian Schools to Meet Child Safe Standard 7 (Victorian Government Department of Education and Training, 2017)
- The Good Practice Guide to Child Aware Approaches: Keeping Children Safe and Well (Australian Institute of Family Studies, 2014)
- The STEPS Decision-Making Framework (The State of Queensland, Department of Education and Training, 2016)
- Adjust Our Settings: A community Approach to Address Cyberbullying among Children and Young People in Queensland (Queensland Anti-Cyberbullying Taskforce, 2018)
- The YeS Project (eSafety Commissioner, 2018).

These documents, when viewed together, cover a broad range of online safety topics but do not align closely with one another. The extent to which they have been implemented varies and, in many cases, is unknown. The documents could be described as a patchwork. They form part of the policy and practice landscape against which a best practice framework for online safety education is set. Individually, none contain sufficient scope and detail to be adopted as an online safety education framework, however, aspects are relevant. These existing frameworks can provide some of the detail needed to inform the development of a best practice framework.

Evidence source 5: Australian non-government organisations

We searched for existing frameworks on Australian non-government organisation's websites, specifically those listed as eSafety Certified Training Providers (CTPs)[1].

Four documents were examined. These related to specific programs and products. Components identified were program-specific rather than school-sector specific.

The three most relevant documents were: the eSmart Schools Evaluation Report (Pope, Colin, Third, Ogus & Campbell, 2015, prepared for The Alannah and Madeline Foundation), the Digital Thumbprint Evaluation Report (Optus, 2018) and 3 Piers to Prevention: Research Report (Johnstone & Ronken, 2017, prepared by Bravehearts Foundation Limited).

From the publicly available material, it appears that none of the online safety education programs offered by Australian Certified Training Providers have been evaluated using rigorous experimental methods — where data are collected from children exposed to a program and results compared with data collected from a control group of children who did not receive the program.

The eSmart Schools Program has signed up almost a quarter of Australian schools (Pope, Colin, Third, Ogus, & Campbell, 2015). The program has been evaluated using an environmental scan, survey and case studies. The Digital Thumbprint Program has reached 170,000 students (Optus, 2018). It has been evaluated using mixed methods including surveys, focus groups and interviews. Both programs include elements of digital citizenship and respectful relationships education and are somewhat aligned with each other as shown in Table 2. Bravehearts' 3 Piers to Prevention framework functions at a higher conceptual level, indicating broad elements required society-wide, specifically for child sexual assault prevention.

Table 2: Australian program elements

eSmart Schools The Alannah & Madeline Foundation	OPTUS Digital Thumbprint OPTUS	3 Piers to Prevention Bravehearts
1. Effective school organisation 2. School plans, policies and procedures 3. Respectful and caring school community 4. Effective teacher practices 5. eSmart curriculum 6. Partnerships with parents and the local community	1. Cybersecurity 2. Cyberbullying and respectful relationships online 3. Digital identity 4. Digital discernment 5. Digital balance	1. Educate 2. Empower 3. Protect

Evidence source 6: international organisations (government and non-government)

[1] Soon to be known as 'Trusted eSafety Providers' esafety.gov.au/education-resources/certified-training-providers

Another avenue for our research was looking for existing frameworks on the international organisations' websites, both government and non-government.

In all, we examined 31 documents, identifying several frameworks. Most focus on digital citizenship in general, rather than specifically looking at online safety education.

The most important of these frameworks were evidence-based, high level, collaboratively developed, far-reaching. These are:

- the Education for a Connected World Framework (UK Council for Child Internet Safety, 2018)
- the DQ Common Framework for Digital Literacy, Skills and Readiness (DQ Institute, 2019a)
- the Digital Citizenship Education Handbook (Council of Europe, 2019)
- three Digital Citizenship framework documents (Common Sense Education, 2016, 2017, 2018), including one entitled Digital Citizenship and Social and Emotional Learning (Common Sense Education, 2017)
- Nine Elements (Ribble, 2017)
- BEaPRO (US iKeepSafe Coalition, 2015) which focuses mainly on privacy.

The key elements of these frameworks are shown in Table 3.

These multi-component frameworks all focus on children in school settings. Many have comparable components which can be matched to overarching digital citizenship concepts such as access and participation, security and privacy, media and digital literacy, and general health and wellbeing. One framework combines components of digital citizenship with social emotional learning (specifically five elements: self-awareness, self-management, responsible decision-making, relationship skills, and social awareness). The frameworks are broad in scope and nature. They touch lightly on risks (such as privacy), but do not focus exclusively or deeply on content or methods for addressing specific risks, vulnerabilities, or harms to children online.

Two UNESCO reports are also relevant. While not framework documents, they identify elements that are important in digital technology education. First, is Fostering Digital Citizenship through Safe and Responsible Use of ICT (UNESCO Bangkok, 2015) which identified four key themes in ICT-related education from twelve countries across Asia and the Pacific. These were: benefits of ICT use/online participation, responsible and ethical behaviour, safety/protection against risks and values reinforcement (highlighting respect and empathy). Second is the recent report, Digital Kids Asia-Pacific: Insights into Children's Digital Citizenship (UNESCO Bangkok, 2019) which identified five domain-specific sets of digital competencies: digital literacy, digital safety and resilience, digital participation and agency, digital emotional intelligence, digital creativity and innovation.

Also relevant to our research, at a higher conceptual level, is a suite of diagnostic and self-audit tools developed by a coalition led by UK not-for-profit organisation South West Grid for Learning Trust (SWGfL, 2018a, 2018b, 2018c, 2018d). These tools, known as 360 Safe, appear to have been widely used. They are organised around four elements: education, infrastructure, policy and leadership, and, standards and inspection. Each element includes a number of strands which, in turn, include a number of aspects.

In addition, the European Commission has developed the Better Internet for Kids Policy Map (O'Neill & Dinh, 2018) which is framed around five pillars:

- Pillar 1: Stimulating Quality Content Online for Young People
- Pillar 2: Digital/Media Literacy in Education
- Pillar 3: Stepping Up Awareness and Empowerment
- Pillar 4: Tools and Regulation for an Online Safe Environment
- Pillar 5: Legislation and Law Enforcement against Child Sexual Abuse and Exploitation.

Table 3: Key elements of existing frameworks (international)

Education for a Connected World Framework UK CCIS	DQ Framework V.1 DQ Institute	DQ Framework V.2 DQ Institute	Digital Citizenship Education Handbook Council of Europe	Cross-Curricular Framework Common Sense Education	Digital Citizenship Curriculum Common Sense Education	Digital Citizenship and Social and Emotional Learning Common Sense Education	Nine elements Mike Ribble	BEaPRO US iKeepSafe Coalition
Health, wellbeing and lifestyle	Screen time management	Digital use	Health and wellbeing		Media balance and wellbeing	Distraction, multitasking and time management	Digital health and welfare	Balance
Privacy and security	Privacy management Cyber security management	Digital rights (privacy management) Digital security	Rights and responsibilities Privacy and security	Privacy and security	Privacy and security	Privacy, surveillance and self-disclosure	Digital rights and responsibility Digital security and privacy	Privacy Online security
Online reputation	Digital footprints	Digital communication	Active participation	Digital footprint and reputation	Digital footprint and identity	Digital footprints and sharing	Digital communication and collaboration	Reputation Ethics
Self-image and identity	Digital citizen identity	Digital identity	e-Presence and communications	Self-image and identity		Social media and body image		
Copyright and ownership		Digital rights (intellectual property rights management)		Creative credit and copyright				
Online relationships	Digital empathy	Digital emotional intelligence	Ethics and empathy	Relationships and communication	Relationships and communication	Digital drama	Digital etiquette	Relationships
Online bullying	Cyberbullying management			Cyberbullying and digital drama	Cyberbullying, digital drama and hate speech	Cyberbullying		
		Digital literacy	Media and information literacy		News and media literacy		Digital fluency	

			Consumer awareness					
Managing online information	Critical thinking			Information literacy				
		Digital safety		Internet safety				
			Access and inclusion				Digital access	
			Learning and creativity					
						Sexting and nude photographs Sexual imagery and the internet		
						Video games and violent content		
							Digital law	
							Digital commerce	

Evidence source 7: Australian inquiries

Final reports from Australian government inquires with findings or recommendations relevant to online safety education for school-aged children were another important source of evidence for this research. In total, eleven reports were examined. Of particular note was the Final Report from the Royal Commission into Institutional Responses to Child Sexual Abuse — Volume 6: Making Institutions Child Safe (Commonwealth of Australia, 2017) which recommends that a national strategy to prevent child sexual abuse should encompass complementary initiatives including online safety education for children, delivered via schools (see Recommendations 6.2d, 6.19 and 6.22).

All inquiries found relevant information, with several clear themes. There were clear calls for greater awareness, and management, of online risks, and repeated calls for state and territory educational authorities to pursue coordinated responses. Inquires also highlighted the need for greater efforts to improve the quality of educational programs for children.

Key themes and recommendations from the inquiries included the characteristics of online safety education curriculum and delivery strategies, which are detailed below.

Characteristics of online safety education curriculum:

- nationally-consistent, devised and implemented with cooperation of all Australian jurisdictions
- focuses on the positive role and benefits of technologies
- comprehensive and adopts a whole-of-community and whole-school approach
- age-appropriate, inclusive, culturally-sensitive and relevant
- child-focused and strengths-based — promotes student participation in decision making and curriculum delivery
- integrated, begins early and corresponds with ages that children enter online environments
- promotes positive and prosocial behaviours and respectful relationships
- is sustainable, acceptable, adaptable and reflects changes in technologies.

Recommended strategies for curriculum delivery:

- a range of child-focused early intervention measures to address cyberbullying
- redefining cyberbullying as a social and public health issue
- student participation in developing anti-cyberbullying programs, initiatives, policies and procedures
- student, parent/carer and community participation in curriculum design and delivery
- partnerships with external specialist services for curriculum delivery and with support services for early intervention and support for targets/victims
- training (beginning in preservice), resources and support for teachers which:
    - reframes thinking around ‘victim blaming’
    - focuses on the social consequences of behaviour as well as legal consequences
    - promotes and encourages children’s help-seeking
    - embeds teaching digital and media literacies throughout the whole curriculum
    - promotes social and emotional competencies in children.

Table 4: List of relevant Australian inquiries (since 2010)

Australian inquiries
Commonwealth of Australia. (2011). High-Wire Act: Cyber-Safety and the Young.
House of Representatives Joint Select Committee on Cyber-Safety. (2013). Inquiry into issues surrounding cyber-safety for Indigenous Australians.
Victorian Law Reform Commission. (2013). Inquiry into Sexting. Report of the Law Reform Committee for the Inquiry into Sexting.
State of Victoria. (2016). Royal Commission into Family Violence: Volume VI Report and recommendations.
The Senate Environment and Communications References Committee. (2016). Harm being done to Australian children through access to pornography on the Internet: Report.
COAG Bullying and Cyberbullying Senior Officials Working Group. (2018). Enhancing community responses to student bullying, including cyberbullying: Report and Work Program.
Commonwealth of Australia. (2017). Royal Commission into Institutional Responses to Child Sexual Abuse. Volume 6: Making Institutions Child Safe.
Department of Communications and the Arts. (2018). Report of the Statutory Review of the Enhancing Online Safety Act 2015 and the Review of Schedules 5 and 7 to the Broadcasting Services Act 1992 (Online Content Scheme).
NSW Government. (2018). Review into the non-educational use of mobile devices in NSW schools.
Queensland Anti-Cyberbullying Taskforce. (2018). Adjust our settings: A community approach to address cyberbullying among children and young people in Queensland report.
The Senate Legal and Constitutional Affairs References Committee. (2018). Adequacy of existing offences in the Commonwealth Criminal Code and of state and territory criminal laws to capture cyberbullying report.

Evidence source 8: 'favourites' (selected by eSafety staff)

Our final source of information reviewed as part of this research came from eSafety staff who provided their favourite or most frequently referenced sources. In all, 11 documents were examined. Frameworks identified and already described (Source 6) include:

- Education for a Connected World (UKCCIS, 2018)
- 360 Safe: School Online Safety Self-Review Tool (SWGfL, 2018d)
- UK Schools Online Safety Policy and Practice Assessment (SWGfL, 2018c).

Other documents focused on children's rights in the digital age, resilience, social cohesion and bullying. These reflect current projects and focus issues, as well as providing relevant contextual detail about the work of eSafety. Themes identified in these sources reinforce those found in other sources. In particular, these sources stressed the importance of strengthening data collection about the prevalence and incidence of negative experiences online including cyberbullying, conducting evaluation of school-based programs, and using this data for program improvement.

Highlighted strategies for online safety education include:

- using simple language
- adopting a positive, achievable and supportive tone
- including specific examples of online risks
- ensuring messaging conveys that online safety is an important issue to consider at all times
- ensuring messaging addresses all target audiences
- referring to 'children and young people'
- ensuring a 'well-balanced' approach to messaging (i.e. on risks and benefits, challenges and opportunties).

Some additional considerations for social and emotional learning programs, not mentioned elsewhere, included:

- understanding how to build children's resilience
- considering the role of empathy in preventing negative behaviour
- identifying, building, strengthening and promoting supportive relationships
- focusing on both autonomy and responsibility
- teaching social and emotional skills and strategies for specifically for managing behaviour.

