Keeping children safe online: A literature review

Background and context

Children and young people born in the last two to three decades are part of a highly digitised and connected world. Despite the advantages this connectivity brings, there are also risks and threats which put children and young people in harm's way. This review of the literature shows that while there is extensive research on cyber-bullying, online sexual exploitation of children and online abuse, there is little information about the long-term impacts of existing cyber-safety programs and approaches.

Purpose

The purpose of this literature review is to better understand how children and young people engage with the digital world. It highlights best available research on key online trends, emerging issues and their implications for children and young people. It explores the potential benefits and risks of their digitised interactions and current approaches to enable users to manage their safety online. It draws on literature that emphasises the need to consider children's views and experiences when designing programs and software/applications for them or drafting policies that govern their digital use. There is also emerging evidence on the value of adopting a systems approach towards cyber safety for a multi-dimensional view of the subject. This paper provides a background for researchers, practitioners, and policy makers conducting research, or developing programs, online courses and policies that take a systems approach to the issue.

The first section of the review provides a background on cyber-safety, including terminology, statistics and key trends of the cyber world. The second section explores its features, risks and protective factors. The third section presents emerging research on strategies and key features of effective cyber-safety programs. The fourth section highlights emerging international and national policy approaches on cyber-safety and discusses gaps where more work is required. The final section concludes the review and makes key recommendations.

Method

This paper draws on a mixture of academic journal articles, published reports, research studies and news articles. In reviewing the literature, we used Google search engines and Google Scholar to search for the following terms: cyber safety, online safety, online abuse, child sexual online abuse, cyberthreats, children and young people, child rights, cyberbullying, image-based abuse, program evaluations, best practices, COVID-19, and pandemics. Other keywords were digital citizenship, digital footprint, digital resilience and problematic use of internet.

The paper draws on 150 documents published since 2014, with detailed analyses of 36 documents.[1]

Terminology

Cyber-safety is generally defined as a holistic approach for safe and responsible engagement with online information and communication technologies. Other terms used are online safety, internet safety, e-safety, and digital safety. Cyber-safety addresses a broad range of issues such as fraud, privacy breaches, identity theft, unwanted exposure to violent or sexualised content, phishing and email scams, addiction to internet and devices, cyberbullying, online etiquette or netiquette, hacking, unsafe online gaming activities and image-based abuse. [2] Appendix 1 lists some of the common terms, including terminology used in this review.

[1] Only two literature reviews were found between 2014 and 2020 – one in 2015, an Australian study, and another in 2017 from the UK.

[2] Third, A., Forrest-Lawrence, P., & Collier, A. (2014). Addressing the Cyber Safety Challenge: from risk to resilience

cfecfw.asn.au
@CFECFW
03 9614 1577
Level 5/50 Market Street, Melbourne, 3000

Cyber world – key trends

Increased use of and access to cyber technologies

The cyber world is characterised by digital/virtual interactions via computer networks.[3] It is more than the devices and the technology of the internet – it is a space where online media is created, shared, and consumed. It has undergone a significant transformation in the last few decades with the advent of smart devices and increased access to the internet.

Global statistics

2020: About 4.57 billion people or 59 percent of global population were active internet users[4]

2020: 3 billion plus smartphone users[5]

2019: Consumers downloaded around 204 billion mobile apps to their connected devices, reflecting a substantial increase from 140.7 billion app downloads in 2016.[6]

Australian statistics

2017: 88% households in major cities were likely to have internet access while 77% had access in remote parts of the country.[7]

2019: Rise in smartphones from 76% to 91% within six years, with 78% of Australian consumers owning or having access to connected home devices such as smart TVs, gaming consoles, Voice-assisted speakers, set- top boxes, smart appliances, and others.[8]

2019: About 17. 1 million Australians above the age of 14 years used Facebook, 15.3 million used YouTube, 8 million Instagram and 7.3 million Pinterest.[9]

Trends in internet and device usage

One of the key trends today is the use of numerous applications for gaming, video-making, photo-editing, music, anonymous chatting, ride-hailing, sports, fitness, banking, payment wallet, online shopping, educational material, and others.

Another cyber trend is the rise of cloud computing. The Australian Bureau of Statistics (ABS) reported that in 2018, the proportion of businesses using paid cloud computing continued to grow, with 42% of businesses using cloud computing compared to 31% in 2015-16.[10]

Other trends include a broad uptake of location-based services through GPS-enabled mobile devices and an increase in use of web-based platforms. The sophisticated location and positioning services and devices combine 'real world data with virtual data'.[11] Navigation services allow people to track each other's locations, find amenities (including transport options) and even locate lost devices.

Increased use of web-based platforms and new technology can be seen in education, health, and government services. This reduces pressures on face-to-face services such as Centrelink and enables creation of large

[3] Plan Australia (2014). Working Together with Children and Young People for Safety in the Cyber World. Specific references have been provided where necessary.

[4] April 2020, https://www.statista.com/statistics/617136/digital-population-worldwide/

[5] February 2020, https://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide/

[6] January 2020, https://www.statista.com/statistics/271644/worldwide-free-and-paid-mobile-app-store-downloads/

[7] https://www.abs.gov.au/ausstats/abs@.nsf/mf/8146.0

[8] Deloitte. (2019). Mobile Consumer Survey: The Australian Cut.

[9] http://www.roymorgan.com/findings/7979-social-media-trends-march-2019-201905170731

[10] https://www.abs.gov.au/ausstats/abs@.nsf/mf/8167.0?OpenDocument

[11] Third, A., Forrest-Lawrence, P., & Collier, A. (2014). *Addressing the Cyber Safety Challenge: from risk to resilience*. Pg. 10

cfecfw.asn.au
@CFECFW
03 9614 1577
Level 5/50 Market Street, Melbourne, 3000

databases which makes inter-agency data sharing a possibility.[12]

Another emerging trend with the advent of large datasets is the rise of Internet of Things (IoT), machine learning, and artificial intelligence or deep learning. Artificial neural networks are machine learning algorithms which are trained to code patterns and make predictions based on available data.[13] For instance, Facebook algorithms can predict consumer behaviour and feature pages based on users' interests.[14]

Cross-generational usage

The cross-generational use of high-speed internet and smart/connected devices is one of the more significant trends observed around the world and in Australia.[15] Users ranging from 2 years to over 65 years are now active participants in the cyber world. They are engaging on multiple social media platforms to see, create and share content.

Children and young people are engaging more with the cyber world and using new technologies.[16] Children as young as two years can swipe through content on touchscreen devices, watch videos on YouTube by the time they are four years and use Voice-activated devices to find an answer from Google by the time they are six years.[17] A new report on a multi-country research study about children's online engagement estimates that 'one in three children globally is already an internet user and, furthermore, that one in three internet users is a child (under 18 years of age)'.[18] The report also suggests that 'youth aged 15–24 years lead on internet access and use in every region of the world'.[19]

Impact of COVID-19 on internet usage

Since the outbreak of COVID-19 and the lockdown environment in many countries globally, engagement with the cyber world has increased dramatically. A consumer survey in March 2020 of around 13,000 people in 13 countries found that 95% of consumers were spending more time on in-home media consumption/activities than prior to COVID-19. Seventy per cent reported spending more time on their smartphones than previously.[20] The survey also highlights that 80% of young people (age group 16-25 years) reported extended use of smartphones. In locations where social distancing and school closures have been implemented, remote learning has increased online activities in all age-groups.[21]

The next section of the review examines key features of cyber-use, its inherent risks, and the benefits of engaging with it and the protective barriers that can reduce or minimise the harms caused to children and young people.

[12] Third, A., Forrest-Lawrence, P., & Collier, A. (2014). *Addressing the Cyber Safety Challenge: from risk to resilience*. Pg. 10

[13] See for example: Kietzmann, J., Lee, L. W., McCarthy, I. P., & Kietzmann, T. C. (2020). Deepfakes: Trick or treat?. *Business Horizons*, *63*(2), 135-146.; Hussain, M., Zhu, W., Zhang, W., Abidi, S. M. R., & Ali, S. (2019). Using machine learning to predict student difficulties from learning session data. *Artificial Intelligence Review*, 52(1), 381-407.

[14] Kachamas, P., Akkaradamrongrat, S., Sinthupinyo, S., & Chandrachai, A. (2019). Application of Artificial Intelligent in the Prediction of Consumer Behavior from Facebook Posts Analysis. *International Journal of Machine Learning and Computing*, 9(1), 91-97.

