Bravehearts
bravehearts.org.au

BRIEFING PAPER

Young People Online

OUR POSITION:

Bravehearts believes in safeguarding children from potential risks and enhancing safety while engaging online.

- **Education and awareness: Children, young people and parents and caregivers should be equipped with the information and skills they need to lessen vulnerability against online harms.**
- **Safety by design: The concept of Safety by Design emphasises the importance of user safety and rights as fundamental in the design and development process of online products and services.**
- **Digital duty of care: Companies should be held responsible for users' safety, placing a duty of care onto digital platforms.**
- **Disruption through AI: AI-driven algorithms have the ability to identify and analyse potentially harmful online content, such as CSAM, grooming activities, and cyberbullying.**
- **Children's Digital Privacy Code: Bravehearts supports the development of a Code.**

Background

The digital environment was not originally designed for children; however, we know it plays a significant role in their lives. The truth is, for many young people, the online space is an avenue for support and connectedness. The online world offers a platform for learning, for creating a space for self-expression, and socialising. Online connections can foster a sense of community and belonging for many young people; where young people can share common interests, connect with those with shared identities, and where children who struggle with social anxiety can forge positive online connections that can help them connect with their peers offline.

On the flipside, we know the incidence of online sexual harm continues to escalate each year. It is essential for parents and caregivers to be aware of how online harms occur and to engage in preventive measures.

Technology has enabled sex offenders to engage in virtual grooming, manipulating children through social media platforms like TikTok, Snapchat, Facebook, Instagram and Discord.

Forms that online child sexual abuse (OCSA) can take include:

- Sextortion
- Online grooming
- Child sexual abuse material (CSAM)
- Exposure to inappropriate content
- Livestreaming of child sexual abuse
- Online privacy

We can support our children in safely traversing online spaces by adopting simple strategies to lessen the risks involved.

(NB: a separate briefing paper explores risks related to AI)

Sexual Extortion and Image-based Abuse

Sexual extortion, commonly referred to as sextortion, constitutes a type of online blackmail in which an individual deceives or

coerces another into providing sexual images of themselves. In some cases, offenders may also attempt to capture sexual images of young individuals during live streams or video sessions, often without their awareness, a practice referred to as ‘capping’.

The perpetrator subsequently threatens to disseminate these images unless the victim meets their demands, which often include requests for additional images, monetary compensation, or sexual acts.

While sexual extortion is a crime that targets both adults and children, it is children who are at a heightened risk. This increased vulnerability is attributed to their significant online activity, along with a greater willingness to take risks and a lower level social and developmental maturity.

A recent report by Thorn (2024), found that 1 in 17 minors reported having personally experienced sextortion.

An Australian study of adolescents found that 11% of the adolescents surveyed reported having encountered sexual extortion at some point in their lives. Among these individuals, one-third had been victimised on several occasions, and over half had faced sexual extortion before the age of 16 (Wolbers et.al., 2024).

The likelihood of experiencing sexual extortion is relatively consistent across all genders (Wolbers et.al., 2024); nonetheless, male victims were more often faced with financial demands and were typically approached by individuals they had never met face-to-face. Female victims were more likely to be solicited for intimate content.

Those who have faced sextortion frequently describe a variety of emotional responses, including fear, anxiety, and a sense of being trapped. They may harbor negative thoughts about themselves, often engaging in self-blame. Feelings of shame, embarrassment, and the compulsion to keep the matter confidential can arise, alongside worries about others learning of the situation, which complicates their ability to trust. Additionally, individuals may struggle to participate in their regular activities, such as working, studying, socialising, or engaging in online interactions. The psychological strain associated with sextortion can significantly affect one's mental well-being, leading some young individuals to contemplate self-harm or suicide.

Sharing nudes and sexting

According to reports, 1 in 7 young individuals between the ages of 9 and 17 has admitted to sharing nude photographs of themselves. A considerable number of these minors are engaging in this behaviour with people they have only interacted with through the internet, with 46% reported sharing explicit content with someone they encountered online (Thorn, 2024). Of those surveyed, only a third, 34%, thought they were sharing their images with an adult. Additionally, an Australian study found that 1 in 13 children under the age of 18 have faced the unauthorised sharing of sexual images of themselves, known as image-based abuse (Walsh et.al., 2025).

The term 'sending nudes' is commonly used among young people to describe the act of sharing personal and intimate photographs or videos with another individual through texts or online. 'Sexting' refers to the transmission of sexual messages, which may include images or videos, or occur solely

through text. The practices of sending nudes and sexting are increasingly prevalent among both youth and adults.

The act of sharing, or threatening to share, intimate images or videos without the consent of the individual depicted is classified as 'image-based abuse.' In cases where individuals are coerced into sharing such content, it is referred to as sexual extortion or 'sextortion,' a specific form of image-based abuse. Given the potential trauma associated with image-based abuse, it is crucial for young individuals to feel empowered to seek support, enabling them to have the images removed and access any necessary assistance.

Online Grooming

Online grooming is defined as the behaviour of an individual who engages in online communication, such as through social media, in a predatory manner with the intention of lowering a child's inhibitions or increasing their curiosity about sexual issues. This may include various forms of online interaction, such as chats and sexting. Any platform, game, app, or website that allows for interpersonal communication can be utilised for grooming, particularly those that are popular among youth.

A recent Australian study found that just under 20% (1 in 6) reported experiences of sexual grooming by adults, as a child, with the study acknowledgment that not all abuse is disclose (Walsh et.al., 2025)

To understand the dynamics of online grooming, it is essential to recognise that young individuals possess the same fundamental desires and requirements as older individuals, including a drive for self-discovery, a demand for validation, and a desire for acknowledgment. The grooming process often begins with the sharing of pornographic content to normalise discussions surrounding sexual activities.