Results: data analysis

This section presents the findings of our analysis that looked inside each document (for all eight sources of evidence). We identified elements, features and characteristics of best practice. We synthesised this detail and based on all the information gathered, the following themes clearly emerged as component parts for a best practice framework for online safety education for school-aged children (F-12):

1. Component 1: big ideas (or principles)
2. Component 2: the landscape
3. Component 3: 'the what' and 'the how'.

Component 1: big ideas (or principles)

Principles are the key ideas that connect, organise and direct a number of smaller ideas. In the context of best practice online safety education, these are that online safety education should be:

i. founded on children's rights
ii. framed positively
iii. based on evidence
iv. embedded within the landscape of school systems and schools
v. well-designed and well-implemented
vi. underpinned by 'principles' of effective prevention
vii. aligned with and informing other priorities.

(i) Founded on children's rights

There is general consensus in the material we examined that online safety education should be based on recognition, acknowledgement and understanding of children's rights in the digital age. A specific classification of children's rights, based on the UNCRC, was frequently applied — children have rights to provision, protection and participation. Children's rights should not be misunderstood, undermined or overlooked.

The literature is replete with suggestions about how children's rights can be placed at the centre of decision making about education in the digital age. Key points include:

- The need to adopt a child-centred focus, in which the full suite of children's rights are known and observed. For example, the Simplified Version of the United Nations Convention on the Rights of the Child may provide one type of checklist for online safety education*
- That measures to ensure children's safety online — such as their rights to digital protection — should be considered alongside their access to resources and services (their rights to digital provision), and their participation in decisions that affect their lives (their rights to digital participation).

- That education needs to have an awareness of the evolving capacities of the child. Online safety education should be child-focused and differentiated according to age, ability, gender and culture, ensuring learning is inclusive and socially relevant. It can be taught at every year level with progression in content. It can begin early.
- That collaboration with children is important. Children must be enabled to participate in decisions that have an impact on their lives including the design, development and implementation of online safety education. Children need to know their concerns are taken seriously. There should be opportunities for children to teach adults about how online issues affect them.
- That children's involvement in (co) design and development should be encouraged, enabled, ethical, effective, authentic and ongoing. This acknowledges students' dignity and agency.

* unicef.org.au/Upload/UNICEF/Media/Our%20work/childfriendlycrc.pdf

(ii) Framed positively

There was general agreement, in the material we examined, that online safety education should be framed positively. Also, that a balanced approach is needed that acknowledges the positive role played by online technologies in children's lives and uses a strengths-based approach to visualise children as competent and safe users of technology. Benefits and risks, opportunities and challenges must be considered side by side (or as twin parts in the same process). There must be acknowledgement that adults can have conscious and unconscious biases and assumptions about children and their use of technology.

(iii) Based on evidence

Online safety education must be based on facts and valid research about children, online safety, and education including:

- research on children's digital practices, issues and concerns — factoring in the most common uses for digital technologies: social connectedness, access to information, education, self-expression/creativity and entertainment
- research on parents' digital practices, issues, and concerns
- accurate, representative data on children's exposure to risks and the resulting potential harms
- research on what works, what does not work, how, why and for whom.

Facts and valid research help to build a picture about the extent, scope and nature of online safety issues that children experience. This also helps to generate knowledge on the underlying risk and protective factors that increase and decrease the likelihood of a child becoming a target or perpetrator of harm. In turn, this helps to identify factors that can be modified using school-based online safety education, including barriers to, and facilitators for, safe and positive experiences online. Facts and valid research work to balance misinformation and misunderstanding.

Two foundation concepts taken from the research (shown in Table 5) can guide the scope and sequence of content for online safety education. These are:

1. Risks to children vary according to their use of, and access to, technologies (this is clearly seen where risks increase with age and time spent online). Differences in use and access result in differences in vulnerability, risk and harm. Not all risk results in harm.
2. Research, including primary research conducted by eSafety, continues to identify the range of safety issues around which online safety education content can be developed. Online safety education must be prepared to address the full range of potential issues, risks and harms that concern students and their parents. These issues are not static and continue to evolve.

Table 5: Evidence on children's vulnerability, risk and harm, issues encountered and those of concern

Levels of vulnerability, risk and harm vary according to:	**Issues encountered/of concern include:**
• Age • Gender • (Dis)ability • Socioeconomic status (SES) • Cultural and language background • Aboriginal and/or Torres Strait Islander background • Sexuality • Appearance (including weight) • Geography/location/postcode • Family background (disengaged, children in out-of-home care, not attending school, home-schooled, distance education students)	• Exposure to inappropriate content online (other than pornography, e.g. violence, animal cruelty, war) • Contact with strangers/offers to meet offline • Receiving unwanted contact or content online • Cyberbullying, aggression, hate • Exposure to sexually-explicit content online/pornography • Sexting/sharing self-generated sexual images • Grooming, child sexual abuse, sexual exploitation • Privacy online • Responding to negative incidents online • Time spent online • Radicalisation • Digital self-harm/self-harassment • The challenges of 'digital distraction' (interferes with homework, relationships, sleep) • Sharing inappropriate images or material online • Being left out/excluded • Lies or rumours • Fake news • Knowing what information to trust online

(iv) Embedded within the landscape of school systems and schools

Online safety education is more than curriculum — what to teach — and pedagogy — how to teach it. It must also include consideration of wider social conditions in which schools are located, for example a schools' governance, leadership and culture and what we refer to here as the 'landscape'. This is addressed below in Component 2.

(v) Well designed and well implemented

Online safety education should be available universally to all Australian children and young people. It should be taught, regardless of where they live or their background, and should address their individual learning needs. In the material we examined, three big ideas emerged:

1. Online safety education must be contemporary and based on the best available evidence — research, contextual and experiential.
2. Online safety education must address technical and relational aspects.
3. Online safety education should be comprehensive, consistent, coherent, coordinated and connected (the 5 Cs).

Component 3 below elaborates on the best practices we identified in online safety education for curriculum (what to teach) and pedagogies (how to teach it).

(vi) Underpinned by principles of effective prevention

In the material we identified a small group of documents detailing characteristics of effective school-based prevention initiatives, as noted above. These included Key Principles of Effective Prevention Education (PHSE Association, 2016) and What Works in Prevention: Principles of Effective Prevention Programs (Nation et al., 2003). Also, a Cochrane review on the WHO Health Promoting School Framework (Langford et al., 2014).

The WHO Health Promoting Schools approach has three aims, to:

1. promote the adoption of lifestyles conducive to good health
2. provide an environment that supports and encourages healthy lifestyles
3. enable students and staff to take action for a healthier community and healthier living conditions (Langford et al., 2014).

This systematic review found some evidence that the approach produced improvements in certain areas of student health (including bullying), but there was not enough data available of sufficient quality to determine its effectiveness for others.

The principles of effective prevention are listed in Table 6 below.

Table 6: Effective prevention education

Key principles of effective prevention education
• A whole school approach including multicomponent interventions • Varied teaching styles addressing a range of factors (including active skill-based learning, psychosocial aspects and normative education) • A developmental program which is appropriate to pupil's age and maturity (including addressing students with learning disabilities) • Learning which is inclusive of difference and is socio-culturally relevant • Well-trained teachers • Theory/research-based and factual • A positive approach, avoiding scare tactics or confrontational strategies • Clear goals and outcomes, and effective monitoring and evaluation • Support from school leadership teams and other authorities • Community, parent and student engagement • Interventions must be of adequate length and intensity

In addition to the principles, we identified a further element — 'attend to who delivers' — that seems particularly important in the context of online safety education. This was evident in statements such as:

- programs should be delivered by knowledgeable and open teachers
- programs should be highly engaging and have trustworthy facilitators
- technological aspects must be led by a young person or person perceived to be technologically competent and relatable
- guest speakers and workshops should be innovative and engaging
- facilitators must always act as positive role models in use of digital technologies, the internet and mobile devices by modelling safe practices while they are working with students
- school counsellors are not usually considered respected sources of information due to age, gender, approach and perceived levels of technological competence (Nation et al., 2003, PSHE Association, 2016, Langford et al., 2014).

We also identified a recurring theme of 'student participation'. However, the evidence base for peer-led online safety education is still in its infancy and it is not yet possible to know if this strategy is effective.

(vii) Aligned with, and informing other, priorities

In the material we examined, it was clear that there is significant alignment between a best practice framework for online safety education, and a number of Australian Government and international policies, initiatives and strategies. These include, but are not be limited to:

- The Sustainable Development Goals "closing the digital gap", for example, is considered vital to attaining sustainable development)
- Australian Student Wellbeing Framework

- National Principles for Child Safe Organisations
- Australian Curriculum: General Capabilities
- Australian Curriculum (HPE, Technology, English)
- Australian Professional Standards for Teachers
- Framework for Protecting Australia's Children 2009-2020
- National Plan to Reduce Violence against Women and their Children 2010–2022.

Component 2: the landscape

In our analyses we identified several features of the background landscape as best practice. These features, which could be described as part of schools' governance, leadership and culture, need to be in place to increase the likelihood that online safety education will have its desired effects. They include:

(i) school system-wide approaches
(ii) policies and procedures
(iii) acceptable use policy
(iv) incident response
(v) companion agencies
(vi) teachers
(vii) parents and carers.

(i) School system-wide approaches

To improve the effectiveness of online safety education, school systems — such as state and territory departments of education, Catholic diocesan education offices and other Independent school authorities (as part of a broader network of child safety agencies) — should ensure:

- regulations for schools' technology use and children's online safety
- processes and schedules for regular self-review/self-audit/self-assessment
- investing in knowledgeable, informed and engaged school leaders and leadership teams
- designating an online safety lead
- continuous, high quality education and training for all school staff
- effective policies and procedures
- sound complaints and incident reporting mechanisms — there must be a culture in which concerns, disclosures, allegations or suspicions of harm are taken seriously and addressed
- using technical safeguarding tools across infrastructure, hardware and software (for school systems and individual schools), including:
    - safety modes, filters and blockers, privacy settings and data protection — which requires specialist technical know-how
    - technical solutions to universal known online safety issues both at school, or for activities connected to school such as homework.

(ii) Policies and procedures

Children's technology use and online safety in school cannot be addressed solely by one single or stand-alone policy. Online safety needs to be incorporated into a broad range of school policies.

Key policies may include but not be limited to:

- student protection policy
- code of conduct
- student charter/student behaviour policy

- student wellbeing policy
- Bring Your Own Device (BYOD) policy
- acceptable use policy
- complaints management
- incident reporting and response
- bullying (incorporating cyberbullying).

The literature identified key features of these policies, including that policies must:

- Specifically address aspects associated with children's use of digital technology and online safety.
- Be clear and consistent as this sends a strong message to the whole school community about the school's commitment to a safe and supportive environment. They must also provide guidelines for school prevention, early response, reporting and case management (congruent with Principles for Child Safe Organisations).
- Outline responsibilities of the school system, school staff, students and parents/caregivers.

(iii) Acceptable use policy

Sound acceptable use policies have the following features. They:

- set clear rules and expectations about the use of technological devices (computers, laptops, mobile phones, tablets, wearable technology, cameras and other personal devices), applications and social media used at school/for school purposes
- are clear, understood and respected by all school stakeholders
- are easily and publicly available
- are subject to annual review
- are accompanied by monitoring and reporting.

Some material suggested that students and parents read and sign the acceptable use policy and receive education about it in school assembly with follow up in classes. However, this cannot and should not, be the only online safety education provided to students at school.

(iv) Incident response

Government guidance from the UK positions schools' online safety incident response in the context of their 'safeguarding' role, that is, as part of student protection. In Australian jurisdictions, this would require alignment with applicable national, state and territory laws, policies and procedures. Generally, schools' incident response policies and procedures should include the following:

- clear reporting pathways for different incident types
- procedures/decision trees for responding to different types of incidents
- consistency, transparency and accountability
- reparation — as indicated in reviews of responsive anti-bullying approaches, these may include: direct sanctions, restorative practices, mediation, support group method and the method of shared concern (NSW, Department of Education, Cross & Walker, 2012)
- root-cause analysis after incidents (Lundberg & Dangel, 2018, Preuss, 2003).

(v) Companion agencies

Schools are part of a wider system of support for students. In online safety incidents, intervention may be required for students at high risk or experiencing harm, both victims and perpetrators/offenders. To manage this, it's important for schools to develop and maintain awareness of, and links to, relevant, affordable, accessible, reliable and effective support services. Some relevant companion agencies mentioned in the literature include:

- eSafety
- Commissioners/Guardians for Children and Young People (federal, state, territory)
- Ombudsman
- Kids Helpline
- Police
- Child protection authorities
- Children's Legal Services (e.g. Legal Aid Centres)
- GPs (via Emerging Minds — National Workforce Centre for Child Mental Health)
- National NGOs for mental health service provision for children and young people, in particular the Beyond Blue schools initiative (Be You) and Headspace.