[15] Third, A., Forrest-Lawrence, P., & Collier, A. (2014). Addressing the Cyber Safety Challenge: from risk to resilience. Pg. 8

[16] United Nations Children's Fund, The State of the World's Children 2017: Children in a Digital World, UNICEF, New York, December 2017.

[17] Danovitch, J. H. (2019). Growing up with Google: How children's understanding and use of internet-based devices relates to cognitive development. *Human Behavior and Emerging Technologies*, 1(2), 81-90.

[18] Global Kids Online (2019). Global Kids Online: Comparative Report, UNICEF Office of Research – Innocenti. Florence. Pg. 8

[19] Ibid.

[20] GWI (2020) a. Coronavirus Research, April 2020, Multi-market research. The 2020 report states that GenZ say they expect to continue using devices at high numbers even after the lockdowns ease.

[21] GWI (2020) b. Coronavirus Research, March 2020, Multi-market research; and Data Trends

cfecfw.asn.au
@CFECFW
03 9614 1577
Level 5/50 Market Street, Melbourne, 3000

Managing online safety of children and young people

Cyber world – features and opportunities

The cyber world enables increased digital connectedness and faster long-distance communications. The availability of high-speed internet has made virtual networking (official or personal), distance learning, and recreational activities easier. Cloud-computing and data-sharing have also enabled online collaborations between agencies working towards common goals, such as combatting crime, developing health initiatives, and others. Mobile phones and the internet are increasingly seen as tools to enhance people's safety.[22]

Cyber-world content is also permanent in nature as information that is shared online is there forever.[23] By posting content on personal views, and interests, people leave their personal digital footprints. This information remains publicly available, despite privacy protocols. Such information is also accessible to anyone, at any time and from any location. People from different ages, backgrounds and abilities can see, create, and share any content.[24] With the right amount of filtering and safety precautions, this opens phenomenal opportunities for learning, capacity development, advocacy and increased digital skills.[25] The cyber world also enables anonymity to users who want to protect their identity.[26] Figure 1 below broadly classifies the various features of the cyber world.

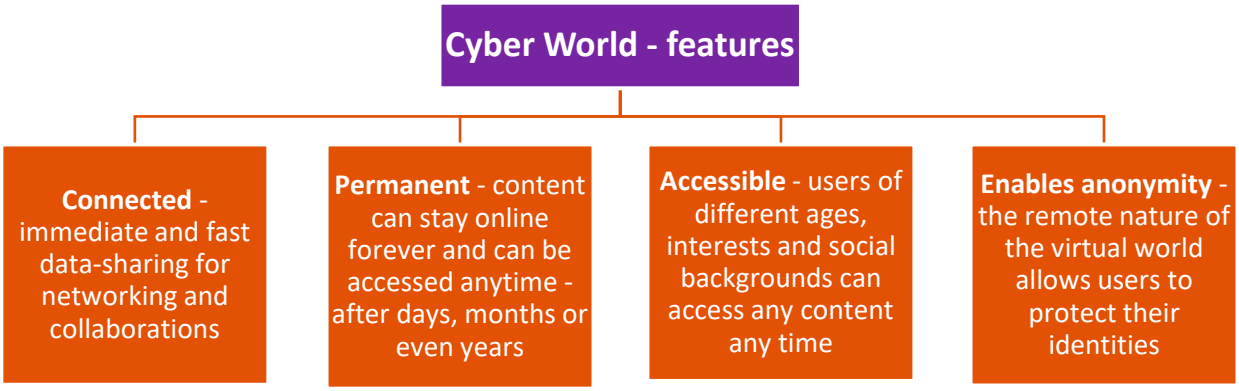

Figure 1: Features of the Cyber World

These features create many opportunities, especially for young learners. Sophisticated search engines and learning applications open up a world of knowledge for children of different age groups. It can enable them to overcome different kinds of disadvantages related to their location and abilities. Social media platforms can also amplify voices of children and adolescents who seek solutions to problems affecting them and their communities.[27] The power of social media and the ability to harness it is well demonstrated by the school strike where 1.6 million students from over 120 countries joined Greta Thunberg for climate action.[28]

[22] Plan Australia (2014). Working Together with Children and Young People for Safety in the Cyber World. Specific references have been provided where necessary. Pg. 9

[23] See for example: https://cyberbullying.org/it-is-time-to-teach-safe-sexting; 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.

[24] Third, A., Forrest-Lawrence, P., & Collier, A. (2014). Addressing the Cyber Safety Challenge: from risk to resilience.

[25] Plan Australia (2014). Working Together with Children and Young People for Safety in the Cyber World. Specific references have been provided where necessary.; and Global Kids Online (2019). Global Kids Online: Comparative Report, UNICEF Office of Research – Innocenti. Florence.

[26] Brighi, A., Menin, D., Skrzypiec, G., & Guarini, A. (2019). Young, bullying, and connected. Common pathways to cyberbullying and problematic internet use in adolescence. *Frontiers in psychology*.

[27] United Nations Children's Fund, The State of the World's Children 2017: Children in a Digital World, UNICEF, New York, December 2017.

[28] Jung, J., Petkanic, P., Nan, D., & Kim, J. H. (2020). When a girl awakened the world: A user and social message analysis of greta thunberg. *Sustainability*, 12(7), 2707.

cfecfw.asn.au
@CFECFW
03 9614 1577
Level 5/50 Market Street, Melbourne, 3000

Cyber world – risks and impact

Risks of online activities

There are several risks associated with engaging in online activities, such as hacking, online abuse, identity theft and others. Limited knowledge about threats or inability to take safety measures increases the risks when online activities increase. Our current digital dependency has heightened the vulnerability to cyberattacks for health and community service organisations, welfare claim systems and databases with personal information in different countries.[29] Similarly, there has been a marked rise in online child abuse: for example, the National Center for Missing and Exploited Children (NCMEC) in the United States, which receives complaints from technology companies on child exploitation, reports that their CyberTipline[30] has received 4.2 million global reports in April, up 2 million from March 2020.[31] In countries such as the US, United Kingdom, Spain, Australia, Denmark, and the Philippines, online child abuse content and attempts to access them have reportedly doubled or tripled since the coronavirus pandemic and resultant global lockdowns.[32]

Impact of risks on children and young people

The very features of the cyber world that make it beneficial for children and young people also pose several risks as well. As online activities increase, so does potential exposure to online risks.[33] For instance, offensive or inappropriate content gets shared and becomes instantaneously viral through large-scale dissemination. Such content can be accessed by anyone, irrespective of their age or background.[34] The anonymity feature can also give cyberbullies or sexual predators power and advantage over their victims as it reduces their risk of identification and prosecution.[35] Within seconds, bullies can attack someone personally; make offensive comments to online posts when they like, i.e., in days, weeks or even months, and share a victim's personal information or content (without consent) with anyone anywhere.[36] User data and digital footprints can also be used to profile and stalk children and young people.[37]

A 2020 survey across thirty-four countries to understand the impact of new technologies on children shows that the majority of the countries ranked bullying and harassment highest in impact, while in-app purchases were ranked lowest.[38] Studies have also documented how certain groups are more vulnerable than others to online risks. This group includes young children (2-10 years): 'girls, children from poor households, children in communities with a limited understanding of different forms of sexual abuse and exploitation of children, children who are out of school, children with disabilities, children who suffer depression or mental health

[29] See for example: https://www.businessinsider.com.au/top-un-official-warned-of-cybercrime-spike-during-pandemic-2020-5; https://www.cyber.gov.au/threats/threat-update-covid-19-malicious-cyber-activity; and https://home.kpmg/au/en/home/insights/2020/05/covid-19-cyber-security-impact-on-retail.html

[30] NCMEC's CyberTipline is a centralised reporting system for the online exploitation of children. The public and electronic service providers can make reports of suspected online enticement of children for sexual acts, extra-familial child sexual molestation, child pornography, child sex tourism, child sex trafficking, unsolicited obscene materials sent to a child, misleading domain names, and misleading words or digital images on the internet. https://www.missingkids.org/gethelpnow/cybertipline#bythenumbers

[31] https://www.forbes.com/sites/thomasbrewster/2020/05/09/online-child-abuse-complaints-surpass-4-million-in-april-this-is-how-cops-are-coping-despite-covid-19/#2a2d24ae48db

[32] See for example: https://www.abc.net.au/news/2020-05-20/afp-concerned-by-child-exploitation-spike-amid-coronavirus/12265544, and https://www.bbc.com/news/world-52773344

[33] Sweeney, T. A., Georg, S. M., & Ben, F. (2019). Home internet use by eight-year-old children. *Australian Educational Computing*, 34(1).

