Centre for Excellence in Child and Family Welfare

Statutory Review of the Online Safety Act 2021

The Centre for Excellence in Child and Family Welfare welcomes the opportunity to provide feedback as part of the independent review of the Online Safety Act 2021 (the Act). The Centre is the peak body for child and family services in Victoria and Tasmania. For over 100 years we have advocated for the rights of children and young people to be heard, to be safe, to access education and to remain connected to family, community, and culture. We represent around 180 community service organisations, students and individuals working across child and family services. Our members work with children and young people with varying degrees of intersecting and complex challenges, making them particularly vulnerable to online harm.

Our response focuses primarily on Part 3 of the Issues paper: Protecting those who have experienced or encountered online harms.

The Act defines online safety for children as *the capacity of Australian children to use social media services and electronic services in a safe manner and includes the protection of Australian children using those services from cyber-bullying material targeted at an Australian child*. However, this barely scratches the surface of the range and types of risks which children and young people can be exposed to in an online environment.

The Australian Childhood Maltreatment Study highlighted five types of harm which Australians have experienced in childhood and the profound impacts of this maltreatment on the mental health of Australians.[1] The study found that 28.5 per cent of Australians (16-over 65) have experienced child sexual abuse, with girls experiencing higher rates than boys (37.3 per cent vs 18.8 per cent). Much of the literature on online safety relates to child sexual abuse in its different online manifestations. In the context of the current debate about how to keep children and young people safe online, the ACMS offers a stark reminder of the long-term costs of failing to act, while other studies show the immediate impacts on children and young people of exposure to a range of harmful behaviours.

Artificial intelligence

Advances in technology, including in generative artificial intelligence, are so rapid that policy and legislative responses become outdated quickly. At the time of writing, a private school in outer Melbourne has reported a series of AI-generated graphic and obscene images of around 50 female students being circulated online. Elsewhere in Australia a group of young people have been accused of terrorism offences characterised by a period of online radicalisation and the use of social media to promote and share acts of violence. A recent research paper in America highlights the emergence of a growing phenomenon called *cyberbullicide*, in which cyberbullying is associated with the suicide of victims.[2] Countless examples appear in mainstream media of children and young people experiencing serious harms from their interactions with the online world.

A 2023 report by the Internet Watch Foundation (IWF) notes the speed of AI development and improvement, with imagery now so lifelike that it is difficult even for trained analysts to identify if material has been artificially generated.[3] The IWF found 20,254 AI-generated images of child sexual abuse posted to a dark web child sexual abuse material site in a one-month period.

Other IWF findings with relevance to considerations about how Australia grapples with the online harms to children include:

- AI technology allows perpetrators to legally download all the images they want and to generate hundreds of child sexual abuse images at the click of a button with little or no risk of detection.

[1] Haslam D, Mathews B, Pacella R, Scott JG, Finkelhor D, Higgins DJ, Meinck F, Erskine HE, Thomas HJ, Lawrence D, Malacova E. (2023). The prevalence and impact of child maltreatment in Australia: Findings from the Australian Child Maltreatment Study: Brief Report. Australian Child Maltreatment Study, Queensland University of Technology.
[2] Schonfeld, A., McNiel, D., Toyoshima, T., & Binder, R. (2024). Cyberbullying and adolescent suicide. *Journal of the American Academy of Psychiatry and the Law*. 52 (2). DOI: https://doi.org/10.29158/JAAPL.220078-22
[3] Internet Watch Foundation. (2023). How AI is being abused to create child sexual abuse imagery. https://www.iwf.org.uk/media/q4zll2ya/iwf-ai-csam-report_public-oct23v1.pdf

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

- Text-to-image technology will only improve and pose more challenges for analysts and law enforcement agencies.
- AI generated child sexual abuse material has increased the potential for the re-victimisation of known child sexual abuse victims in addition to the victimisation of children in the public realm or known to perpetrators.
- AI generated child sexual abuse material is offering new commercial opportunities for perpetrators to profit from child sexual abuse.
- The legal status of the files used for generating AI images of AI child sexual material presents a complex challenge.[4]

Children with vulnerabilities

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/trolling and harassment highest in impact, followed by sexting and cyber grooming with in-app purchases ranked lowest.[5] Radicalisation was ranked sixth of the eleven forms of harm. Studies have documented how certain groups of children 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 limited understanding of different forms of sexual abuse and exploitation of children, children who are disengaged from school, children with disabilities, children who suffer depression or mental health problems and children from marginalised groups, including children on the move, those in foster care, and those in juvenile justice systems.[6]

Children in out of home care are particularly vulnerable as many have grown up in households that cannot provide a safe or nurturing environment, with financial hardship, violence, drug and alcohol abuse, mental illness or disability, and often a lack of stability in out of home care placements. Given their trauma backgrounds, children in care are at greater risk online due to potential concerns such as trauma-impacted attachment and online behaviours that undermine children's sense of self-worth. They are also more susceptible to the harmful messages in pornography and the negative impacts on their sexual health and development as noted in a 2015 Commission for Child and Young Person (CCYP) inquiry.[7] The Inquiry into the sexual exploitation of children in residential care in Victoria identified some of the harmful effects of the online environment on children in residential care settings:

> *The Inquiry saw evidence that pornography, social media and the internet play a significant role in the lives of vulnerable children and young people in residential care. The challenge for the Victorian Government and the entire service system is how to prevent and manage the inevitable and ongoing risk that social media poses to our children in care who, prior to entering into care, have experienced significant trauma, psychological damage and abuse.*[8]

In 2021, the Centre hosted several online sessions with 85 foster and kinship carers in Victoria to identify key concerns about their children's online safety. Carers described a range of unsafe online situations in which their children and young people had found themselves, including:

- Racial vilification in online chat
- Screen addiction
- Hidden chat options

[4] Ibid.
[5] OECD (2020). Protecting children online: An overview of recent developments in legal frameworks and policies. OECD Digital Economy Papers, No. 295, OECD Publishing, Paris.
[6] United Nations Children's Fund (2017). The State of the World's Children 2017: Children in a Digital World, UNICEF, New York.
[7] Commission for Children and Young People (2015). *…as a good parent would… Inquiry into the adequacy of the provision of residential care services to Victorian children and young people who have been subject to sexual abuse or sexual exploitation whilst residing in residential care*. CCYP
[8] Ibid. p.57.

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

- Child sexual exploitation
- Porn exposure to young children
- Online bullying
- Online shopping transactions
- Financial scams
- Radicalisation and exposure to extremism, including white supremacist forums and misogynistic ideologies.

The carers highlighted specific instances where the children in their care were at risk of online predatory and criminal behaviour including grooming, scams, bullying, sexting, and requests from unknown people to be 'friends'. In one instance, police contacted the carer to let them know their child was communicating online with a person wanted for several cases of grooming and child sexual exploitation. This was through an apparently safe website.

Impact of COVID

It is not only technology which has changed profoundly since the advent of the Act. Since the outbreak of COVID-19 and the lockdown environment in many countries globally, engagement with the cyber world has increased dramatically. Carers in our online consultation sessions, for example, discussed how COVID-19 has intensified their children's online use, and the associated issues and impacts, and were acutely aware of their limited information and lack of understanding of different risks, platforms, digital citizenship, and evolving technologies.

A 2020 consumer survey of around 13,000 people in 13 countries found that 95 per cent of consumers were spending more time on in-home media consumption and activities than prior to COVID-19, with 80 per cent of young people aged 16-25 years reporting extended use of smartphones. 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 in 2023, reports made to their CyberTipline increased by 12 per cent from the previous year, with more than 36.2 million reports of suspected child sexual exploitation online.[9] 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.[10]

Survey results from a 2021 study by the University of New South Wales concluded that during COVID-19 there was an increase in the following behaviours:

- Adults viewing and sharing child sexual abuse material and grooming minors
- Adults blackmailing minors into online sexual activity
- Minors engaging in risky online activities such as sending nude or sexual images of themselves
- Minors engaging in sexual activity on live streams or webcams.[11]

There appear to be three broad factors contributing to this increase in harmful behaviours and sexual exploitation of children online as a result of COVID.

- Lockdowns resulted in children's physical and social isolation from friends and trusted adults, thereby increasing risk and reducing protective factors for children
- Lockdowns encouraged children to spend more time online communicating with others, with limited caregiver capacity to supervise

[9] See https://www.missingkids.org/gethelpnow/cybertipline
[10] 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
[11] Salter, M. & Wong, T. (2021). The impact of COVID-19 on the risk of online sexual exploitation and the implications for child protection and policing. University of New South Wales. https://www.arts.unsw.edu.au/sites/default/files/documents/eSafety-OCSE-pandemic-report-salter-and-wong.pdf

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

- COVID lockdowns also affected people who present a risk to children, with self-reported escalation of concerning behaviours, such as sexual thoughts and behaviour towards children and young people.[12]

Reducing harm and maximising the benefits of online engagement

In relation to online child sexual exploitation, the Federal Government needs to ensure a universal, multi-pronged, whole-of-community approach across multiple stakeholders and sectors of society, not only reliance on legislation. Universal measures include getting big technology companies to remove images when they appear, creating safer online spaces for children, and preventing abuse in the first place by developing clear messaging for all children, parents and carers and identifying people who pose a risk to children with a view to deterring, disrupting and supporting them to not offend.[13]

Protective factors to mitigate the harms of online threats for children can be broadly classified into four areas:

- Increasing individual capabilities by enabling children to recognise their agency,[14] and supporting their social and emotional competencies to assist with critical thinking, high self-esteem and empathy.[15]
- Increasing the technical knowledge and capabilities of children, parents, caregivers, and educators to better understand the risks and help establish well-informed filters and security measures.[16]
- Encouraging 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.[17]
- Developing age-appropriate mediation strategies for actively monitoring and supervising technology use.[18]

The carers in our online discussion sessions called for more accessible and easy-to-find information about technology, parental tools, trustworthy online advice to help them support their children's safe use of the online environment. The views of children themselves, despite being such significant users on the Internet, have scarcely been recognised in the online governance space or in contemporary online safety discourse in Australia.