(vi) Teachers

Teachers and specialists who teach online safety education are role models for students. As noted in the literature, school systems would be wise to 'support the people who can support the children'. Several key points identified include that:

- younger teachers are more likely to be respected as online safety education leaders
- teachers need high quality, knowledge-rich resources to support implementation
- teachers must be appropriately skilled and trained, and to achieve this they need professional development, support and capacity building to develop digital knowledge, skills, and capabilities
- teachers must be aware of the most common/number, and diversity of digital devices, platforms, services, applications and sites that children use
- teachers must be clear on reporting pathways, help-seeking and referral mechanisms for their students
- all school staff must have education and training
- training must begin in preservice teacher education and continue.

This evidence can, alternatively, be grouped under two key indicators:

1. Teachers are competent and aware of their roles and responsibilities:
    - nominated members of staff with appropriate skills and responsibilities are trained and available to deal with the various issues related to online safety
    - staff role model positive behaviours in their use of digital technologies, the internet, social media and mobile devices
    - teachers know about the websites, applications and games children and young people use

    - teachers are vigilant in monitoring student online access and activity during school time
    - school staff are familiar with reporting mechanisms and escalation processes.

2. Teachers are supported and well trained:
    - online safety training is regular, ongoing and effective and contains quality up-to-date information about the knowledge, skills and competencies that children and young people need to keep safe online including how to report a problem/complaint, escalate a concern, and refer children for support services
    - staff delivering the curriculum should be well trained and involved in program planning to enhance a sense of ownership
    - training content is updated to reflect current research evidence, advances in technology, and school system policies and procedures
    - expertise is developed across a pool of staff, to ensure there is sound leadership and that knowledge and training is effectively shared in a sustainable way
    - schools train all staff to know and understand online safety within the broader network of interconnected policies and procedures, including student protection
    - teachers should be properly trained to ensure sensitive topics are conveyed in a manner that protects the health and wellbeing of vulnerable students
    - teachers should be aware of possible disclosures of sexual abuse, harassment, violence, grooming, exploitation and cyberbullying — and know how to respond appropriately
    - teachers' wellbeing (including digital wellbeing) should be considered and access to employee assistance programs made available for confidential counselling and support about incidents of concern.

(vii) Parents and carers

The material we examined and the eSafety research, specifically, is very clear on the important role parents play in children's online safety. Parents are most frequently described as partners in the process. Some specific parental actions identified in the literature include to:

- learn — upskill in digital technology
- enable — access and opportunity
- talk — with children about their experiences
- respect — children's emerging competencies and strengths
- teach — better ways of responding
- model/lead — ways of using/responding, as parents are role models — children say they wish their parents would spend less time on their devices
- mediate — between different interests, conflicts, provide emotional support
- empower — children to engage safely
- advocate — for children's safety online
- connect — be clear on reporting pathways and where to get help, ensure sources are trustworthy and children perceive trust
- help — get practical help.

In summary, parents, families and carers must be empowered and supported in their role through ongoing access to information and resources. These resources should support parents to reinforce positive online behaviours at home, help children solve problems they encounter online (including

where to find help and support) and make use of reporting pathways when necessary. There should be regular opportunities for schools' engagement with parents about online safety issues.

Online safety information distributed to parents from schools should be made available in a variety of formats which cater to the different needs of parents from diverse cultural and linguistic backgrounds.

Component 3: 'the what' and 'the how'

This component covers what should be taught in online safety education for primary and secondary school students — the curriculum/topics/contents/knowledge/skills/dispositions, and how it should be taught — the pedagogies/teaching methods/strategies/approaches. It also looks at who should teach the content (their qualifications, training, experience), when and where it should be taught, how often and how much (where this information was available).

We identified four themes in the material examined:

(i) Digital citizenship (DC)
(ii) Social emotional learning (SEL)
(iii) Specific risks (SRs)
(iv) Help-seeking.

(i) Digital citizenship

Digital citizenship fosters students' critical awareness and civic engagement. eSafety defines a digital citizen as 'a person with the skills and knowledge to effectively use digital technologies to participate in society, communicate with others and create and consume digital content'.

In the material examined, we identified a large number of statements that fit the theme 'elements of digital citizenship'. An online safety program needs to include, for example (in no particular order):

- Details about platforms and applications, and the activities that take place on each. It also needs to include key platforms for specific ages, groups and activities, and to highlight those used for video and image sharing, social networking, gaming, texting and messaging.
- Content that is specific to particular platforms, including strategies to manage issues such as inappropriate posting, nasty comments, pop-up advertisements, and generic for issues that cross different platforms e.g. gender equity, violence, fake news.
- Activities that promote democratic participation and fundamental rights on the internet.
- How individuals can manage negative experiences arising and who/what can help.
- Content about respecting privacy (the relational component), avoiding over-sharing without permission, not sharing private one-to-one communications, and strategies for not sharing personal information online.
- Information about privacy settings (the technical component), managing, storing and sharing online information.
- Information about a digital footprint including the 5 P's for a positive digital footprint: profiles, positive, permission, protect, privacy.
- Detail about the potential consequences of information sharing about, or by, children and how this might be further disseminated in different settings and by others.
- Content to help students understand that anything they put online can be seen by people they may not intend to see it, and may be there forever.
- Detail on how information is found, viewed and interpreted — and how personal online information can be used, stored, processed or shared.
- Information about:

- Digital rights licensing, copyright and ownership.
- The concept of ownership of online content and the legal implications of breaching (e.g. plagiarism and piracy).
- Respecting age limits for online services.
- Avoiding scams and malware.
- Protecting against identity theft.
- Data and credit.
- Securing passwords and devices.
- Activities to encourage critical thinking around different types of media and evaluating content for truthfulness and reliability.
- Problem-solving, promoted with the use of hypothetical online risk scenarios.

We also encountered several well-established digital citizenship frameworks as noted above (Source 6) including: the Education for a Connected World Framework (UKCCIS, 2018), the DQ Common Framework for Digital Literacy, Skills and Readiness (DQ Institute, 2019a), the Digital Citizenship Education Handbook (Council of Europe, 2019), three Digital Citizenship framework documents (Common Sense Education), including one entitled Digital Citizenship and Social and Emotional Learning (Common Sense Education, 2017), Nine Elements (Ribble, 2017) and BEaPRO (US iKeepSafe Coalition) which focuses mainly on privacy.

These frameworks acknowledge the central role of technology in students' lives. Key elements of the frameworks are shown in Table 3.

(ii) Social and emotional learning

Social and emotional learning is defined by the worldwide peak body, the Collaborative for Academic, Social, and Emotional Learning (CASEL, 2019, para. 1) as 'the process through which children and adults understand and manage emotions, set and achieve positive goals, feel and show empathy for others, establish and maintain positive relationships, and make responsible decisions'.

In the material examined, we identified statements that we coded as 'elements of social and emotional learning'. For example, learning about (in no particular order):

- digital resilience
- proactive coping strategies
- dealing with negative situations and emotions, including online
- how to respond to others' behaviours in a range of scenarios
- respecting others and being respected — understanding and respecting our own and others' rights, giving and receiving respect
- communicating respectfully — not doing or saying anything online that the person wouldn't in real life
- understanding rights and responsibilities in the digital environment
- bystanders/upstanders — e.g. 'Save it, Speak up, Be supportive, Report it, Check it, Don't stand by. It could be you'
- sharing responsibility for online safety and welfare
- how to support and connect with others
- relationships, relationship skills, and developing positive and collaborative relationships

- cooperation, decision making, problem solving, compromise, asking for help, group entry and participation and dealing with feelings including anger.

In our searches we did not search, specifically, for social and emotional learning programs. The statements we found were in, and across, the broad range of material we examined and were clearly identifiable as elements from social and emotional learning. Although it was beyond the scope of this review to assess specific social and emotional learning programs, previous reviews have shown universal school-based social and emotional learning programs can promote student wellbeing, and have positive effects on a range of problem student behaviours as well as their academic performance (Durlak et al., 2011).

The statements above overlap with many of the elements we identified as effective in addressing specific risks. Our findings suggest, therefore, that incorporating social and emotional learning in online safety education would be a sound approach.

(iii) Specific risks

In the material reviewed for this research we identified several specific online safety risks that should be addressed within online safety education (shown in Table 5). However, we did not find specific 'what and how' strategies that educators can use to address the risks identified. There is conflicting advice in the literature about the benefits of integrated versus discrete content, and generic versus specific skills development. For example, we found statements calling for 'integration of multicomponent programmes within a whole school approach, based on generic social and emotional skills training addressing common risk and protective factors'. Yet, the broader literature on interventions (not reviewed as part of this project) suggests that specific risks will require discrete content and specific skills development. The specific risks for which we identified an evidence base included: online safety, cyberbullying, sexual violence, and internet/gaming addiction. The tables below present the evidence-based information considered necessary when teaching about specific online safety risks.

Table 7: Online safety

Online safety	
What to teach	**How to teach**
Content needs to be structured in a way that makes sense to students and teachers and ensures consistency in delivery. Content should be documented in program manuals and lesson plans. **General rules of thumb** • Need to have a clear understanding of what specific issues, problems, behaviours and outcomes are to be prevented.	**What works** • Stimulating, trustworthy, credible, meaningful, and contextually relevant learning experiences with creative and interactive message delivery. • Skill-based programs with active learning strategies and defined theoretical rationales. • Active, focused, skill-based lessons, focused on causal and risk factors identified by research, with adequate

- Need to have facts about the extent of these issues, problems, behaviours for children and young people (to focus on actual rather than perceived risks).
- Need to understand the dynamics of the issue/problem/behaviour very well.
- Content needs to address risk factors and build protective factors: empower children to protect themselves and others and find appropriate help when needed.

Internet safety messages

Young people need to:

- be cautious about risky sites and modes of communication — safety first
- learn to keep their identities private
- understand how to keep themselves safe from relevant risks online and on social media
- develop empathy, sense of self and self-awareness, coping, healthy behaviours and social skills (overlap with social and emotional learning and cyberbullying prevention).

Effective programs

Effective online safety programs should:

- include specific examples of online risks
- include children in curriculum development — so they have relevant knowledge and expertise, and bottom-up approach fosters ownership
- know language children and young people use to describe risk/harm online — terms such as drama, toxic, gross, bullying, hurtful, creepy, upsetting, disgusting, terrifying overwhelming, offensive, traumatising (children will be more engaged when these terms are used rather than 'harm')

dosage (i.e., single-session lessons were not enough, several lessons are needed with each lesson building on the previous) (Jones et al., 2013).

- Peer-education in prevention/peer-led programs.
- Homework.
- Regular reinforcement of concepts and skills.

Hallmarks of effective approaches

(SAFE — structured and sequenced, active, focused and explicit)

1. Structured and sequenced — children learn skills sequentially from less complex to more complex — each lesson builds on the last and includes review of prior learning.
2. Active — youth act on the material, discuss, debate, ask questions, respond to open-ended questions, role play, practice what they have been taught, and receive feedback.
3. Focused — there is adequate time, effort and attention to skill-building.
4. Explicit — there are clear and specific learning objectives.

Other suggested strategies

- Establish and maintain a culture of respect and integrity where students feel comfortable raising issues and talking with adults about their experiences online and feel confident that meaningful steps can, and will, be taken to help them resolve problems.
- Remember that technical skills may be taught in shorter amount of time. Relational skills need longer time.
- Note that booster sessions may be required. In the literature this is tied up with the notion of homework as a

• use positive and effective content delivered in a climate of mutual respect, responsibility, integrity, and accountability • use empowering messages to support young people to help themselves and their friends • make educational materials personally relevant for children • ensure whatever is taught is up-to-date, current, contemporary and relevant.	booster and a way to involve parents/families. • Ensure consistent and continuous implementation. • Use trained facilitators/teachers. • Use school-based champions to oversee implementation. • Seek parent involvement — can act as a type of booster. **What can help** • Positioning children as capable, creative and competent. • Listening. • Not judging. • Using simple language. • Adopting a positive and supportive tone. **What does not work** • Fear-inducing and scare tactics, lectures as a means of disseminating information, short sessions for complex issues — relational issues, for example, require longer than one x 45 minute session. • Non-interactive/one-way, lecture-based, one-off sessions. • Zero tolerance and 'get tough' suspensions and exclusions in the absence of positive and preventive approaches. • Rigid control of student behaviour. • Students receiving punitive and negative consequences in all cases. • Punishment without support. • Unfair and inconsistent use of discipline.