[34] 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*.

[35] United Nations Children's Fund, The State of the World's Children 2017: Children in a Digital World, UNICEF, New York, December 2017. Pg. 70; Brighi, A., Menin, D., Skrzypiec, G., & Guarini, A. (2019). *Young, bullying, and connected. Common pathways to cyberbullying and problematic internet use in adolescence*. Frontiers in psychology.

[36] Schiamberg, L. B., Barboza, G., Chee, G., & Hsieh, M. C. (2018). *The adolescent parent context and positive youth development in the ecology of cyberbullying*. Pg. 6

[37] OECD (2020). Protecting children online: An overview of recent developments in legal frameworks and policies. OECD Digital Economy Papers, No. 295, OECD Publishing, Paris.

[38] Ibid. Pp. 8-9

cfecfw.asn.au
@CFECFW
03 9614 1577
Level 5/50 Market Street, Melbourne, 3000

problems and children from marginalised groups'.[39] This group includes children on the move, those in foster care, and those in juvenile justice systems.[40]

The literature highlights the online risks and opportunities using a child-focused approach as depicted in the table below.[41]

Table 1:Mapping online opportunities and risks, by child role

		Content risk (as a recipient of mass productions)	Contact risk (as a participant in adult-initiated activities)	Conduct risk (as an actor who can be abuser or victim)
OPPORTUNITIES	**Education learning and digital literacy**	Educational resources	Contact with others sharing similar interests	Self-initiated or collaborative learning
	Participation and civic engagement	Global information	Exchange among interest groups	Concrete forms of civic engagement
	Creativity and self-expression	Diversity of resources	Being invited/inspired to create or participate	User-generated content creation
	Identity and social connection	Advice (personal/health/sexual etc.)	Social networking, shared experiences with others	Expression of identity
RISKS	**Aggressive**	Violent/gory content	Harassment, stalking	Bullying, hostile peer to peer activity
	Sexual	Pornographic or harmful sexual content	Online sexual solicitation including grooming or offline meeting with stranger	Sexual harassment, sexting, producing and sharing explicit content without permission
	Values	Misleading, hateful, and racist content, inciting self-harm through drug use, suicide, anorexia and other forms	Ideological persuasion, extremism, indoctrination	Misuse of personal information, defamation
	Commercial	Manipulative advertising, spam, embedded marketing i.e. in-app purchases, scams	Production of child pornography, trafficking, harvesting personal info	Gambling, plagiarism
	Legal	Breach of privacy, data privacy, identity theft, defamation	Purchase of illegal or age-restricted products	Copyright infringements, piracy

[39] United Nations Children's Fund, The State of the World's Children 2017: Children in a Digital World, UNICEF, New York, December 2017. Pg. 81

[40] Ibid. Pg. 85

[41] Table adapted from: Global Kids Online (2019). Global Kids Online: Comparative Report, UNICEF Office of Research – Innocenti. Florence.; Sweeney, T. A., Georg, S. M., & Ben, F. (2019). Home internet use by eight-year-old children. *Australian Educational Computing*, 34(1).; Livingstone, S., Davidson, J., Bryce J., Batool, S., Haughton, C., and Nandi, A. (2017). Children's online activities, risks and safety: A literature review by the UKCCIS evidence group. Technical Report. UKCCIS evidence group.; Livingstone, S. (2016). A framework for researching Global Kids Online: understanding children's well-being and rights in the digital age.; and Plan Australia (2014). Working Together with Children and Young People for Safety in the Cyber World. Specific references have been provided where necessary.

cfecfw.asn.au
@CFECFW
03 9614 1577
Level 5/50 Market Street, Melbourne, 3000

Online risks can be high and can cause irreversible harm to people, particularly to children and young people, which is why it is so important to better understand this world and make sure users are adequately protected. Each online risk can affect children and young people psychologically, socially, and even physically. Cyberbullying, image-based abuse, exposure to inappropriate content or harmful advice – all of these result in negative experiences causing loss of contact with reality, anxiety, depression, emotional distress, suicidal ideation, self-harm, sexual or physical assault and reputational damage.[42]

Cyber world – the ecology of risks and protective factors

Researchers have argued that an ecological framework is important to understand contextual risks, vulnerabilities, and protective factors. The wider context, where notions of race, ethnicity, gender, class, and religion influence social behaviour, also dictate online behaviour. Thus, children and young people face risks and enjoy protective barriers at multiple levels due to the complex interactions at individual, family, peers, and community levels.[43] Offenders and bullies operate in a society where gender stereotypes, inequalities, coercion, victim-blaming, blurred boundaries between sexting and harassment, and a lack of understanding of consent are normal.[44] Some studies argue that abuse occurring from harmful digital behaviour is a manifestation of gender-based violence.[45] This is because even though technology-facilitated abuse is not gender-specific, there is substantial data to show that girls are more at risk.[46]

These research reflections are confirmed by a 2017 Australian survey on experiences of image-based abuse which highlights that young people, women, people with disability or people from LGBTIQ, culturally and linguistically diverse (CALD) and Aboriginal and Torres Strait Islander communities experience higher percentage of risks.[47] There is also evidence that children or young people who have witnessed family violence, or have experienced child maltreatment and suffer from emotional dysregulation internalise a belief system that normalises violence[48]. As a result, some are more likely to demonstrate behaviour to victimise their peers while others become victims themselves. In such situations, it does not matter if the abuse takes place online or offline.[49]

Low technical skills – such as knowledge about privacy settings, filtering mechanisms, how to monitor security or recognise fake news – among children, young people, parents, and educators can increase the vulnerability of exposure to different kinds of risk.[50]

Protective factors for children and young people

Protective factors follow a similar trajectory where individual, family, peer and community interactions can help protect against online threats. Based on the evidence, these factors can be broadly classified into four

[42] See for example: Office of the eSafety Commissioner, Australia. (2018). State of play—Youth, kids, and digital dangers.; Livingstone, S., Davidson, J., Bryce J., Batool, S., Haughton, C., and Nandi, A. (2017). Children's online activities, risks and safety: A literature review by the UKCCIS evidence group. Technical Report. UKCCIS evidence group.; Schiamberg, L. B., Barboza, G., Chee, G., & Hsieh, M. C. (2018). *The adolescent parent context and positive youth development in the ecology of cyberbullying*

[43] Brighi, A., Menin, D., Skrzypiec, G., & Guarini, A. (2019). Young, bullying, and connected. Common pathways to cyberbullying and problematic internet use in adolescence. *Frontiers in psychology*.

[44] Livingstone, S., Davidson, J., Bryce J., Batool, S., Haughton, C., and Nandi, A. (2017). Children's online activities, risks and safety: a literature review by the UKCCIS evidence group. Technical Report. UKCCIS evidence group.

[45] Henry, N., & Powell, A. (2015). Beyond the 'sext': Technology-facilitated sexual violence and harassment against adult women. *Australian & New Zealand Journal of Criminology*, 48(1), 104-118.

[46] Green, A., Wilkins, C., & Wyld, G. (2019). Keeping Children Safe Online. Think. UK. Pg. 17.; Livingstone, S., Davidson, J., Bryce J., Batool, S., Haughton, C., and Nandi, A. (2017). Children's online activities, risks and safety: A literature review by the UKCCIS evidence group. Technical Report. UKCCIS evidence group. Pg. 3;

[47] Henry, N., Powell, A., & Flynn, A. L. G. (2017). Not Just 'Revenge Pornography': Australians' Experiences of Image-Based Abuse: A Summary Report. RMIT University.

[48] Schiamberg, L. B., Barboza, G., Chee, G., & Hsieh, M. C. (2018). *The adolescent parent context and positive youth development in the ecology of cyberbullying.* Pp. 13-14.

[49] Ibid.

[50] See for example: Sweeney, T. A., Georg, S. M., & Ben, F. (2019). Home internet use by eight-year-old children. *Australian Educational Computing*, 34(1).; Livingstone, S., Davidson, J., Bryce J., Batool, S., Haughton, C., and Nandi, A. (2017). Children's online activities, risks and safety: a literature review by the UKCCIS evidence group. Technical Report. UKCCIS evidence group.

cfecfw.asn.au
@CFECFW
03 9614 1577
Level 5/50 Market Street, Melbourne, 3000

domains:

- Increased individual capabilities by enabling children to recognise their agency,[51] and supporting their social and emotional competencies can assist with critical thinking, high self-esteem and empathy.[52]
- Increased technical capabilities of children, parents, caregivers, and educators to understand the risks can help establish well-informed filters and security measures.[53]
- Positive two-way relational communication with peers and adults, and a healthy school climate where positive peer status, academic performance, and support can act as barriers to online abuse.[54]
- Age-appropriate mediation strategies for actively monitoring and supervising technology use can act as protective factors.[55]

The literature identifies four types of mediation strategies:

- Enabling/active social (direct and indirect conversations to discuss and evaluate risks and benefits)
- Enabling technical (monitoring digital media and physical movement through surveillance and checking of online activities)
- Restrictive social (conditional, time-based or activity-based)
- Restrictive technical (filtering software, restricting access to some content).[56]

To reduce harm and maximise the benefits of online engagement, a combination of these strategies is recommended.