A recently released study by eSafety, Deakin University and the Queensland University of Technology sought the views of 117 young men aged 16-21 years in relation to their online experiences.[19] The study was strengths-based and youth-centred and its findings are important at a time when there has been such an intensive focus on how online immersion is shaping children's values and views of masculinity and gender.

The study found that while young men in the study demonstrated a high capacity for critical reflection about their behaviours and experiences online, young men could benefit from *'support to address their experiences of isolation and personal disempowerment, as well as strengths-based, empowering education about the causes of gender inequality and the benefits of gender equality*.[20] The report highlights the complexity of an online environment in which children and young people who are still developing their identities and values are

[12] Harris, M., Allardyce, S., & Findlater, D. (2021). Child sexual abuse and COVID-19: Side effects of changes societies and positive lessons for prevention. *Crim Behav Ment Health* 31(5): 289-92. doi: 10.1002/cbm.2214
[13] Ibid.
[14] 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.
[15] 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.
[16] Schiamberg, L., Barboza, G., Chee, G., & Hsieh, M. (2018). *The adolescent parent context and positive youth development in the ecology of cyberbullying*. p.19.
[17] Green, A., Wilkins, C., & Wyld, G. (2019). *Keeping Children Safe Online*. Think. UK; Zych, I., Farrington, D., & Ttofi, M. (2019). Protective factors against bullying and cyberbullying: A systematic review of meta-analyses. *Aggression and violent behavior*, 45, 4-19.
[18] Schiamberg et al.
[19] eSafety Commissioner (2024). Being a young man online: Tensions, complexities and possibilities, Canberra: Australian Government.
[20] Ibid, p.77.

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

exposed to harmful messaging, particularly in relation to gender and sexuality; predatory behaviours such as grooming, sexting, normalisation of pornographic images, emotional and financial blackmail and scamming; and unsafe situations with long-term consequences.

A literature review undertaken by the Centre in 2021 identified the following elements as critical when developing a cyber safety program:

- Adopting a child rights perspective, which enables equitable, age-appropriate access and meaningful participation, school and legal policy development, and includes children and young people in decision-making
- Teaching digital resilience, through enhancing the technical skills and critical thinking of all stakeholders
- Developing evidence-informed, outcomes-focused and context-specific cyber safety programs
- Providing adequate training for teachers, parents, caregivers, program delivery consultants and community members on safe internet practices and children and young people's perspectives of the internet
- Establishing a system-response through collaborations between families, school and communities
- Providing clear, safe and effective pathways for reporting abuse
- Developing consistent approaches and ongoing support for the different stakeholders
- Developing appropriate program content, which should be easy, age- and culturally- appropriate, and focus on respect, and feelings
- Providing a range of delivery modes, including cyber safety campaigns, interactive videos, role plays, games, posters, offline and online media
- Developing in-built data collection strategies to monitor and evaluate the short-term and long-term outcomes of programs.[21]

In addition to these kinds of strategies to build children's and caregivers' digital literacy, we need well-crafted policies and legal frameworks. A recent example of innovative child online safety legislation is Maryland's Age Appropriate Design Code (or the Kids Code) which 'requires online products and services reasonably likely to be accessed by children and teens under 18 to be age appropriate and designed in kids' best interests'.[22] Companies are required to take such actions as setting all default settings to the most private, designing age-appropriate experiences for children based on set age ranges, determining whether children are reasonably likely to access the company's products or services online, making it easy for children to report privacy concerns, letting children know when they are being tracked and monitored and conducting a risk assessment of how they use children's data.

Such legislation is not new – Age Appropriate Design Codes have been legislated in the UK (2021) and California (2022) for example – but the Maryland legislation is distinctive because of its constitutional approach to compelling tech companies to comply using a 'privacy by default and safety by design approach' rather than an approach which focuses on policing content or shutting down access to entire platforms.[23]

Australia has several effective mechanisms in place already through the Online Safety Act 2021 and impressive range of work carried out by the eSafety Commissioner. But the rapidity of technological advances and the lingering impact of COVID lockdowns on children's Internet usage, and on adult predatory behaviours, means legislation needs to be reviewed regularly, policies need to be constantly updated, and the perspectives of children and young people need to be reflected in the design of cyber safety tools and development of robust internet governance. The Maryland legislation shows what a workable legally sound approach might look like in relation to keeping children safe online and holding tech companies to account. The literature on effective cyber safety programs shows the importance of building the digital literacy and technical skills of children, parents, caregivers, educators, and community members, and of adopting a systems approach that involves

[21] Mitra, D. (2021) Keeping children safe online: A literature review. Centre for Excellence in Child and Family Welfare. Unpublished paper.
[22] See https://marylandkidscode.com/
[23] Miller, G. (2024). Maryland Kids Code signed into law but may face legal challenges. Tech Policy Press. https://www.techpolicy.press/maryland-kids-code-becomes-law/

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

policy makers, commercial stakeholders and law enforcement bodies. It also reinforces the importance of regular data collection, monitoring, research and continuing to build the evidence base relating to effective online safety approaches.

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