Table 8: Cyberbullying prevention

Cyberbullying prevention	
What to teach	**How to teach**
Redefining cyberbullying as a social and public health issue and adopting a public health approach to addressing it. Comprehensive prevention includes 'whole of community': (i) laws and policies (ii) educational approaches (iii) school initiatives (iv) parents. **Key components of effective bullying prevention identified in reviews** • Whole school approach — collaborative and systemic, involving students, teachers, parents, other school staff and wider community. • Educational content that supports students to develop social emotional skills. • Teaching effective ways to respond to cyberbullying. For example **technical aspects** (specific strategies such as 'block and tell', 'untag', 'avoid', 'ignore', 'close', 'turn off', 'delete', 'mute', 'capture and report' etc.) and **relational aspects** (specific strategies for dealing with nastiness and unkindness, gossip and rumours, aggressive or violent comments, trolling, roasting, catfishing, sextortion etc.) and **help seeking aspects** (telling a trusted adult, get assistance, peers, helplines etc.). • Teaching the difference between bullying and other forms of conflict, violence and aggression. **Other suggested content** • Addressing specific risks for specific platforms (different for different age	**What works** • Creation of supportive environments for children, young people, parents, carers and communities. • More structured interventions over a longer duration. • Interventions need to be intensive and long-lasting to have an impact. • Child-focused and targeted early intervention measures to address cyberbullying that involve working with the person being targeted, their family and school, social media services, the perpetrator, the bystanders and, when appropriate, the police. **What does not work** • Bans on use of ICT in response to bullying — as this may result in under-reporting of bullying behaviour. **Effective strategies to reduce victimisation include** videos/multimedia/games, disciplinary measures, working with peers, parent training and cooperative group work. **Effective strategies to reduce perpetration include** parent training, improved supervision, disciplinary measures, school assemblies, videos, information for parents, classroom rules and classroom management. **Other suggested strategies** • Discussion to foster empathy, perspective taking. • Use of hypothetical scenarios.

groups and sub-groups), and generic risks for generic use. • Fostering and promoting alternatives to conflict rather than focusing on 'stopping' cyberbullying. • Providing opportunities to enhance personal and relationship skills. • Teaching upstander behaviour — what it looks like and when it may work then use small group activities, role playing and debriefing.	• Videos and multimedia to create problem-based scenarios. • Role playing in small groups to develop skills (can be learned via modelling, rehearsal, practice, and feedback). • Games that promote respectful behaviours – e.g. in virtual learning environments. • Consistent recurring messages, including online (for example on a school website), with information explaining how schools ensure students' online safety. • Strategies to foster school connectedness and a positive school climate. Extracurricular activities, for example, can help develop connectedness to school (e.g. sport, arts, music, recreation, volunteering). • Early intervention and support for targets. • Support for bullying targets by high-status peers.

Table 9: Violence prevention

Sexual violence prevention	
What to teach	**How to teach**
Sexual violence prevention Effective programs include: • Information about perceived peer group expectations in the context of sexual development. • Interventions with girls to focus on relational aggression. • Interventions with boys to focus on increasing affective and cognitive empathy. • Teaching legal aspects — but not as the exclusive focus. Similarly, partnerships with police/law enforcement are important, but are one of many partnerships required. • Social and emotional strategies for sexual bullying prevention. • Community participation, service provider collaboration, strong school policy and codes of conduct.	**What works** Effective programs are: • Comprehensive — skill building, establishing social norms, policy change, community intervention, physical environment alterations. • Appropriately timed — begins early, target younger students. • Taught using interactive methods —with active learning activities for skill development. • Of sufficient duration — longer programs achieve longer lasting results. • Positive — fostering healthy relationships among and between, students, parents, peers, teachers, and other adults. • Is socio-culturally relevant — sensitive to and reflect community norms. • Conducted by well-trained staff — stable, committed, competent and can connect with participants. • Theory driven — explains how the various elements of the program contributes to achieving the desired outcomes for students.
Child sexual abuse prevention Effective programs include: • Teaching safety and prevention concepts such as body ownership, private parts, distinguishing appropriate and inappropriate touches, distinguishing types of secrets, grooming behaviours, safe and unsafe situations, and who to tell.	**What works** Effective programs include: • Rehearsal, practice or role-play, discussion, modelling. • A specific suite of teaching strategies used together including instruction, modelling, rehearsal, social reinforcement, shaping, feedback, and group mastery. • Revising material previously taught.

• Peer bystander education, noticing warning signs, what to do if someone discloses abuse. • Clear messages that children are not to blame. • Links to personal safety/child protection curriculum/keeping safe curriculum.	• Delivery formats such as film, video, and DVD formats, and multimedia in a few. Additional resources included songs puppets, comics, a colouring book, a storybook, and games • More than one single session. **What does not work** • 'Good touch, bad touch' (confusing and conveys the message that sexual touching is bad) — instead teach children how to recognise appropriate and inappropriate touches.
Harmful sexual behaviour with peers, sexual offending, technology-assisted harmful sexual behaviour Effective programs should: • Be nested in whole-school, whole-community, policy-driven approach. • Focus on sexual knowledge, beliefs and behaviours. • Have clear messages about the inappropriateness and illegality of engaging younger children in sexual behaviour. • Restrict access to high-risk websites. • Understand power and consent, and pressure. • Challenge unhelpful beliefs and attitudes. • Provide sexual cyber-victim empathy (overlap with cyberbullying).	**What works** Effective prevention programs include: • Appropriate developmental timing before average age of onset (as determined by the most recent, reliable, rigorous research). • Prevention beginning early and corresponding with ages that children enter online environments. • Acknowledgement that positive effects are enhanced for boys when interventions are delivered in mixed gender classroom settings. • Promoting parental awareness of higher risk situations. • Shared understandings between parents and youth about what constitutes appropriate and inappropriate sexual behaviour. • Sufficient multisession dosage. • Presentation of information in multiple formats. • Opportunities to practice skills. • Intervention implementation with fidelity.
Unwanted online sexual exposure and solicitation Programs should teach:	**What works** Effective programs: • Involve health, education and criminal justice systems (i.e. multi-sectorial).

• Healthy relationships (on- and off-line) — changing social norms, attitudes and behaviours. • How to recognise and respond to solicitation online — unwanted contact online). • Social skills, which overlap with social and emotional learning.	• Have messages that target young people and parents (this is difficult for children experiencing family violence and abuse, or who are involved with child protection system or disengaged from school). • Recognise that for children at risk, filtering and blocking software will not work. • Foster strong connections with peers. • Acknowledge the role of peers in assisting disclosure and help seeking — how to support disclosure by dropping judgement, shame, guilt and embarrassment. • Use strategies to discourage self-blame. • Offer a whole-school approach.
Grooming Programs should teach: • The specifics about grooming behaviour: cultivating personal and friendly relationships, regular intense contact, requests increasing in intensity, gifts, flattery, simultaneous grooming of those close to victim, manipulation, deception, secrecy/isolation, sexualisation, erratic temperament and nastiness. • To increase knowledge of grooming strategies and behaviours and how to respond (e.g. raise awareness of strategies adults use for encouraging adolescents to engage in sexually explicit discussions and interactions online). • To raise awareness of coercion into sexual activity for material reward — label this as sexual exploitation.	**What works** No strategies identified.
Exposure to pornography Effective programs:	**What works** No strategies identified.

• Include sex education which can help counter negative effects of viewing pornography. • Address the messages that boys take from pornography, their expectations for the girls with whom they interact. • Address the messages that girls take from pornography, how they may be influenced within actual or potential sexual relationships. • Gender equality — drivers of gender-based violence (overlap with sexual violence, above). • Explore what sexual harassment is. • Look at coercion and consent in relationships. • Include victim blaming and shaming. • Include sharing of self-generated sexual images and videos (aggravated/deliberate/experimental).	
Sharing sexual images Effective programs include: • Promotion of positive and preventative behaviours and respectful relationships. • What healthy relationships look like. • Power and consent in relationships — what do power differentials look like? • Understanding and respecting the concept of genuine, enthusiastic consent. • How to manage requests or pressure to provide (or forward) sexual images. • How to manage receipt of sexual images, including who to tell, what to say, what to do, and where to get support from within or outside the school. • Sexual abuse prevention concepts for this purpose: body ownership (my body belongs to me), saying no and how to be assertive, trusting intuition, using support systems (for example, knowing who to tell and where to seek advice),	**What works** Effective programs: • Reframe thinking around victim-blaming. • Do not focus on blaming the victim and instead frame the non-consensual sharing of images as bullying behaviour, where third parties can discourage the sharing of these images. • Acknowledge, for image-sharing, young people's rights and responsibilities around self-representation and sexual expression. • Use 'harm reduction' principles rather than promoting abstinence. • Distinguish between non-consensual image production and sharing (distribution) and consensual image production and/or sharing (distribution). Use tree diagrams to understand pathways through sharing and consent including for conditions under which images are generated (e.g. voluntary, aggravated, coercion, unsure).

distinguishing different types of touches (safe/unsafe), secrets and surprises and that victims are not to blame. • Understand youth-self-produced sexual imagery — what it is, how and when it is most likely to be encountered. • Discuss the consequences of requesting, forwarding or providing images, and understanding when this is and is not coercive and/or abusive. • Teach laws but do not focus solely on laws or use threatening language. • Understanding the risk of damage to people's feelings and reputation. • Recognising abusive and coercive language and behaviours. • Sharing of sexual images — challenging gendered double-standards in relation to concepts such as 'provocativeness', 'self-confidence', 'responsibility', 'consequences' and 'reputation'. • Not shaming young people for sharing self-produced sexual images, instead, challenging the behaviour of people who share images without consent.	

Table 10: Prevention of internet and gaming addiction

Prevention of internet and gaming addiction	
What to teach	**How to teach**
Effective programs: • Address underpinning risk factors by building positive relationships with others, offer opportunities to diversify experiences and learn healthy and valued behaviours, values, morals and skills. • Teach life skills: life skills are defined as a group of psychosocial competencies and interpersonal skills that help people make informed decisions, solve problems, think critically and creatively, communicate effectively, build healthy relationships, empathise with others, and cope with and manage their lives in a healthy and productive manner (overlap with social and emotional learning, cyberbullying prevention). • Address gaming, anonymity including in-game chat — which is a potential space for grooming — bullying in the context of gaming, victimisation and perpetration. • Acknowledge content overlap with gaming and other prevention programs: drugs, alcohol, risky sex and gambling prevention in schools (evidence is not specific or strong, however).	Effective programs: • Start early. • Involve the whole school community, including community service providers. • Include peer-led interventions and peer support systems. • Use promotion of positive psychology variables (i.e. self-esteem, self-efficacy). • Aim to enhance skills and competencies to prevent addiction (i.e. self-control, emotion regulation, and social interaction) as well as increase positive emotions and enhance social competencies. • Complement school programs by providing parents with strategies that reinforce what is being taught in school.

(iv) Help-seeking

Teaching help-seeking and help-seeking behaviour was a very common theme in the examined material. It appeared in digital citizenship programs, social emotional learning programs, cyberbullying prevention programs, sexual violence prevention programs, and internet and gaming addiction prevention programs. It is viewed as a protective factor against victimisation, and as a

behaviour that can be taught and learned. The best practice features are presented in Table 11. Help-seeking appears integral in preventing and responding to online safety issues.

Table 11: Help-seeking

Help seeking	
What to teach	**How to teach**
Effective programs include: • Information about where to find and how to contact people who can help. • The importance of telling a parent or other adult if they have a negative experience online • Where to go for advice and support — both for victims and offenders/perpetrators. • Information about the role of Kids Helpline and how to access their services. • How to seek help from a parent for serious issues. • Information encouraging disclosure to a trusted person. • How to help friends by passing on concerns. • Formal channels and clear processes for reporting/dealing with online issues. • What action is taken when they report. • Remedies and seeking redress — understanding that they have rights in a digital environment • A restorative justice approach (support for bullies and victims).	Effective programs include: • How to identify and report negative online experiences and critical incidents. • How to make informed choices about disclosing abuse, victimisation or targeting. • Role of peers in assisting with disclosure and help seeking — how to support disclosure by dropping judgement, shame, guilt, embarrassment. Strategies to discourage self-blame.

Other observations

In the material examined for this research there were other relevant points that did not fit neatly into the seven components. These are our observations on: details relevant to external providers delivering online safety education in schools, and what seems to be missing.

Observations relevant to external providers of online safety education

- There is very little independent, rigorous evaluation of online safety education programs worldwide.
- Programs need logic models, and rigorous evaluation.
- Need to improve program quality by looking at effective prevention principles.
- Only cyberbullying seems to conceptualise prevention using a public health approach.
- Education providers need to engage with the literature — especially research on children's use of digital technology (e.g. Global Kids Online, UK Kids Online, EU Kids Online, eSafety, Netsafe and UNICEF's State of the World's Children).
- There is a need to translate these reports/research into policy and practice points — looking for recommendations and including these in education offerings.
- Communities of practice could be used to increase engagement with research by asking: what does this research tell us about what and how we need to teach online safety education in schools?
- Not all risk results in harm. Risk and harms differ and there is a concept of 'risking on/for purpose'.
- Programs require regular review to ensure relevance (annually is mentioned).
- Strategies to be avoided include: scaremongering, prohibition/abstinence, 'law-only' approaches, poor information or translation of information about the law, victim blaming and shaming, once-off/one shot (but need more research about which children and young people, if any, benefit from one-shot and why), didactic/lecture-only formats and the misuse/incorrect contextual use of terminology which children will perceive outdated content and approaches.
- In adopting a public health approach there is scope to design and implement universal prevention (for all children), as well as designing and implementing more nuanced targeted prevention to vulnerable children and children at greater risk.

Observations on what seems to be missing

- Terminology of anti-discrimination/the right to non-discrimination and the concept of vilification.
- Terminology of harassment including sexual harassment — the difference between harassment, bullying and other types of violence/aggression.
- Discussion about what counts as 'freedom of speech' online.
- Violence as an overarching concept for online issues.
- In Australia, clear links to statutory child protection for serious, harmful online experiences.
- System-wide approaches, as opposed to school-wide or whole-school approaches.
- A more accessible, publicly available portal where Australian online safety education programs and providers are listed, including information about their contents (the what) and methods (the how).
- Online safety education program listings in program guides and registries that are provided to schools to assist with program adoption decisions (e.g. CASEL Programs Guide or the UK Education Endowment Foundation).
- Duty of care/liability in negligence information for teachers in education and training, and professional learning.
- An examination of the circumstances where trauma-informed approaches may be warranted and what is best practice in universal delivery of school-based online safety education.
- Clear information on how online safety education should be customised for specific groups.
- Randomised controlled trials on the effectiveness of specific online safety education programs offered in Australian schools.