The 2019 Global Kids Online study cites a multi-level framework to understand the diverse influences in children's lives at different levels, which are governed by their skills to engage and which shape their identity in the online world. This study is based on 18 countries where more than 14,000 internet-using children were surveyed and interviewed about their online experiences. The Global Kids Online network works with multiple partners around the world to consider policy options and suggest practical solutions based on the data it generates.[57] This framework puts the child at the centre and assesses the interplay of factors across individual, social and country level. Figure 2 below shows the multi-level framework to understand the interconnecting influences on children's lives.

[51] Global Kids Online (2019). Global Kids Online: Comparative Report, UNICEF Office of Research – Innocenti. Florence.; Livingstone, S. (2016). A framework for researching Global Kids Online: understanding children's well-being and rights in the digital age.

[52] Green, A., Wilkins, C., & Wyld, G. (2019). *Keeping Children Safe Online*. Think. UK; 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.

[53] Schiamberg, L. B., Barboza, G., Chee, G., & Hsieh, M. C. (2018). *The adolescent parent context and positive youth development in the ecology of cyberbullying*. Pp. 19.

[54] Green, A., Wilkins, C., & Wyld, G. (2019). *Keeping Children Safe Online*. Think. UK; 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.

[55] Sweeney, T. A., Georg, S. M., & Ben, F. (2019). Home internet use by eight-year-old children. *Australian Educational Computing*, 34(1).

[56] Ibid.

[57] Global Kids Online (2019). Global Kids Online: Comparative Report, UNICEF Office of Research – Innocenti. Florence. Pp. 9-10

cfecfw.asn.au
@CFECFW
03 9614 1577
Level 5/50 Market Street, Melbourne, 3000

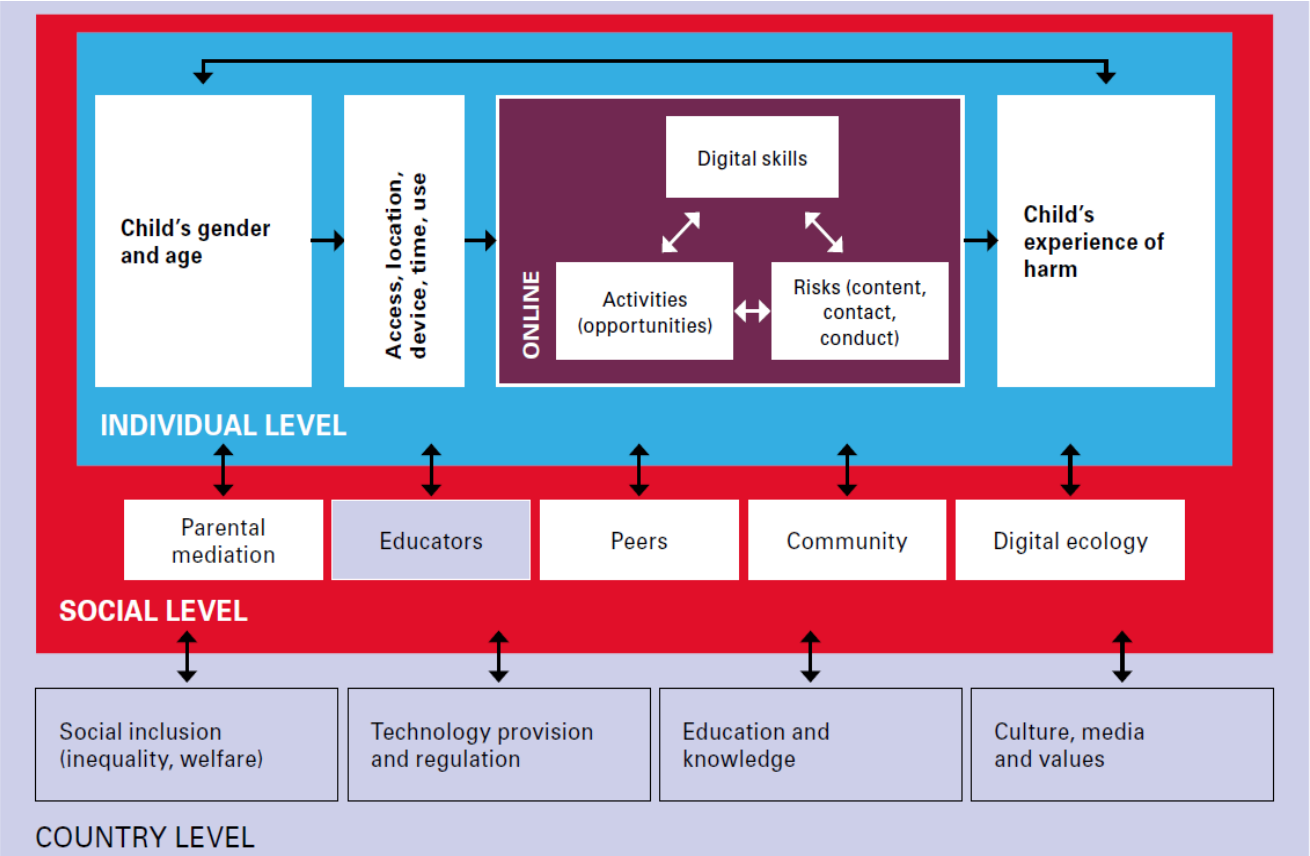

Image 1: Individual and social influences on child rights and well-being; Source - Global Kids Online report 2019

The next section of the review focuses on the emerging strategies to develop a holistic cyber-safety model that recommends a system response and a child rights approach.

cfecfw.asn.au
@CFECFW
03 9614 1577
Level 5/50 Market Street, Melbourne, 3000

Cyber-safety strategies – what works?

Rise of a multidimensional approach to cyber safety

Given that the cyber world is a permanent feature of children's lives today, and that there are associated risks and benefits with this exposure to technology, how do we know what makes cyber safety strategies effective? As mentioned earlier, there is a lack of literature examining effective approaches to children and online safety.

Most of the cyber safety literature has been dominated by studies on cyberbullying and online sexual exploitation of children rather than on what works, and on immediate rather than long term outcomes.[58] The needs of children have not been a priority in the literature.[59]

In response to these challenges, a different approach to cyber safety has emerged which seeks to understand the reasons that make children and young people vulnerable to risks and to develop strategies accordingly. This new body of research on cyber safety has moved away from a fear-driven discourse to a well-informed, multi-dimensional discourse where the interplay between online and offline worlds is being documented and investigated. Emerging research is also documenting children and young people's skills, perspectives, and vocabulary about the cyber world. Such an approach is strengths-based, recognises and respects children's agency, and advocates for digital literacy of all stakeholders to help them navigate through the cyber world.

Child rights and strengths-based approach: Earlier literature on cyber practices and digital citizenship framed children and young people in a limited, moralistic, and risk-dominated approach. More recent studies advocate the use of a child-rights approach, where children and young people have the right to access accurate and age-appropriate knowledge about the online world with equitable access to safe reporting pathways and legal processes. This approach is strengths-based[60] (building on existing child and youth cultures, skills, and capabilities) and maximises the benefits of online engagement and limiting harm.[61]

Promoting critical thinking in young minds: Another approach to cyber safety for children and young people draws on Vygotsky's theory of everyday concepts to advocate for an incremental approach to building children's knowledge about the online world, starting from when they are young (as early as two years old).[62] According to this approach, parenting and teaching approaches should merge everyday concepts with scientific concepts. For instance, as young children are taught about the concept of stranger-danger in the real world, they need to be informed about the consequences of clicking pop-ups or in-app messages or requests in the online world. The studies highlight the importance of understanding how children perceive the internet and how their views are being shaped through their everyday online interactions. Age-appropriate exploratory discussions about how online information is 'socially constructed and distributed, and how it can be globally accessed' between children and adults has been found to be an effective cyber safety strategy.[63]

Data from the 2019 Global Kids Online study shows that as children grow up, they climb the ladder of online participation, as seen in this image below.[64] Children start by enjoying videos, playing games, learning for school homework, and move on to civic participation, increasing their operational knowledge as they climb.