References

References to documents included in this review (n=199)

Ang, R. P. (2015). Adolescent cyberbullying: A review of characteristics, prevention and intervention strategies. Aggression and Violent Behavior, 25, 35-42. doi: 10.1016/j.avb.2015.07.011

Antcliff, G., Daniel, B., Burgess, C., & Sale, A. (2011). Resilience practice framework. Retrieved from benevolent.org.au

Atkinson, C., & Newton, D. (2010). Online Behaviours of Adolescents: Victims, Perpetrators and Web 2.0 (Vol. 16, pp. 107-120): Journal of Sexual Aggression, 16(1), 107–120. doi:10.1080/13552600903337683

Australian Communications and Media Authority. (2011). Like, post, share: Young Australians' experience of social media. Qualitative Research Report. Retrieved from acma.gov.au

Australian Human Rights Commission. (2016). Bullying and harassment. Retrieved from www.humanrights.gov.au

Australian Human Rights Commission. (2018). National principles for child safe organisations. Retrieved from humanrights.gov.au

Australian Institute of Family Studies. (2014). The good practice guide to Child Aware Approaches: Keeping children safe and well. Retrieved from aifs.gov.au

Aynsley, C., Davies, H., Girling, S., Hammond, R., & Hughes, T. (n.d.). 'Sexting' in schools: Advice and support around self-generated images. What to do and how to handle it. Retrieved from parentsprotect.co.uk/files/Sexting-in-Schools-eBooklet-FINAL-30APR13.pdf

Backe, E. L., Lilleston, P., & McCleary-Sills, J. J. (2018). Networked individuals, gendered violence: a literature review of cyberviolence. 5(3), 135-146. doi: 10.1089/vio.2017.0056

Baek, J., & Bullock, L. M. (2014). Cyberbullying: a cross-cultural perspective. Emotional and Behavioural Difficulties, 19(2), 1–13. doi: 10.1080/13632752.2013.849028.

Baldry, A. C., Farrington, D. P., & Sorrentino, A. (2015). 'Am I at risk of cyberbullying'? A narrative review and conceptual framework for research on risk of cyberbullying and cybervictimization: The risk and needs assessment approach. Aggression and Violent Behavior, 23, 36-51. doi: 10.1016/j.avb.2015.05.014

Barnard-Willis, D. (2012). E-safety education: Young people, surveillance and responsibility. Criminology and Criminal Justice, 12(3), 239-255. doi: 10.1177/1748895811432957

Barry, M., Clarke, A., Jenkins, R., & Patel, V. (2013). A systematic review of the effectiveness of mental health promotion interventions for young people in low and middle income countries. Bmc Public Health, 13(1), 835. doi: 10.1186/1471-2458-13-835

Best, P., Manktelow, R., & Taylor, B. (2014). Online communication, social media and adolescent wellbeing: A systematic narrative review. Children and Youth Services Review, 41, 27–36. doi: 10.1016/j.childyouth.2014.03.001

Beyond Blue Ltd. (2017). Building resilience in children aged 0–12: A practice guide. Retrieved from resources.beyondblue.org.au/prism/file?token=BL/1810_A

Blazer, C., & Miami-Dade County Public Schools, R. S. (2012). Social Networking in Schools: Benefits and Risks; Review of the Research; Policy Considerations; and Current Practices. Information Capsule, 1109, 1-23. Retrieved from files.eric.ed.gov/fulltext/ED536527.pdf

Brown, E. A. (2019, February 15th). Suicide Memes Might Actually Be Therapeutic. *The Atlantic*. Retrieved from theatlantic.com/health/archive/2019/02/suicide-memes/582832/

Bullying. No Way! (2016). Launchpad: Your school's resources for talking and teaching about bullying. Retrieved from bullyingnoway.gov.au/Resources/lessonplans/Launchpad.pdf

Bullying. No Way! (2016). STEPS Decision Making Framework. Retrieved from bullyingnoway.gov.au

Burrow-Sanchez, J. J., Call, M. E., Zheng, R., & Drew, C. J. (2011). How School Counselors Can Help Prevent Online Victimization. Journal of Counseling & Development, 89(1), 3–10. doi: 10.1002/j.1556-6678.2011.tb00055.x

Cantone, E., Piras, A., Vellante, M., Preti, A., Daníelsdóttir, S., D'Aloja, E., & Bhugra, D. (2015). Interventions on bullying and cyberbullying in schools: a systematic review. Clinical Practice and Epidemiology in Mental Health : CP & EMH, 11(Suppl 1 M4), 58–76. doi: 10.2174/1745017901511010058

Cassidy, W., Faucher, C., & Jackson, M. (2013). Cyberbullying among youth: A comprehensive review of current international research and its implications and application to policy and practice. School Psychology International, 34(6), 575-612. doi:10.1177/0143034313479697

Centre for Evidence and Implementation. (2017). Implementation in education – findings from a scoping review. Retrieved from researchgate.net/publication/319176978_Implementation_in_Education_-_Findings_from_a_Scoping_Review

Chan, H., & Wong, D. (2015). Traditional school bullying and cyberbullying in Chinese societies: Prevalence and a review of the whole-school intervention approach. Aggression and Violent Behavior, *23*, 98–108. doi: 10.1016/j.avb.2015.05.010

Childnet International. (2016). Cyberbullying: Understand, prevent, respond. Guidance for schools. Retrieved from childnet.com/ufiles/Cyberbullying-guidance2.pdf

Childnet International. (2017). Online Reputation Checklist. Retrieved from childnet.com/ufiles/Online-Reputation-Checklist.pdf

Childnet International. (2018). STAR SEN Toolkit: New resource. Retrieved from http://childnet.com/resources/star-sen-toolkit

Childnet International. (2018). Using Technology Safely: A checklist for using technology safely with young people in the classroom, at school or even at home. Retrieved from

childnet.com/ufiles/Using-technology-safely-checklist.pdf

Chisholm, J. F. J. (2014). Review of the status of cyberbullying and cyberbullying prevention. 25(1), 77.

Choi, A. (2018). Emotional well-being of children and adolescents: Recent trends and relevant factors. Paris: Organisation for Economic Cooperation and Development (OECD).

Choo, K.-K. R. (2009). Responding to online child sexual grooming: an industry perspective. Trends and Issues in Crime and Criminal Justice, 379, 1-6. Retrieved from aic.gov.au

Chung, T. W. H., Sum, S. M. Y., & Chan, M. W. L. (2019). Adolescent Internet Addiction in Hong Kong: Prevalence, Psychosocial Correlates, and Prevention. Journal of Adolescent Health, 64(6, Supplement), S34-S43. doi: 10.1016/j.jadohealth.2018.12.016

Cohen-Almagor, R. (2018). Social responsibility on the Internet: Addressing the challenge of cyberbullying. Aggression and Violent Behavior, 39, 42-52. doi: 10.1016/j.avb.2018.01.001

Common Sense Education. (2017). Digital Citizenship & Social and Emotional Learning: Navigating Life's Digital Dilemmas. Retrieved from commonsense.org/education/sites/default/files/tlr-blog/cse-digitalcitizenship-sel.pdf%20

Common Sense Media. (2018). The new normal: Parents, teens and devices around the world. Retrieved from commonsensemedia.org/research/The-New-Normal-Parents-Teens-and-Devices-Around-the-World

Commonwealth of Australia. (2011). High-Wire Act: Cyber-Safety and the Young. Joint Select Committee on Cyber Safety: Interim Report. Retrieved from aph.gov.au/parliamentary_business/committees/house_of_representatives_committees?url=jscc/report/fullreport.pdf

Commonwealth of Australia. (2017). Royal Commission into Institutional Responses to Child Sexual Abuse Final Report Volume 6: Making Institutions Child Safe. Retrieved from childabuseroyalcommission.gov.au/sites/default/files/final_report_-_volume_6_making_institutions_child_safe.pdf

Council of Australian Governments. (2009). Protecting children is everyone's business: National framework for protecting Australia's children 2009-2020. Retrieved from dss.gov.au

Council of Australian Governments (COAG) Bullying and Cyberbullying Senior Officials Working Group. (2018). Enhancing community responses to student bullying, including cyberbullying: Report and Work Program. Retrieved from coag.gov.au/sites/default/files/communique/bcsowg-report-work-program.pdf%20%20

Council of Europe. (2018). Guidelines to respect, protect and fulfil the rights of the child in the digital environment. Retrieved from rm.coe.int/guidelines-to-respect-protect-and-fulfil-the-rights-of-the-child-in-th/16808d881a

Council of Europe. (2019). Digital Citizenship Education Handbook. Retrieved from rm.coe.int/16809382f9

Couvillon, M., & Ilieva, V. (2011). Recommended Practices: A Review of Schoolwide Preventative Programs and Strategies on Cyberbullying. Preventing School Failure: Alternative Education for Children and Youth, 55(2), 96–101. doi: 10.1080/1045988X.2011.539461

Cross, D., Li, Q., Smith, P., & Monks, H. (2012). Understanding and Preventing Cyberbullying: Where Have We Been and Where Should We Be Going? In Cyberbullying in the Global Playground: Research from International Perspectives (pp. 287–305). Wiley-Blackwell. doi: 10.1002/9781119954484.ch14

Cross, D., Monks, H., Campbell, M., Spears, B., & Slee, P. (2011). School-based strategies to address cyber bullying. Centre for Strategic Education, *119*, 1-12. Retrieved from ro.ecu.edu.au/cgi/viewcontent.cgi?referer=https://scholar.google.com.au/&httpsredir=1&article=1355&context=ecuworks2011

Cross, D., & Walker, J. (2012). Using research to inform cyberbullying prevention and intervention. In Principles of Cyberbullying Research: Definitions, Measures, and Methodology (pp. 274–293). Taylor and Francis. doi: 10.4324/9780203084601

Degue, S., Valle, L., Holt, M., Massetti, G., Matjasko, J., & Tharp, A. (2014). A systematic review of primary prevention strategies for sexual violence perpetration. Aggression and Violent Behavior, 19(4), 346–362. doi: 10.1016/j.avb.2014.05.004

Della Cioppa, V., O'Neil, A., & Craig, W. (2015). Learning from traditional bullying interventions: A review of research on cyberbullying and best practice. Aggression and Violent Behavior, 23, 61–68. doi: 10.1016/j.avb.2015.05.009

Department for Education and Child Development South Australia. (2017). Parent easy guide 63: Cyber safety. Retrieved from parenting.sa.gov.au/pegs/cybersafety-parent-easy-guide-pdf-172kb.pdf

Department of Communications and the Arts. (2018). Report of the Statutory Review of the Enhancing Online Safety Act 2015 and the Review of Schedules 5 and 7 to the Broadcasting Services Act 1992 (Online Content Scheme). Retrieved from communications.gov.au/publications/report-statutory-review-enhancing-online-safety-act-2015-and-review-schedules-5-and-7-broadcasting

Department of Education and Training Victoria. (2017). Protect: A Guide to Support Victorian Schools to Meet Child Safe Standard 7: Strategies to Promote Child Empowerment and Participation. Retrieved from education.vic.gov.au/Documents/about/programs/health/protect/ChildSafeStandard7_Guidance.pdf

Department of Education and Training Victoria. (2019). School Policy: Bullying. Retrieved from education.vic.gov.au/school/principals/spag/safety/Pages/bullying.aspx

Department of Education New South Wales. (2019). Digital Citizenship. Retrieved from digitalcitizenship.nsw.edu.au

Department of Education Tasmania. (2018). 2018-2021 Child and Student Wellbeing Strategy: Safe, well and positive learners. Retrieved from documentcentre.education.tas.gov.au/Documents/Child%20and%20Student%20Wellbeing%20Strategy.pdf

Department of Education Tasmania. (2018). 2018-2021 Respectful Schools and Workplaces

Framework. Retrieved from documentcentre.education.tas.gov.au/Documents/Respectful-Schools-and-Workplaces-Framework.pdf

Department of Education, Training and Employment Queensland. (2012). Cybersafety and cyberbullying: A guide for parents and caregivers. Retrieved from qed.qld.gov.au

Department of Education, Training and Employment Queensland. (2013). Cyberbullying and reputation management: Incident management guidelines for principals. Retrieved from qed.qld.gov.au

Department of Education Training and Employment Queensland. (2013). Young people and sexting in Australia: Ethics, representation and the law. Final Report. Retrieved from qed.qld.gov.au

Department of Families Housing Community Services and Indigenous Affairs & National Framework Implementation Working Group Australia. (2011). An outline of National Standards for out-of-home care: A priority under the National Framework for Protecting Australia's Children 2009-2020. Retrieved from dss.gov.au

Department of Social Services Australia. (2018). Supporting families, communities and organisations to keep children safe: national framework for protecting Australia's children 2009-2020. Fourth action plan 2018-2020. Retrieved from dss.gov.au

DQ Institute. (2017). Digital Intelligence (DQ): A Conceptual Framework & Methodology for Teaching and Measuring Digital Citizenship Retrieved from dqinstitute.org/wp-content/uploads/2017/08/DQ-Framework-White-Paper-Ver1-31Aug17.pdf

DQ Institute. (2019a). DQ Global Standards Report 2019: Common Framework for Digital Literacy, Skills and Readiness. Retrieved from dqinstitute.org/wp-content/uploads/2019/03/DQGlobalStandardsReport2019.pdf

DQ Institute. (2019b). What is the DQ Framework: Global standards for digital literacy, skills, and readiness. Retrieved from dqinstitute.org/dq-framework/

Dunkels, E. (2010). A Critical Perspective on Online Safety Measures. Nordic Journal of Digital Literacy, 5, 72–85. Retrieved from doaj.org/article/7a7855b8c3aa4898b5f4036d346e415f

Education Services Australia. (2018). Australian Student Wellbeing Framework. Retrieved from studentwellbeinghub.edu.au

Englander, E. K. (2012). Spinning Our Wheels: Improving Our Ability to Respond to Bullying and Cyberbullying. Child and Adolescent Psychiatric Clinics of North America, 21(1), 43-55. doi: 10.1016/j.chc.2011.08.013

Erebus International. (2017). Review of current theoretical and design principles underpinning the Life Education program, Report to Life Education Australia. Retrieved from lifeeducation.org.au/content/legacy/images/pdfs/erebus-report-to-life-education-australia-february-2017-v7.pdf

Espelage, D. L., & Hong, J. S. (2017). Cyberbullying prevention and intervention efforts: current knowledge and future directions. Canadian Journal of Psychiatry, 62(6), 374-380. doi: 0.1177/0706743716684793

Espelage, D. L., Hong, J. S., & Valido, A. (2018). Cyberbullying in the United States. In A. Baldry, C. Blaya, & D. Farrington (Eds.) International Perspectives on Cyberbullying. Palgrave Studies in Cybercrime and Cybersecurity. Palgrave Macmillan, Cham. doi: 10.1007/978-3-319-73263-3_4

Espelage, D. L., Valido, A., Hatchel, T., Ingram, K. M., Huang, Y., & Torgal, C. (2019). A literature review of protective factors associated with homophobic bullying and its consequences among children & adolescents. Aggression and Violent Behavior, 45, 98-110. doi: 10.1016/j.avb.2018.07.003

EU Kids Online. (2014). EU Kids Online: Findings methods recommendations. Retrieved from lsedesignunit.com/EUKidsOnline/html5/index.html?page=1&noflash

Evans, C., Fraser, M., & Cotter, K. (2014). The effectiveness of school-based bullying prevention programs: A systematic review. Aggression and Violent Behavior, 19(5), 532–544. doi: 10.1016/j.avb.2014.07.004

Farah, R. (2018). Early Interventions: Preventing at-risk youth from the path of Sexual Exploitation: A Systematic Review. Retrieved from Sophia, the St. Catherine University repository website: sophia.stkate.edu/msw_papers/847

Finkelhor, D. (2014). Commentary: Cause for alarm? Youth and internet risk research — a commentary on Livingstone and Smith (2014). Journal of Child Psychology and Psychiatry, 55(6), 655-658. doi: 10.1111/jcpp.12260

Fryda, C., & Hulme, P. (2015). School-Based Childhood Sexual Abuse Prevention Programs: An Integrative Review. The Journal of School Nursing, 31(3), 167–182. doi: 10.1177/1059840514544125

Gaffney, H., Farrington, D. P., Espelage, D. L., & Ttofi, M. M. (2019). Are cyberbullying intervention and prevention programs effective? A systematic and meta-analytical review. Aggression and Violent Behavior, 45, 134-153. doi: 10.1016/j.avb.2018.07.002

Gaffney, H., Ttofi, M. M., & Farrington, D. P. (2019). Evaluating the effectiveness of school-bullying prevention programs: An updated meta-analytical review. Aggression and Violent Behavior, 45, 111-133. doi: 10.1016/j.avb.2018.07.001

Gentile, D. A., Bailey, K., Bavelier, D., Brockmyer, J. F., Cash, H., Coyne, S. M., ... Young, K. (2017). Internet Gaming Disorder in Children and Adolescents. Pediatrics, 140, S81-S85. doi: 10.1542/peds.2016-1758H

Global Kids Online. (2019). Children's rights in the digital age: Gathering global evidence on children's rights opportunities and risks. Retrieved from globalkidsonline.net

Her Majesty's Government. (2019). Online Harms White Paper. Retrieved from assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/793360/Online_Harms_White_Paper.pdf

Hong, J. S., & Espelage, D. L. (2012). A review of research on bullying and peer victimization in school: An ecological system analysis. Aggression & Violent Behavior, 17(4), 311-322. doi:10.1016/j.avb.2012.03.003

House of Representatives Joint Select Committee on Cyber-Safety. (2013). Inquiry into Issues Surrounding Cyber-Safety for Indigenous Australians. Retrieved from

aph.gov.au/Parliamentary_Business/Committees/House_of_Representatives_Committees?url=jscc/indigenous_australians/report.htm

International Centre for Missing and Exploited Children. (2018). Child protection training checklist. Retrieved from icmec.org/wp-content/uploads/2018/02/ICMEC-FINAL-Child-Protection-Training-Checklist.pdf

Johnston, H., & Ronken, C. (2017). The 3 Piers to Prevention: Educate, Empower, Protect. Solid Foundations to Making Australia the Safest Place in the World to Raise a Child. Bravehearts Research Report Retrieved from bravehearts.org.au/wp-content/uploads/2018/01/Research-Report_The-3-Piers.pdf

Jones, L. M. (2010). The future of internet safety education: Critical lessons from four decades of youth drug abuse prevention. Retrieved from publius.cc/printpdf/future_internet_safety_education_critical_lessons_four_decades_youth_drug_abuse_prevention

Jones, L. M., & Mitchell, K. J. (2016). Defining and measuring youth digital citizenship. New Media and Society, 18(9), 2063-2079. doi: 10.1177/1461444815577797

Jones, L. M., Mitchell, K. J., & Walsh, W. A. (2013). Evaluation of internet child safety materials used by ICAC task forces in school and community settings: NIJ evaluation final report. Retrieved from ncjrs.gov/pdffiles1/nij/grants/242016.pdf

Jones, L. M., Mitchell, K. J., & Walsh, W. A. (2014a). A Content Analysis of Youth Internet Safety Programs: Are Effective Prevention Strategies Being Used? Durham, NH: Crimes Against Children Research Center (CCRC), University of New Hampshire. Retrieved from scholars.unh.edu/cgi/viewcontent.cgi?article=1040&context=ccrc

Jones, L. M., Mitchell, K. J., & Walsh, W. A. (2014b). A Systematic Review of Effective Youth Prevention Education: Implications for Internet Safety Education. Durham, NH: Crimes Against Children Research Center (CCRC), University of New Hampshire. Retrieved from scholars.unh.edu/cgi/viewcontent.cgi?article=1041&context=ccrc

Katz, I., Keeley, M., Spears, B., Tadedeo, C., Swirski, T., & Bates, S. (2014). Research on youth exposure to, and management of, cyberbullying incidents in Australia: Synthesis report (SPRC Report 16/2014). Retrieved from Sydney: communications.gov.au/file/1413/download?token=V2qQoHRG

Kiriakidis, P., & Kavoura, P. (2010). Cyberbullying: A Review of the Literature on Harassment Through the Internet and Other Electronic Means. Family & Community Health, 33(2), 82–93. doi: 10.1097/FCH.0b013e3181d593e4

Kowalski, R. M., Limber, S. P., & McCord, A. (2019). A developmental approach to cyberbullying: Prevalence and protective factors. Aggression and Violent Behavior, 45, 20-32. doi: 10.1016/j.avb.2018.02.009

Krieger, M. A. (2017). Unpacking 'sexting': A systematic review of nonconsensual sexting in legal, educational, and psychological literatures. Trauma, Violence, and Abuse, 18(5), 593-601. doi: 10.1177/1524838016659486

Lambe, L. J., Cioppa, V. D., Hong, I. K., & Craig, W. M. (2019). Standing up to bullying: A social ecological review of peer defending in offline and online contexts. Aggression and Violent Behavior, 45, 51-74. doi: 10.1016/j.avb.2018.05.007

Langford, R., Bonell, C. P., Jones, H. E., Pouliou, T., Murphy, S. M., Waters, E., ... Campbell, R. (2014). The WHO Health Promoting School framework for improving the health and well-being of students and their academic achievement (Review). Cochrane Database of Systematic Reviews, 2014(4). doi: 10.1002/14651858.CD008958.pub2

Lemaigre, C., Taylor, E. P., & Gittoes, C. (2017). Barriers and facilitators to disclosing sexual abuse in childhood and adolescence: A systematic review. Child Abuse & Neglect, 70, 39-52. doi: 10.1016/j.chiabu.2017.05.009

Letourneau, E. J., Schaeffer, C. M., Bradshaw, C. P., & Feder, K. A. (2017). Preventing the onset of child sexual abuse by targeting young adolescents with universal prevention programming. Child Maltreatment, 22(2), 100-111. doi: 10.1177/1077559517692439

Lewis, R. (2018). Literature review on children and young people demonstrating technology-assisted harmful sexual behavior. Aggression and Violent Behavior, 40, 1-11. doi: 10.1016/j.avb.2018.02.011

Livingstone, S., Davidson, J., Bryce, J., Batool, S., Haughton, C., & Nandi, A. (2017). Children's online activities, risks and safety: A literature review by the UKCCIS Evidence Group. Retrieved from assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/759005/Literature_Review_Final_October_2017.pdf

Livingstone, S., Lemish, D., Lim, S. S., Bulger, M., Cabello, P., Claro, M., ... Wei, B. (2017). Global perspectives on children's digital opportunities: An emerging research and policy agenda. Pediatrics, 140, S132-S141. doi:10.1542/peds.2016-1758S

Madigan, S., Villani, V., Azzopardi, C., Laut, D., Smith, T., Temple, J. R., Browne, D., & Dimitropoulos, G. (2018). The prevalence of unwanted online sexual exposure and solicitation among youth: A meta-analysis. Journal of Adolescent Health, 63(2), 133-141. doi: https://doi.org/10.1016/j.jadohealth.2018.03.012

Marczak, M., & Coyne, I. (2010). Cyberbullying at school: Good practice and legal aspects in the United Kingdom. 20(2), 182-193.

Meeus, W., Van Ouytsel, J., & Driesen, A. (2014). Media Literacy in the Digital Age: How to benefit from media use while protecting against harm — An overview of competencies needed by learners, teachers and teacher educators using 'Media Didactica'. Journal of Didactics, 5(1/2), 64-79.

Menesini, E., & Salmivalli, C. (2017). Bullying in schools: the state of knowledge and effective interventions. 22(sup1), 240-253.

Ministry for Women, & Netsafe. (2017). Insights into digital harm: The online lives of New Zealand Girls and Boys. Retrieved from netsafe.org.nz/wp-content/uploads/2017/11/Insights-Into-Digital-Harm-Ministry-for-Women-Netsafe_R3_v6b-Web.pdf

Nation, M., Crusto, C., Wandersman, A., Kumpfer, K. L., Seybolt, D., Morrissey-Kane, E., & Davino, K. (2003). What works in prevention: Principles of effective prevention programs. American

Psychologist, 58(6/7), 449-456. doi: 10.1037/0003-066X.58.6-7.449

Nawaila, M., Kanbul, S., & Ozdamli, F. (2018). A review on the rights of children in the digital age. Children and Youth Services Review, 94, 390–409. doi: 10.1016/j.childyouth.2018.09.028

Netsafe. (2017). Young People and Sexting – A Comparative Report. Retrieved from netsafe.org.nz/young-people-sexting-report

Netsafe. (2018). Parenting and Pornography Report. Retrieved from netsafe.org.nz/parents-and-sexually-explicit-content-2018

Netsafe. (2018). Parenting and Pornography NZ, UK and AUS Report. Retrieved from netsafe.org.nz/parents-and-sexually-explicit-content_three-country-comparison-2018/

Netsafe. (2018). Youth Accessing Support Factsheet. Retrieved from netsafe.org.nz/youth-accessing-support-factsheet-2018/

Netsafe New Zealand. (2018). Children's exposure to sexually explicit content: Parents' awareness, attitudes and actions. Retrieved from netsafe.org.nz/wp-content/uploads/2018/12/Parents-and-Pornography-2018_10Dec2018.pdf

Netsafe New Zealand. (2018). New Zealand teens' digital profile: A factsheet. Retrieved from netsafe.org.nz/wp-content/uploads/2018/02/NZ-teens-digital-profile_factsheet_Feb-2018-1.pdf

Netsafe New Zealand. (2019). Digital self-harm: Prevalence, motivations and outcomes for teens who cyberbully themselves. Retrieved from netsafe.org.nz/wp-content/uploads/2019/05/Digital-self-harm-report-2019.pdf

Netsafe New Zealand (2019). The DIY Guide for Developing User Agreements. Retrieved from netsafe.org.nz/the-kit/wp-content/uploads/2018/06/Netsafe-Kit-Student-User-Agreement-DIY-Guide.pdf