[58] 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. Pg. 20

[59] Livingstone, S., Davidson, J., Bryce J., Batool, S., Haughton, C., and Nandi, A. (2017). Children's online activities, risks and safety: A literature review by the UKCCIS evidence group. Technical Report. UKCCIS evidence group. Pg. 8

[60] Spears, B., Taddeo, C., Collin, P., Swist, T., Razzell, M., Borbone, V., & Drennan, J. (2016). Safe and Well Online: Learnings from Four Social Marketing Campaigns for Youth Wellbeing. ; and Swist, T., Collin, P., McCormack, J., & Third, A. (2015). Social Media and the Wellbeing of Children and Young People: A Literature Review

[61] United Nations Children's Fund, The State of the World's Children 2017: Children in a Digital World, UNICEF, New York, December 2017.; and Third, A., & Collin, P. (2016). Rethinking (children's and young people's) citizenship through dialogues on digital practice. *Negotiating digital citizenship: Control, contest and culture*, 41-60. Pg. 42;

[62] See for example: Edwards, S., Nolan, A., Henderson, M., Mantilla, A., Plowman, L., & Skouteris, H. (2018). Young children's everyday concepts of the internet: A platform for cyber-safety education in the early years. *British Journal of Educational Technology*, *49*(1), pg. 2; and Third, A., & Collin, P. (2016). Rethinking (children's and young people's) citizenship through dialogues on digital practice. *Negotiating digital citizenship: Control, contest and culture*, 41-60. Pg. 52

[63] Eskelä-Haapanen, S., & Kiili, C. (2019). 'It Goes Around the World'–Children's Understanding of the Internet. *Nordic Journal of Digital Literacy*, 14(03-04), 175-187.

[64] Global Kids Online (2019). Global Kids Online: Summary Report, UNICEF Office of Research – Innocenti. Florence. Pg. 25

cfecfw.asn.au
@CFECFW
03 9614 1577
Level 5/50 Market Street, Melbourne, 3000

Many factors influence how children climb this ladder, and different children will have different levels of participation, meaning that interventions can be designed which serve as building blocks for children's digital literacy at each step.

Image 2 Ladder of participation; Source: Global Kids Online Summary report 2019

Meaningful participation in decision-making: These strategies strategies need to be adopted alongside children's right to meaningfully participate, not only to voice their concerns but also to design their own cyber-safety strategies. One-off participation or limited duration consultations have been found to be less effective than creating systems and opportunities where children and young people have the ability to influence decision-making.[65] Recent studies have documented the importance of moving away from earlier adult-centred concepts to diverse child-centric perspectives.[66]

Systems approach and promoting communicative competence: Research shows that cyber safety approaches should also take a systems point of view, with 'non-linear, webbed interactional relationships between parts and subsystems'.[67] As described in the Global Kids Online multi-level framework, risks or protective factors cannot be seen in isolation but as interacting with each other. Effective cyber safety strategies require a multi-dimensional response with strategies to equip caregivers, teachers, policy makers, and community members

[65] 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. Pg. 21

[66] Global Kids Online (2019). Global Kids Online: Summary Report, UNICEF Office of Research – Innocenti. Florence.; Office of the eSafety Commissioner, Australia. (2018). State of play—Youth, kids, and digital dangers.; and 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.

[67] Alfandari, R. (2019). Approaching the study of cyberbullying towards social workers from a systems perspective. *Aggression and Violent Behavior*.

cfecfw.asn.au
@CFECFW
03 9614 1577
Level 5/50 Market Street, Melbourne, 3000

with resources to talk about the online world. This includes understanding children's motives for engaging online and to provide training on safe reporting.[68]

Contextual and evidence-based: Research on mediation strategies has found that parents from different cultural and linguistic backgrounds adopt different strategies towards online safety.[69] Similarly, online parenting styles and confidence can vary according to education, socio-economic status, cultural background and geographical location.[70] Another Australian survey[71] on children and youth shows that young people from different cultural backgrounds and from special needs groups were more active in their management of social media and often displayed greater self-disclosure of personal information. However, young people from diverse backgrounds were more restrained in revealing their negative experiences to their family members. Such studies show that it is valuable to consider a range of contexts, experiences, barriers, and perspectives while developing evidence-informed programs and policies.

Overall, the literature suggests the following elements are important when developing a cyber-safety program:

1. A child rights perspective, which enables equitable, age-appropriate access and meaningful participation, school and legal policy development, and including children and young people in decision-making
2. Digital resilience, through enhancing the technical skills and critical thinking of all stakeholders
3. Evidence-informed, outcomes-focused and context-specific cyber safety programs
4. Adequate training of teachers, parents, care givers, program delivery consultants and community members about safe internet practices and children and young people's perspectives of the internet
5. A system-response through collaborations between families, school and communities
6. Clear, safe and effective pathways for reporting abuse
7. Consistent approaches and ongoing support for the different stakeholders
8. Appropriate program content, which should be easy, age- and culturally-appropriate, and focus on respect, and feelings
9. Range of delivery modes, including cyber safety campaigns, interactive videos, role plays, games, posters, offline and online media
10. In-built data collection strategies to monitor and evaluate the short-term and long-term outcomes of programs.

National and international approaches to address cyber safety

Using strategies to build resilience are not sufficient on their own to build digital literacy in children and young people and other stakeholders. These also need to be supported by policies and legal frameworks. 'Internet governance' has expanded from technical infrastructure to the domains of cybersecurity, human rights, and e-commerce and sits across multiple entities such as governments, private sector and civil society. This section explores some of the multi-stakeholder initiatives that have been implemented, emerging practices and approaches to cyber safety.

The literature documents a rise in collaborative practices in research, program development, legislative policies and even cybercrime fighting. A recent OECD study surveyed 34 countries about their legal and policy responses regarding online safety for children. The study shows how governments are caught between balancing the complexities of managing the digital world and minimising harm while supporting greater use of technology. The study shows the different approaches adopted by countries in responding to such a challenging environment. Some countries have extended existing frameworks to respond to new risks, while

[68] González-Alonso, F., Guillén-Gámez, F. D., & de Castro-Hernández, R. M. (2020). Methodological Analysis of the Effect of an Anti-Bullying Programme in Secondary Education through Communicative Competence: A Pre-Test—Post-Test Study with a Control-Experimental Group. *International journal of environmental research and public health*, 17(9), 3047.; and Green, A., Wilkins, C., & Wyld, G. (2019). Keeping Children Safe Online. Think. UK. Pg. 24

[69] Family Online Safety Institute (FOSI). (2014). Parenting in the Digital Age: How Parents Weigh the Potential Benefits and Harms of Their Children's Technology Use

[70] Office of eSafety Commissioner (Australia). (2019). Parenting in the Digital Age.

[71] Office of the eSafety Commissioner, Australia. (2018). State of play—Youth, kids, and digital dangers

cfecfw.asn.au
@CFECFW
03 9614 1577
Level 5/50 Market Street, Melbourne, 3000

others have developed national digital policies to protect all their citizens.[72] When it comes to online protection of children, some countries have taken a more targeted approach:

Developing a single oversight body: In the recent years, countries such as Australia, Costa Rica, Israel, Italy, Japan and New Zealand have developed a statutory body that guides digital policies, has a special focus on children's protection, monitors content, trains/supports multiple stakeholders, provides information and raises awareness in the community.