New South Wales Department of Education, Centre for Education Statistics and Evaluation. (2017). Anti-bullying interventions in schools – what works? Retrieved from cese.nsw.gov.au//images/stories/PDF/anti_bullying_in_schools_what_works_AA.pdf

New South Wales Government. (2018). Review into the non-educational use of mobile devices in NSW schools. Retrieved from. education.nsw.gov.au/about-us/strategies-and-reports/our-reports-and-reviews/mobile-devices-in-schools/review-into-the-non-educational-use-of-mobile-devices-in-nsw-schools

New South Wales Government Department of Education (2019). Digital Citizenship. Retrieved from digitalcitizenship.nsw.edu.au

New South Wales Parliamentary Research Service. (2016). E-brief: Cyberbullying of children. Retrieved from parliament.nsw.gov.au/researchpapers/Documents/cyberbullying-of-children/Cyberbullying%20of%20Children.pdf

Northern Territory Government. (2016). Charter of Rights for Children in Care in the Northern Territory. Retrieved from territoryfamilies.nt.gov.au/publications-and-policies/charter-of-rights

O'Neill, B., & Dinh, T. (2018). The Better Internet for Kids Policy Map: Implementing the European

Strategy for a Better Internet for Children in European Member States. Retrieved from betterinternetforkids.eu/documents/167024/2637346/BIK+Map+report+-+Final+-+March+2018/a858ae53-971f-4dce-829c-5a02af9287f7

Office of the Children's eSafety Commissioner. (2016). Digital Participation Survey: Research Insights - Young and Social Online, Research Insights - Connected Kids and Teens, Research Insights - Teens, Kids and Digital Dangers. Retrieved from esafety.gov.au/about-us/research/digital-participation/young-social-online and esafety.gov.au/about-the-office/research-library (scroll down to Research: Digital Participation)

eSafety Commissioner. (2019). Parenting in the digital age. Retrieved from esafety.gov.au/about-us/research/parenting-digital-age

eSafety Commissioner. (2016). Social Cohesion Research Project (Qualitative Research Report) (unpublished internal report)

eSafety Commissioner. (2017). Social Cohesion Research Project (Quantitative Findings Research Report) (unpublished internal report)

eSafety Commissioner. (2017). eSafety checklist for schools. Retrieved from http://www.esafety.gov.au/about-the-office/resource-centre/esafety-checklist-for-schools-and-parent-communication-strategy

eSafety Commissioner. (2018). State of Play – Youth and Online Gaming in Australia. Retrieved from eSafety website: esafety.gov.au/sites/default/files/2019-07/Youth-and-online-gaming-report-2018.pdf

eSafety Commissioner. (2018). State of Play – Youth, Kids and Digital Dangers. Retrieved from eSafety website: esafety.gov.au/sites/default/files/2019-10/State%20of%20Play%20-%20Youth%20kids%20and%20digital%20dangers.pdf

eSafety Commissioner. (2019). Digital Citizenship. Retrieved from esafety.gov.au/media/2563

eSafety Commissioner. (2019). Start the chat and stay safe online: A guide to help parents, carers and educators protect kids online. Retrieved from esafety.gov.au

eSafety Commissioner. (2019). The YeS Project. Retrieved from esafety.gov.au/education-resources/classroom-resources/yes-project

eSafety Commissioner. (2019). Young and eSafe. Retrieved from esafety.gov.au/youngandesafe

eSafety Commissioner. (2019). Your Online Journey: Find out how to get online and be safe. Trainer's guide. Retrieved from esafety.gov.au/key-issues/tailored-advice/aboriginal-and-torres-strait-islander-peoples/your-online-journey

eSafety Commissioner, Netsafe New Zealand, UK Safer Internet Centre, & Plymouth University. (2018). Parenting and pornography: findings from Australia, New Zealand and the United Kingdom Summary report. Retrieved from netsafe.org.nz/wp-content/uploads/2018/12/summary-report-parenting-and-pornography.pdf

eSafety Commissioner, Netsafe New Zealand, UK Safer Internet Centre, & University of Plymouth.

(2018). Parenting and pornography: findings from Australia, New Zealand and the United Kingdom: summary report. Retrieved from esafety.gov.au/about-the-office/research-library/parenting-and-pornography

eSafety Commissioner, Netsafe New Zealand, SWGfl/UK Safer Internet Centre, & University of Plymouth. (2017). Young People and Sexting – attitudes and behaviours: Research findings from the United Kingdom, New Zealand and Australia. Retrieved from esafety.gov.au/sites/default/files/2019-07/Young%20people%20and%20sexting-netsafe-UK%20Safer%20Internet%20Centre-Plymoth%20University-eSafety%20Commissioner.pdf

Optus. (2018). Digital Thumbprint Evaluation Report: Creating a safer online environment for young Australians. Retrieved from digitalthumbprint.com.au/wp-content/uploads/2018/02/Digital-Thumbprint-Evaluation-Report-Feb_2018.pdf

Ospina, M., Harstall, C., & Dennett, L. (2010). Sexual exploitation of children and youth over the internet: A rapid review of the scientific literature.

Pearce, N., Cross, D., Monks, H., Waters, S., Erceg, E., & Falconer, S. (2011). Current Evidence of Best Practice in Whole-School Bullying Intervention and Its Potential to Inform Cyberbullying Interventions. Australian Journal of Guidance and Counselling, 21(1), 1-21.

Pepler, D., Craig, W. M., Cummings, J., Petrunka, K., & Garwood, S. (2017). Mobilizing Canada to Promote Healthy Relationships and Prevent Bullying Among Children and Youth. In P. Sturmey (Ed.), The Wiley Handbook of Violence and Aggression: John Wiley and Sons. doi: 10.1002/9781119057574.whbva123

Perren, S., Corcoran, L., Cowie, H., Dehue, F., Garcia, D., Mc Guckin, C., ... Völlink, T. (2012). Tackling cyberbullying: Review of empirical evidence regarding successful responses by students, parents, and schools. International Journal of Conflict and Violence, 6(2), 283–292. doi: 10.4119/UNIBI/ijcv.244

Pope, J., Colin, P., Third, A., Ogus, N., & Campbell, J. (2015). eSmart Schools Evaluation Report. Retrieved from communications.gov.au/sites/default/files/submissions/alannah_and_madeline_foundation_appendix_a.pdf

Prevnet. (2019). What Teens Can Do: Stop and think - before you send and regret. Retrieved from prevnet.ca/bullying/cyber-bullying/teens

PSHE Association. (2016). Key principles of effective prevention education. Retrieved from pshe-association.org.uk/curriculum-and-resources/resources/key-principles-effective-prevention-education

Qing, L. (2015). When cyberbullying and bullying meet gaming: A systemic review of the literature. Journal of Psychology and Psychotherapy, 5(4), 1. Doi: 10.4172/2161-0487.1000195

Queensland Anti Cyberbullying Taskforce. (2018). Adjust our settings: A community approach to address cyberbullying among children and young people in Queensland. Retrieved from campaigns.premiers.qld.gov.au/antibullying/taskforce/assets/anti-cyberbullying-taskforce-final-report.pdf

Radford, L., Allnock, D., & Hynes, P. (2015). Preventing and responding to child sexual abuse and exploitation: Evidence review. Retrieved from researchgate.net/profile/Patricia_Hynes/publication/330093929_Preventing_and_Responding_to_Child_Sexual_Abuse_and_Exploitation_Evidence_review/links/5c2d1e2ba6fdccfc7078f917/Preventing-and-Responding-to-Child-Sexual-Abuse-and-Exploitation-Evidence-review.pdf

Ribble, M. (2017). Nine Elements. Retrieved from digitalcitizenship.net/nine-elements.html

Rideout, M. A., & Robb, M. B. (2018). Social media, social life: Teens reveal their experiences in 2018. Retrieved from commonsensemedia.org/sites/default/files/uploads/research/2018_cs_socialmediasociallife_fullreport-final-release_2_lowres.pdf

Romano, J. L. (2014). Prevention in the Twenty-First Century: Promoting Health and Well-Being in Education and Psychology. Asia Pacific Education Review, 15(3), 417-426. doi: 10.1007/s12564-014-9327-8

Savina, E., Mills, J. L., Atwood, K., & Cha, J. (2017). Digital media and youth: A primer for school psychologists. Contemporary School Psychology, 21(1), 80-91. doi: 10.1007/s40688-017-0119-0

Scottish Government. (2017). National Action Plan on Internet Safety for Children and Young People. Retrieved from gov.scot/binaries/content/documents/govscot/publications/strategy-plan/2017/04/national-action-plan-internet-safety-children-young-people/documents/00516921-pdf/00516921-pdf/govscot%3Adocument/00516921.pdf

The Senate Environment and Communications References Committee. (2016). Harm being done to Australian children through access to pornography on the Internet: Report. Retrieved from aph.gov.au/Parliamentary_Business/Committees/Senate/Environment_and_Communications/Onlineaccesstoporn45/Report

The Senate Legal and Constitutional Affairs References Committee. (2018). Adequacy of existing offences in the Commonwealth Criminal Code and of state and territory criminal laws to capture cyberbullying report. Retrieved from aph.gov.au/Parliamentary_Business/Committees/Senate/Legal_and_Constitutional_Affairs/Cyberbullying/Report

Shetgiri, R. (2013). Bullying and victimization among children. Advances in Pediatrics, 60(1), 33-51. doi: 10.1016/j.yapd.2013.04.004

Sivaraman, B., Nye, E., & Bowes, L. (2019). School-based anti-bullying interventions for adolescents in low- and middle-income countries: A systematic review. Aggression and Violent Behavior, 45, 154-162. doi: 10.1016/j.avb.2018.07.007

Slonje, R., Smith, P., & Frisén, A. (2013). The nature of cyberbullying, and strategies for prevention. Computers in Human Behavior, 29(1), 26–32. doi: 10.1016/j.chb.2012.05.024

South West Grid for Learning (SWGfL). (2018a). School Online Safety Policy Templates. Retrieved from swgfl.org.uk/assets/documents/online-safety-policy-templates-without-appendicies.pdf

SWGfL. (2018b). UK Schools Online Safety Policy and Practice Assessment. Retrieved from

swgfl.org.uk/assets/documents/uk-schools-online-safety-policy-and-practice-assessment-2018.pdf?_=1553703046

SWGfL. (2018c). 360DegreeSafe. The Free Online Safety Self-Review Tool for Schools. Retrieved from 360safe.org.uk

SWGfL. (2018d). 360safe: The online safety self-review tool. School online safety self-review tool. Retrieved from 360safe.org.uk/Overview/PDF-Version

SWGfL/UK Safer Internet Centre, University of Plymouth United Kingdom, Netsafe New Zealand, & eSafety Commissioner Australia. (2017). Young People and Sexting - Attitudes and Behaviours. Retrieved from esafety.gov.au/sites/default/files/2019-07/Young%20people%20and%20sexting-netsafe-UK%20Safer%20Internet%20Centre-Plymoth%20University-eSafety%20Commissioner.pdf

The State of Queensland, Department of Education and Training. (2016). Bullying. No Way! STEPS Decision-making framework. Retrieved from bullyingnoway.gov.au/PreventingBullying/STEPS/Documents/steps-framework.pdf

State of Victoria. (2016). Royal Commission into Family Violence: Volume VI Report and Recommendations. Retrieved from rcfv.com.au/MediaLibraries/RCFamilyViolence/Reports/Final/RCFV-Vol-VI.pdf

Stonard, K. E., Bowen, E., Lawrence, T. R., & Price, S. A. (2014). The relevance of technology to the nature, prevalence and impact of Adolescent Dating Violence and Abuse: A research synthesis. Aggression and Violent Behavior, 19(4), 390-417. doi: doi.org/10.1016/j.avb.2014.06.005

Tanrikulu, I. (2018). Cyberbullying prevention and intervention programs in schools: A systematic review. School Psychology International, 39(1), 74-91. doi: 10.1177/0143034317745721

Telethon Kids Institute, Supré, & Headspace. (n.d.). BULLYING. SO NOT OK: A girls' education and prevention booklet. Retrieved from bullyingnoway.gov.au/Resources/TeachingResources/Documents/A-Girls-Education-and-Prevention-Booklet.pdf

ThinkUKnow. (n.d.). SOS guide to cyber security. Retrieved from thinkuknow.org.au/resources/guides/sos-guide-cyber-security

ThinkUKnow. (n.d.). ThinkUKnow classroom promo pack. Retrieved from thinkuknow.org.au/index.php/resources/multimedia/thinkuknow-classroom-promo-pack

Third, A., Bellerose, D., Dawkins, U., Keltie, E., & Pihl, K. (2014). Children's rights in the digital age: A download from children around the world. Retrieved from aeema.net/WordPress/wp-content/uploads/2014/10/Childrens-Rights-in-the-Digital-Age.pdf

Third, A., Bellerose, D., De Oliveira, J. D., Lala, G., & Theakstone, G. (2017). Young and Online: Children's perspectives on life in the digital age: The State of the World's Children 2017 Companion Report. Retrieved from unicef.org/publications/files/Young_and_Online_Children_perspectives_Dec_2017.pdf

Throuvala, M. A., Griffiths, M. D., Rennoldson, M., & Kuss, D. J. (2019). School-based prevention for adolescent Internet addiction: Prevention is the key. A systematic literature review. Current

Neuropharmacology, 17(6), 507–525. doi: 10.2174/1570159X16666180813153806

Torres, F. C., & Vivas, G. M. (2016). Cyberbullying and education: A review of emergent issues in Latin America research. In Cyberbullying Across the Globe: Gender, Family, and Mental Health (pp. 131–147). Springer International Publishing. doi: 10.1007/978-3-319-25552-1_7

Ttofi, M., & Farrington, D. (2011). Effectiveness of school-based programs to reduce bullying: a systematic and meta-analytic review. Journal of Experimental Criminology, 7(1), 27–56. doi.org/10.1007/s11292-010-9109-1

UK Council for Child Internet Safety. (2015). Child Safety Online: A Practical Guide for Providers of Social Media and Interactive Services. Retrieved from assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/487973/ukccis_guide-final__3_.pdf

UK Council for Child Internet Safety. (2015). UKCCIS Education Working Group: Online Safety in Education Report. Retrieved from assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/517217/Online_Safety_in_Education_December_2015__2_.pdf

UK Council for Child Internet Safety. (2016). Online Safety in Schools and Colleges: Questions from the Governing Board. Retrieved from gov.uk/government/publications/online-safety-in-schools-and-colleges-questions-from-the-governing-board

UK Council for Child Internet Safety. (2017). Tackling race and faith targeted bullying face to face and online: A short guide for schools. Retrieved from assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/759004/Tackling_race_and_faith_targeted_bullying_face_to_face_and_online_-_a_guide.pdf

UK Council for Child Internet Safety. (2018). Education for a Connected World: A framework to equip children and young people for digital life. Retrieved from assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/759003/Education_for_a_connected_world_PDF.PDF

UK Council for Child Internet Safety (2018). Using External Visitors to Support Online Safety Education: Guidance for Educational Settings. Retrieved from assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/759006/Using_External_Visitors_to_Support_Online_Safety__July_2018.pdf

UK Council for Child Internet Safety. (2019). Safeguarding Children and Protecting Professionals in Early Years Settings: Online Safety Considerations for Managers. Retrieved from assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/776470/UKCIS_Early_Years_Online_Safety_Considerations_for_Managers.pdf

UK Council for Child Internet Safety. (2019). Safeguarding Children and Protecting Professionals in Early Years Settings: Online Safety Considerations for practitioners. Retrieved from gov.uk/government/publications/safeguarding-children-and-protecting-professionals-in-early-years-settings-online-safety-considerations/safeguarding-children-and-protecting-professionals-in-early-years-settings-online-safety-guidance-for-practitioners

UK Council for Child Internet Safety. (n.d.). Sexting: Responding to incidents and safeguarding learners: Guidance for educational settings in Wales. Retrieved from thinkuknow.co.uk/globalassets/welsh-sexting-guidance--english-version.pdf

UNESCO Bangkok. (2015). Fostering Digital Citizenship through Safe and Responsible Use of ICT: A review of current status in Asia and the Pacific as of December 2014. Bangkok: UNESCO Bangkok. Retrieved from http://teams.unesco.org/ORG/fu/bangkok/public_events/Shared%20Documents/EISD/2017/Oct2017%20-%20KFIT%203%20Launch%20-%20Dig%20Citizenship/SRU-ICT_mapping_report_2014.pdf

UNESCO Bangkok. (2019). Digital Kids Asia-Pacific: Insights into Children's Digital Citizenship. Retrieved from bangkok.unesco.org/content/digital-kids-asia-pacific-insights-childrens-digital-citizenship

US iKeepSafe Coalition. (2015). Privacy Curriculum Matrix K-12 BEaPRO. Retrieved from ikeepsafe.org/wp-ikeepsafe.org/wp-content/uploads/2017/08/2017iKeepSafe-Privacy-Curriculum-Matrix-K-12-BEaPRO.pdf

Van Noorden, T., Haselager, G. J., Cillessen, A. H., & Bukowski, W. M. (2015). Empathy and Involvement in Bullying in Children and Adolescents: A Systematic Review. Journal of Youth and Adolescence, 44(3), 637–657. doi: 10.1007/s10964-014-0135-6

Vega, V., & Robb, M. (2019). The Common Sense Census: Inside the 21st century classroom. Retrieved from commonsensemedia.org/sites/default/files/uploads/research/2019-educator-census-inside-the-21st-century-classroom_1.pdf

Victorian Law Reform Commission. (2013). Inquiry into Sexting. Report of the Law Reform Committee for the Inquiry into Sexting. Retrieved from parliament.vic.gov.au/file_uploads/LRC_Sexting_Final_Report_0c0rvqP5.pdf

Vondrackova, P., & Gabrhelik, R. (2016). Prevention of Internet addiction: A systematic review. Journal of Behavioral Addictions, *5*(4), 568–579. doi: 10.1556/2006.5.2016.085

Voulgaridou, I., & Kokkinos, C. M. (2015). Relational aggression in adolescents: A review of theoretical and empirical research. Aggression and Violent Behavior, 23, 87-97. doi: 10.1016/j.avb.2015.05.006

Walker, K., & Sleath, E. (2017). A systematic review of the current knowledge regarding revenge pornography and non-consensual sharing of sexually explicit media. Aggression and Violent Behavior, 36, 9-24. doi: 10.1016/j.avb.2017.06.010

Walsh, K., Zwi, K., Woolfenden, S., & Shlonsky, A. (2015). School-based education programmes for the prevention of child sexual abuse. Cochrane Database of Systematic Reviews, 36(4), 1-124. doi: 10.1002/14651858.CD004380.pub3

We PROTECT Global Alliance (2016). Preventing and Tackling Child Sexual Exploitation and Abuse (CESA): A Model National Response. Retrieved from static1.squarespace.com/static/5630f48de4b00a75476ecf0a/t/582ba50bc534a51764e8a4ec/1549388168335/WeP

Welsh Government (2018). Digital Competence Framework Guidance. Retrieved from

hwb.gov.wales/storage/337437b8-cfe3-4305-ae32-f47ad82f3e76/digital-competence-framework-guidance-2018.pdf

Wingate, V. S., Minney, J. A., & Guadagno, R. (2013). Sticks and stones may break your bones, but words will always hurt you: A review of cyberbullying. Social Influence, 8(2-3), 87-106. doi: 10.1080/15534510.2012.730491

World Health Organisation. (2016). INSPIRE: Seven strategies for ending violence against children. Retrieved from who.int/violence_injury_prevention/violence/inspire/en/

Wurtele, S. K. (2017). Preventing cyber sexual solicitation of adolescents. In R. Alexander (Ed.), Research and Practices in Child Maltreatment Prevention (Ed.) Vol 1 of 2 (pp.361-393). Retrieved from researchgate.net/profile/Sandy_Wurtele/publication/318726379_Preventing_cyber_sexual_solicitation_of_adolescents/links/597a48fd0f7e9b0469b33c0a/Preventing-cyber-sexual-solicitation-of-adolescents.pdf

Wurtele, S. K., & Miller-Perrin, C. (2017). What Works to Prevent the Sexual Exploitation of Children and Youth. In L. Dixon, D. F. Perkins, C. Hamilton-Giachritsis, & L. A. Craig (Eds.), The Wiley Handbook of What Works in Child Maltreatment (pp. 176-197). doi:10.1002/9781118976111.ch12

Zych, I., Baldry, A. C., Farrington, D. P., & Llorent, V. J. (2019). Are children involved in cyberbullying low on empathy? A systematic review and meta-analysis of research on empathy versus different cyberbullying roles. Aggression and Violent Behavior, 45, 83-97. doi: doi.org/10.1016/j.avb.2018.03.004

Zych, I., Farrington, D. P., & Ttofi, M. M. (2019). Protective factors against bullying and cyberbullying: A systematic review of meta-analyses. Aggression and Violent Behavior, 45, 4-19. doi: doi.org/10.1016/j.avb.2018.06.008

Additional references

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. Qualitative Research in Psychology, 3(2), 77–101. doi: 10.1191/1478088706qp063oa

Collaborative for Academic, Social, and Emotional Learning. (2019). What is SEL? Retrieved from casel.org/what-is-sel

Durlak, J. A., Weissberg, R. P., Dymnicki, A. B., Taylor, R. D., & Schellinger, K. B. (2011). The impact of enhancing students' social and emotional learning: A meta-analysis of school-based universal interventions. Child development, 82(1), 405-432.

Ganann, R., Ciliska, D., & Thomas, H. (2010). Expediting systematic reviews: methods and implications of rapid reviews. Implementation Science, 5: 56. doi: 10.1186/1748-5908-5-56

Lundberg, A., & Dangel, R. F. (2018). Using root cause analysis and occupational safety research to prevent child sexual abuse in schools. Journal of Child Sexual Abuse, 28(2), 187-199. doi: 10.1080/10538712.2018.1494238

Preuss, P. G. (2003). School leader's guide to root cause analysis: using data to dissolve problems. Larchmont, NY: Eye on Education. doi: 10.4324/9781315854960

Puddy, R. W. & Wilkins, N. (2011). Understanding Evidence Part 1: Best Available Research Evidence. A Guide to the Continuum of Evidence of Effectiveness. Atlanta, GA: Centers for Disease Control and Prevention. Retrieved from cdc.gov/violenceprevention/pdf/understanding_evidence-a.pdf

UNICEF. (1990). A simplified version of the United Nations Convention on the Rights of the Child. Retrieved from unicef.org.au/Upload/UNICEF/Media/Our%20work/childfriendlycrc.pdf

Appendix 1: internet searches

Multiple internet searches were undertaken using combinations of the predefined search terms listed below.

Synonyms for online contexts	**Synonyms for target children**
Online	Child
Digital	Children
Internet	Childhood
Media	Adolescent
Mobile	Adolescence
Technology	Teen
Tech	Teenager
Web	Young people
Cyber	Young person
Social network	Youth
	Student
	Pupil
	School
	Class
Synonyms for risks, harms, dangers	**Synonyms for framework**
Safety	Framework
Risk	Model
Harm	Guideline
Danger	Standard
Abuse	Tool
Maltreatment	
Violence	
Threat	

Synonyms for specific risks, harms, dangers	**Synonyms for positive prevention**
Bullying/cyberbullying Cyberbullying Online child exploitation Online grooming Sexting Sexploitation Stalking Exposure to pornography online Online solicitation Unwanted contact Digital reputation Radicalisation Profiling Privacy Datafication The internet of things Fake news/reliability of information	Safety Management Security Education Support Critical literacy/digital literacy/media literacy Digital citizenship Digital leadership **Synonyms for program** Program(me) Project Activity Resource Initiative Policy

Appendix 2: academic database searches

Databases searched

1. ERIC
2. Education Source
3. Digital Education Research Network (DERN)
4. ScienceDirect
5. Campbell Library
6. Cochrane Library
7. EPPI-Centre (UK)
8. PROSPERO (for protocols)
9. Google Scholar (limit to hits on first five pages)

Search terms used

Search strategies included variations on those listed below.

(online or digital or web or internet or cyber*) AND (safety or harm or risk or danger) AND (child* or adolesc* or teen* or youth or student* or school*) AND (systematic or meta analysis or review)
(online OR digital OR internet OR media OR mobile OR tech* OR web OR cyber OR 'social network') AND (risk OR harm OR danger OR abuse OR violence OR threat) AND (bullying OR cyberbullying OR grooming OR sexting OR exploitation OR stalking) AND (child* OR adolesc* OR school OR Student* OR Young) AND (framework OR model OR Guideline OR Standard OR Tool) AND (safe* OR Manage* OR secur* OR educat* OR support) AND (program* OR project OR activity OR initiative OR policy OR publication)
(prevent* or reduc* or educat* or promot* or implement* or increas* or decreas* or facilitat* or barrier* or encourag* or discourag*) AND (school* or class* or pupil* or student*) AND (guideline* or guidance or policy or policies or recommendation* or tool*

or standard* or ‘best practice*’ or framework* or ‘good practice*’ or ‘effective practice*’) AND (online or digital or web or internet or cyber*)

Additional searches focused on specific risks including:

Cyberbullying

Online child exploitation

Online grooming

Sexting

Sexual exploitation

Stalking

Pornography online

Online solicitation

Unwanted contact

Digital reputation

Radicalisation

Profiling

Privacy

Appendix 3: screening inclusion criteria

Internet searches: inclusion criteria

Prompt question	Response
Is it written in English?	Yes/No/Unclear
Is it child-focused or relevant to children?	Yes/No/Unclear
Is it relevant to online safety education or schools?	Yes/No/Unclear
Does it include information/recommendations/a framework/a model/a list of guidelines/standards/tools/checklists that can be extracted into statements for the best practice framework?	Yes/No/Unclear
Was it developed on the basis of evidence (i.e. is the development process traceable)?	Yes/No/Unclear

Database searches: inclusion criteria

Prompt question	Response
Is it written in English?	Yes/No/Maybe
Is it child-focused or relevant to children?	Yes/No/Maybe
Is it relevant to online safety education or schools?	Yes/No/Maybe
Does it include information/recommendations that can be extracted into statements for the best practice framework?	Yes/No/Maybe