Dedicated multi-stakeholder bodies: Some countries have established multi-stakeholder bodies where everyone has shared responsibilities towards children's online safety. These bodies include local civic organisations including parenting groups and educators, policy makers, law enforcement, researchers, business, and international technical experts. The United Kingdom's Council for Internet Safety (UKCIS) works solely on children issues and is recognised by the UK government. While not a statutory body, it advocates, conducts internet safety research, creates good practice guides, and has pioneered several positive initiatives.[73]

Creating industry codes of conduct: Some countries have responded to the changes in technology and have developed or improved their codes of conducts to regulate social media platforms that operate across borders. For instance, in Mexico, the UK and US, legislation prohibits publicity or marketing strategies that could mislead vulnerable members, including children. Some legislation also prohibits collection of personal data of children under 13 years (as in the US).[74]

Prioritising digital and media literacy of children and parents/educators: Countries such as UK and Australia have developed dedicated online portals which share carefully curated information to promote critical thinking and safer internet practices among children and young people. Media literacy campaigns such as the Safer Internet Day, which is celebrated across 150 countries, are beneficial in promoting safe practices and sharing information. Recent mass media campaigns such as 'Keep it real online' by the New Zealand Government, have been designed to educate children and help them develop online safety skills.[75] Such campaigns also aim to educate and inform adults about privacy and filtering possibilities. There are also projects[76] which use animated storytelling as a technique to discuss age appropriate information about online behaviour.[77]

International and regional cooperation: Intergovernmental organisations such as the Asia-Pacific Economic Cooperation (APEC), Council of Europe (COE), European Union, Internet Governance Forum, International Telecommunication Union (ITU), Organisation for Economic Co-operation and Development (OECD), and UNICEF Innocenti Research Centre have each adopted a targeted approach and developed frameworks to promote digital literacy and make the internet a safe and positive platform for children. Multi-country projects such as the Global Kids Online study, the EU Kids Online Network and UNICEF are working towards filling gaps in comprehensive global research.[78]

The 2020 OECD survey on policy and legal responses highlighted some of the gaps countries need to address:[79]

Need to take a systems response: Government responses are still siloed whereas the online risks go beyond

[72] OECD (2020). Protecting children online: An overview of recent developments in legal frameworks and policies. OECD Digital Economy Papers, No. 295, OECD Publishing, Paris. Pg. 11

[73] Ibid. Pg. 42-43

[74] Ibid. Pg. 30

[75] Keep it real online – series of ads on online bullying, pornography, online grooming and reporting harmful or illegal content - https://www.keepitrealonline.govt.nz/

[76] Some examples are - "Owce w Sieci" (Sheep on the web) video series which is available in multiple European languages; the Be Deadly Online resource which offers lesson plans, videos and posters created by and for Aboriginal and Torres Strait Islander peoples; and videos by UK's Child Exploitation and Online Protection command (CEOP) and Thinkyouknow UK[76] and US-based iKeepSafe Faux paw the techno Cat series and Be Internet Awesome.

[77] Tomczyk, Ł., & Kopecký, K. (2016). Children and youth safety on the Internet: Experiences from Czech Republic and Poland. Telematics and Informatics, 33(3), 822-833.

[78] OECD (2020). Protecting children online: An overview of recent developments in legal frameworks and policies. OECD Digital Economy Papers, No. 295, OECD Publishing, Paris. Pp. 48-49

[79] Ibid. Pg. 6

cfecfw.asn.au
@CFECFW
03 9614 1577
Level 5/50 Market Street, Melbourne, 3000

traditional legislations. For instance, issues caused by sexting and cyberbullying are relevant to justice, health, education and child protection and require cross-departmental rather than siloed responses, with complementary policy actions and programs.

Lack of monitoring and implementation: Despite the presence of laws and legislations, countries do not always monitor and implement these, particularly with regard to contact and commercial risks.

Measuring and monitoring effectiveness of policies: There is a lack of consistency in approaches, definitions, methods and indicators. Except for countries such as Japan and Sweden where policies on digital literacy for children are analysed and critically evaluated,[80] most countries demonstrated an evidence gap in systematic measuring of risks or effectiveness of programs.

Towards a child rights approach in policy and legislation – progress and gaps

Taking a children's rights perspective in relation to cyber safety is a relatively recent approach. A 2016 study argued that recognition of children as a substantial group of internet users was barely recognised in the internet governance space and called for a child rights approach to be embedded into activities, policies and structures.[81] Since then there has been a drive among international research communities to remedy this by undertaking projects such as the Global Kids Online study to document the perspectives of children and inform internet governance. UNICEF is leading another 14-country research study, Disrupting Harm, in partnership with ECPAT International and INTERPOL, which aims to generate high-quality evidence on technology-facilitated abuse of children.[82]

However, while analysing the policy responses in this space, the OECD report confirms that countries still take the protection approach, which tends to diminish the rights of children who are now active digital content users and creators. The protection approach also impedes on the 'right to participate in matters that affect them, right to provision of information, and right to a freedom of expression'.[83] There is still a dearth of programs where children and young people inform design and implementation of cyber safe approaches.[84]

Australia's approach

According to the 2020 report on Child Online Safety Index, which was developed on the basis of data collected from 145,426 children and adolescents in 30 different countries from 2017-2019, Australia is ranked second after Spain.[85] As seen in Figure 3 below, it ranks the highest in legal framework and privacy management while second in promoting critical thinking.

[80] OECD (2020). Protecting children online: An overview of recent developments in legal frameworks and policies. OECD Digital Economy Papers, No. 295, OECD Publishing, Paris. Pg. 47

[81] Livingstone, S., Carr, J., & Byrne, J. (2016). One in three: Internet governance and children's rights.

[82] https://www.unicef-irc.org/research/disrupting-harm/

[83] OECD (2020). Protecting children online: An overview of recent developments in legal frameworks and policies. OECD Digital Economy Papers, No. 295, OECD Publishing, Paris. Pg. 51

[84] Ibid.

[85] COSI (2020). Child Online Safety Index 2020: Findings and Methodology Report. DQInstitute. Pg. 27

cfecfw.asn.au
@CFECFW
03 9614 1577
Level 5/50 Market Street, Melbourne, 3000

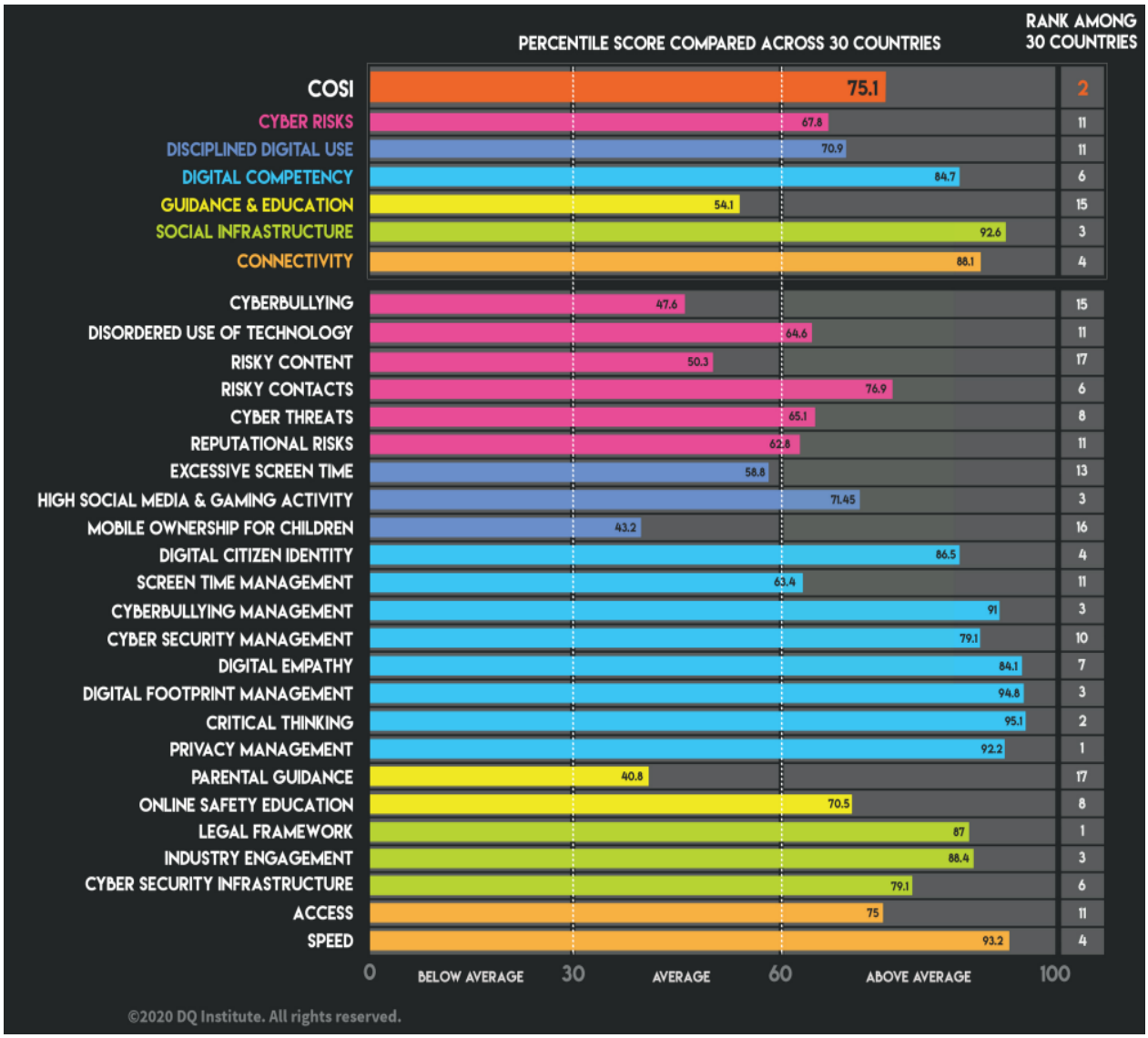

Image 3: Australia's report for the Child Online Safety Index; Source - COSI Report 2020

Australia's work in this space is evident from the work of the Office of eSafety Commissioner, which promotes digital literacy and provides a safe regulatory platform to investigate complaints. It seeks to break siloes by working with various agencies and multi-disciplinary partners to deliver content to children from different age groups and learning/teaching resources for parents, caregivers, and educators.[86] The eSafety Commissioner is also required to review and report on key policy targets set by the Australian Enhancing Online Safety Act every three years. It uses quantitative and qualitative data to 'monitor the effectiveness of content regulation measures'.[87] The Office has developed Safety By Design principles which place the safety and rights of users at the centre of design, development and implementation of online products and services. This was developed on the basis of consultations with industry and trade bodies, parents, carers and young people (aged 14-17).[88]

However, as seen in the COSI ranking image, work still needs to be done in the space of guidance and education and in reducing cyber risks. The Royal Commission into Institutional Responses to Child Sexual

[86] OECD (2020). Protecting children online: An overview of recent developments in legal frameworks and policies. OECD Digital Economy Papers, No. 295, OECD Publishing, Paris. Pg. 16

[87] Ibid. Pg. 45

[88] eSafety (2019). Safety by Design. Office of eSafety Commissioner, Australia.

cfecfw.asn.au
@CFECFW
03 9614 1577
Level 5/50 Market Street, Melbourne, 3000

Abuse called for prioritising online safety education for children, parents and communities in Australia. It also stated that it is 'everybody's business' to intervene early, provide support or report issues when concerns for children's safety online are raised.[89] Effective cyber safety programs require the meaningful participation of children and young people.

Conclusion

It is clear from this review that rapid changes in technology have brought unprecedented risks and opportunities for children and young people. With the right technical and age-appropriate filters and access to accurate information, the cyber world can be a place where young minds can thrive. Research shows that a multidimensional approach to cyber-safety is emerging, which acknowledges the power and potential of the internet and uses a harm minimisation rather than a protection approach. The recent COVID-19 situation has amplified these discussions and demonstrated the need for building digital literacy and digital resilience.

There is also growing interest in knowing more about children's and young people's understanding of the digital environment and their motivations for engaging with the digital world. By documenting children and young people's perspectives globally, studies such as the Global Kids online contribute to this emerging body of knowledge on perspectives. In keeping with the child rights perspective, this new approach respects children's skills and capabilities and supports meaningful participation in decision-making processes.

The literature highlights the importance of building the digital literacy and technical skills of parents, carers, educators, and community members, and of adopting a systems approach that involves policy makers, commercial stakeholders and law enforcement bodies. Finally, the literature reinforces the importance of regular data collection, monitoring, research and continuing to build the evidence base relating to effective cyber safety approaches.

[89] Royal Commission into Institutional Responses to Child Sexual Abuse, Final Report Recommendations - Volume 6, Making institutions child safe recommendations Pg. 15

cfecfw.asn.au
@CFECFW
03 9614 1577
Level 5/50 Market Street, Melbourne, 3000

References:

Brighi, A., Menin, D., Skrzypiec, G., & Guarini, A. (2019). Young, bullying, and connected. Common pathways to cyberbullying and problematic internet use in adolescence. *Frontiers in psychology*

Chaudron, C. (2015). Young children (0-8) and digital technology: A qualitative exploratory study across seven countries. Luxembourg, European Union: Joint Research Centre

COSI (2020). Child Online Safety Index 2020: Findings and Methodology Report. DQInstitute

Danovitch, J. H. (2019). Growing up with Google: How children's understanding and use of internet-based devices relates to cognitive development. *Human Behavior and Emerging Technologies*, 1(2), 81-90.

Deloitte. (2019). Mobile Consumer Survey: The Australian Cut.

Edwards, S., Nolan, A., Henderson, M., Mantilla, A., Plowman, L., & Skouteris, H. (2018). Young children's everyday concepts of the internet: A platform for cyber-safety education in the early years. *British Journal of Educational Technology*, 49(1).

Eskelä-Haapanen, S., & Kiili, C. (2019). 'It Goes Around the World'–Children's Understanding of the Internet. *Nordic Journal of Digital Literacy*, 14(03-04), 175-187.

Family Online Safety Institute (FOSI). (2014). Parenting in the Digital Age: How Parents Weigh the Potential Benefits and Harms of Their Children's Technology Use

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.

Global Kids Online (2019). Global Kids Online: Comparative Report, UNICEF Office of Research – Innocenti. Florence

GWI (2020) a. Coronavirus Research, April 2020, Multi-market research, Global Web Index

GWI (2020) b. Coronavirus Research, March 2020, Multi-market research, Global Web Index

González-Alonso, F., Guillén-Gámez, F. D., & de Castro-Hernández, R. M. (2020). Methodological Analysis of the Effect of an Anti-Bullying Programme in Secondary Education through Communicative Competence: A Pre-Test—Post-Test Study with a Control-Experimental Group. *International journal of environmental research and public health*, 17(9), 3047.

Green, A., Wilkins, C., & Wyld, G. (2019). Keeping Children Safe Online. Think. UK.

Henry, N., & Powell, A. (2015). Beyond the 'sext': Technology-facilitated sexual violence and harassment against adult women. *Australian & New Zealand Journal of Criminology*, 48(1), 104-118.

Henry, N., Powell, A., & Flynn, A. L. G. (2017). Not Just 'Revenge Pornography': Australians' Experiences of Image-Based Abuse: A Summary Report. RMIT University.

Hussain, M., Zhu, W., Zhang, W., Abidi, S. M. R., & Ali, S. (2019). Using machine learning to predict student difficulties from learning session data. *Artificial Intelligence Review*, 52(1), 381-407.

Jung, J., Petkanic, P., Nan, D., & Kim, J. H. (2020). When a girl awakened the world: A user and social message analysis of Greta Thunberg. *Sustainability*, 12(7), 2707.

Kachamas, P., Akkaradamrongrat, S., Sinthupinyo, S., & Chandrachai, A. (2019). Application of Artificial Intelligent in the Prediction of Consumer Behavior from Facebook Posts Analysis. *International Journal of Machine Learning and Computing*, 9(1), 91-97.

Kietzmann, J., Lee, L. W., McCarthy, I. P., & Kietzmann, T. C. (2020). Deepfakes: Trick or treat?. *Business Horizons,* 63(2), 135-146.

Livingstone, S. (2016). A framework for researching Global Kids Online: understanding children's well-being

cfecfw.asn.au
@CFECFW
03 9614 1577
Level 5/50 Market Street, Melbourne, 3000

and rights in the digital age

Livingstone, S., Carr, J., & Byrne, J. (2016). One in three: Internet governance and children's rights.

Livingstone, S., Davidson, J., Bryce J., Batool, S., Haughton, C., and Nandi, A. (2017). Children's online activities, risks and safety: a literature review by the UKCCIS evidence group. Technical Report. UKCCIS evidence group.

Nadal, K. L. (Ed.). (2017). *The SAGE encyclopedia of psychology and gender*. Sage Publications. (accessed via Google Books)

OECD (2020). Protecting children online: An overview of recent developments in legal frameworks and policies. OECD Digital Economy Papers, No. 295, OECD Publishing, Paris.

Office of eSafety Commissioner (Australia). (2019). Parenting in the Digital Age.

Office of the eSafety Commissioner, Australia. (2018). State of play—Youth, kids, and digital dangers

Pencheva, D., Hallett, J., & Rashid, A. (2020). Bringing cyber to school: Integrating cybersecurity into secondary school education. *IEEE Security & Privacy*, 18(2), 68-74.

Plan Australia (2014). Working Together with Children and Young People for Safety in the Cyber World. Specific references have been provided where necessary

Schiamberg, L. B., Barboza, G., Chee, G., & Hsieh, M. C. (2018). *The adolescent parent context and positive youth development in the ecology of cyberbullying*.

Spears, B., Taddeo, C., Collin, P., Swist, T., Razzell, M., Borbone, V., & Drennan, J. (2016). Safe and Well Online: Learnings from Four Social Marketing Campaigns for Youth Wellbeing.

Sweeney, T. A., Georg, S. M., & Ben, F. (2019). Home internet use by eight-year-old children. *Australian Educational Computing*, 34(1).

Swist, T., Collin, P., McCormack, J., & Third, A. (2015). Social Media and the Wellbeing of Children and Young People: A Literature Review

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.

Third, A., Forrest-Lawrence, P., & Collier, A. (2014). Addressing the Cyber Safety Challenge: from risk to resilience

Tomczyk, Ł., & Kopecký, K. (2016). Children and youth safety on the Internet: Experiences from Czech Republic and Poland. *Telematics and Informatics*, 33(3), 822-833.

United Nations Children's Fund, The State of the World's Children 2017: Children in a Digital World, UNICEF, New York, December 2017

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.

Websites:

https://www.statista.com/statistics/617136/digital-population-worldwide/
https://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide/
https://www.statista.com/statistics/271644/worldwide-free-and-paid-mobile-app-store-downloads/
https://www.abs.gov.au/ausstats/abs@.nsf/mf/8146.0
http://www.roymorgan.com/findings/7979-social-media-trends-march-2019-201905170731
https://www.abs.gov.au/ausstats/abs@.nsf/mf/8167.0?OpenDocument "
Data trends: https://blog.globalwebindex.com/trends/coronavirus-international-study/
https://cyberbullying.org/it-is-time-to-teach-safe-sexting

cfecfw.asn.au
@CFECFW
03 9614 1577
Level 5/50 Market Street, Melbourne, 3000

https://www.abc.net.au/news/2020-05-20/afp-concerned-by-child-exploitation-spike-amid-coronavirus/12265544,
https://www.bbc.com/news/world-52773344
https://www.keepitrealonline.govt.nz/
https://www.unicef-irc.org/research/disrupting-harm/
http://pl.sheeplive.eu/en
https://www.esafety.gov.au/educators/classroom-resources/be-deadly-online
https://ikeepsafe.org/resource_type/family-resources/
https://www.youtube.com/user/ceop/videos
https://www.forbes.com/sites/thomasbrewster/2020/05/09/online-child-abuse-complaints-surpass-4-million-in-april-this-is-how-cops-are-coping-despite-covid-19/#2a2d24ae48db
https://www.missingkids.org/gethelpnow/cybertipline#bythenumbers
https://home.kpmg/au/en/home/insights/2020/05/covid-19-cyber-security-impact-on-retail.html
https://www.cyber.gov.au/threats/threat-update-covid-19-malicious-cyber-activity
https://www.businessinsider.com.au/top-un-official-warned-of-cybercrime-spike-during-pandemic-2020-5
https://www.youthpolicy.org/national/Australia_2010_National_Youth_Strategy.pdf
https://www.1800respect.org.au/violence-and-abuse/image-based-abuse/
https://www.esafety.gov.au/about-us/tech-trends-and-challenges/deepfakes-position-statement
https://cyberbullying.org/it-is-time-to-teach-safe-sexting

cfecfw.asn.au
@CFECFW
03 9614 1577
Level 5/50 Market Street, Melbourne, 3000

Appendix 1 – Definitions of key terms[90]

Child/young person: any person below the age of 18, as stipulated by the United Nations (UN) Convention on the Rights of the Child. Based on national[91] and international[92] definitions, a young person is someone within the age group of 15-25.

Internet of Things (IoT): the smart and connected devices, such as smart TVs, speakers, children's toys, security cameras, switches, appliances, and others, which are becoming a growing part of households today. They tend to blur the lines between online and offline activities.[93]

Technology-facilitated abuse[94]: a range of abuses caused by using digital communications such as social media, text messages or emails and smart devices such as mobiles, tablets, etc. Following are the different ways in which technology-facilitated abuse occurs -

- **Image-based abuse**: when someone shares or threatens to share an intimate/sexual image of another person, without consent. This includes a range of activities[95] –
    - Cyber flashing
    - Upskirting – taking an image up a woman's skirt without her knowledge and consent
    - Downblousing – taking an image of a woman's breasts or cleavage without her knowledge and consent
    - Secretly recording intimate videos/consensual sexual activity
    - Filming and or sharing sexual assault images/videos
    - Photoshopping someone's image onto a sexually explicit image
    - Deepfakes[96] – using a form of artificial intelligence called deep learning where algorithms are trained to make fake images and videos
    - Sexting – sending or receiving "sexually explicit or sexually suggestive images (photos or video) usually via mobile devices".[97]

- **Cyberbullying or trolling**: deliberate harmful behaviour carried out by individuals or groups, repeated over a period, using technology to harass or humiliate someone.[98] The intention is to hurt the victim socially, psychologically, or physically. In some cases, anonymous/fake social media accounts are used for this purpose.
- **Email scams or sextortion**: a blackmail email where a victim is threatened with exposing some sexual activity (usually fake/fictional) unless a payment is made.
- **Romance scams (catphishing)**: engineering a scam through fake online accounts/profiles to exploit unsuspecting online users and engage in virtual romantic relationships to play with someone's emotions/establish control on them.
- **GPS tracking/smart home stalking/hidden cameras**: GPS trackers and spyware apps enable an abuser to track the victim's whereabouts.
- **Harmful digital behaviour/cyber-violence**: the use of digital media to commit aggression or inflict abuse or harm on dating partners. It is not a new phenomenon, but a new context of

[90] Unless specified, this section has primarily been adapted from two papers: Third, A., Forrest-Lawrence, P., & Collier, A. (2014). Addressing the Cyber Safety Challenge: from risk to resilience; Plan Australia (2014). Working Together with Children and Young People for Safety in the Cyber World. Specific references have been provided where necessary.

[91] https://www.youthpolicy.org/national/Australia_2010_National_Youth_Strategy.pdf;

[92] Plan Australia (2014). Working Together with Children and Young People for Safety in the Cyber World

[93] https://www.esafety.gov.au/parents/children-under-5/start-talking-online-safety

[94] Henry, N., & Powell, A. (2015). Beyond the 'sext': Technology-facilitated sexual violence and harassment against adult women. *Australian & New Zealand Journal of Criminology*, *48*(1), 104-118.

[95] https://www.1800respect.org.au/violence-and-abuse/image-based-abuse/

[96] https://www.esafety.gov.au/about-us/tech-trends-and-challenges/deepfakes-position-statement

[97] https://cyberbullying.org/it-is-time-to-teach-safe-sexting

[98] Office of the eSafety Commissioner, Australia. (2018). State of play—Youth, kids, and digital dangers.

cfecfw.asn.au
@CFECFW
03 9614 1577
Level 5/50 Market Street, Melbourne, 3000

psychological abuse behaviours in the field of interpersonal violence.[99]

Digital Ecology: the way children use digital devices, platforms and services shape the ways in which they engage with the internet and the wider world.[100]

Digital citizenship: describes as skills and knowledge to regulate screen time, use critical thinking and empathy in online activities, managing security and online privacy, and participate in civic life with roles and responsibilities.

Digital inclusion: ensuring an equitable access to digital technologies, enhanced learnings and active civic participation.

Digital media literacy: technical skills to access, understand, create, and participate in the digital world. It also includes social skills to follow civic norms and ability to make judgements about the quality and the reliability of online information.

Digital resilience: is ability to deal with negative online experiences achieved by using a strength-based approach that builds user knowledge.

Digital footprint: online activities and interactions create a profile of a person. It is often referred to as a user's online reputation. It can be self-created or created by others (intentionally or unintentionally).[101] This information can be accessed permanently unless deliberate action is taken to delete or modify it.

Problematic Internet Use: is an entity of dysfunctional online behaviour related to impulse control disorders.[102]

[99] Nadal, K. L. (Ed.). (2017). *The SAGE encyclopedia of psychology and gender*. Sage Publications. (accessed via Google Books)

[100] Livingstone, S. (2016). A framework for researching Global Kids Online: understanding children's well-being and rights in the digital age.

[101] Pencheva, D., Hallett, J., & Rashid, A. (2020). Bringing cyber to school: Integrating cybersecurity into secondary school education. *IEEE Security & Privacy*, 18(2), 68-74.

[102] Brighi, A., Menin, D., Skrzypiec, G., & Guarini, A. (2019). Young, bullying, and connected. Common pathways to cyberbullying and problematic internet use in adolescence. *Frontiers in psychology*. Pg.2

cfecfw.asn.au
@CFECFW
03 9614 1577
Level 5/50 Market Street, Melbourne, 3000