The ultimate aim is to facilitate a face-to-face encounter for sexual purposes, have the child share intimate images or engage in sexual acts on a webcam.

Social Media, Messaging and Gaming

At the end of 2024, the Australian Government passed the *Online Safety Amendment (Social Media Minimum Age) Bill 2024*, introducing a mandatory minimum age of 16 for accounts on certain social media platforms. Seeking avenues that will ensure safety for children in the online space is critical, however, Bravehearts position is that increasing the minimum age on a selection of online social media platforms simply will not work.

As Bravehearts outlined in our submission to the Bill, legislating a minimum age for social media comes with huge challenges and concerns around balancing the prevention of online harms and the digital rights of children and young people.

A recently released research report (eSafety Commissioner, 2025) reveals that:

- 80% of the surveyed children aged 8 to 12 used one or more of the eight social media services in 2024, despite policies prohibiting users under 13.
- Around 54% of children aged 8 to 12 who used social media accessed these services via their parent’s or carer’s account(s)

- 36% of children aged 8-12 who had used social media had their own account with 77% of those saying they had help to set up their account(s). This help came mostly from parents or carers.
- 84% of children (aged 8 to 12) with accounts reported that their parents or carers knew about their account(s).

Given current social media policies, prohibiting users under the age of 13, are not working, it is clear we need to do more to protect children and young people in the online space.

It is not just social media that poses a risk for children and young people.

Children access online multiplayer games (e.g., Roblox, Minecraft and Fortnite) as it provides them with the opportunity to play with people from all over the world, which exposes them to risks such as cyberbullying and sexual grooming. Gaming online potentially allows strangers to interact with children and young people, and to exploit the anonymity of avatars to hide their real identities. Sexual predators use gaming platforms to target potential victims. If they build online relationships with children, this could lead to offline dangers. Online gaming also potentially exposes children and young people to inappropriate and explicit content and images.

Messaging apps are an indispensable tool for children to communicate with friends and family. Popular messaging tools like WhatsApp, Telegram, Teams and Slack all pose potential risks to children and young people. Apps such as KIK and Whisper (removed and restored to Apple/IOS app stores multiple times) have infamously been involved in online risks to children and young people. Identified risks again include: cyberbullying, participating in a conversation with strangers who may want to harm them, sending or receiving inappropriate content and falling victim to an online predator who may manipulate and exploit the child.

Child Sexual Abuse Material

The persistent issues of child sexual abuse material (CSAM) and child exploitation have a devastating impact on thousands of children each year. CSAM involves the production, distribution, and consumption of explicit materials that feature minors, thereby perpetuating the abuse they experience. Such content is typically created through coercive, manipulative, or exploitative means targeting vulnerable children. The prevalence of this material on multiple online platforms makes it difficult to eliminate entirely.

In 2023, there were an overwhelming 36.2 million reports worldwide regarding suspected instances of child sexual abuse material online. In addition, a comprehensive study conducted globally by Economist Impact on behalf of WeProtect Global Alliance revealed that 54% of respondents aged 18 to 20 had encountered online sexual harms during their formative years (Suojellaan Lapsia Protect Children, 2024).

Exposure to Inappropriate Content

Inappropriate content can take on various forms, ranging from false information, violence, extremism to adult material or illegal content. Children with may come across such content by accident or purposively or receive it directly from other children or adults.

In an Australian study, exploring the exposure of young people to pornography, the average age of initial exposure was found to be 13.2 years for males and 14.1 years for females, with medians of 13 and 14 years, respectively (Crabbe, Flood, & Adams, 2024).

NB: A separate Briefing Paper explores the impact of exposure to pornography to children and young people.

Livestreaming of child sexual abuse

As a result of technological development, there has been an increase not only in videos and images of child sexual abuse and exploitation, but also in the phenomenon of live streaming of child sexual abuse. Live streaming of child sexual abuse involves distribution of the sexual abuse of children live via webcam to people anywhere in the world.

The 'real-time' characteristic of child sexual abuse livestreaming sets it apart from other types of child sexual abuse material that are shared on the internet. Live streaming of child sexual abuse is predominantly associated with Southeast Asia. Research on Australians involved in financials transaction relating to live streaming of sexual abuse in the Philippines, identified 256 individuals. (Brown, Napier and Smith, 2020). This research focusing on Australians viewing live streamed child sexual abuse (Brown, Napier & Smith, 2020) demonstrates that this is a global issue and a concern for Australia. As such, we have an important opportunity to lead real-world change in how governments and NGOs respond to and ultimately prevent technology-facilitated child sexual abuse, particularly within our region.

Legislation has been developed both here in Australia and internationally to address live streaming of child sexual abuse.

Online Privacy

In today's digital age, children often engage with the internet to socialise, acquire knowledge, and find entertainment. It is impractical to expect that children can be completely shielded from online access. Nevertheless, many online platforms aimed at youth may not guarantee safety, suitability, or privacy protection. A recent survey revealed that 85% of Australian parents are worried about these issues, emphasising the need for children to be equipped to navigate the internet while ensuring their data privacy is safeguarded (Office of the Australian Information Commissioner, 2023).

Information collected online can be exploited, leading to issues such as spam, scams, fraud, identity theft, grooming, and unwanted interactions, which may ultimately contribute to online child sexual abuse.

Images of children shared online or through social media platforms may circulate beyond the intended audience, or they could be 'harvested' from these platforms and utilised for inappropriate purposes.

Bravehearts Position

There is no denying that the online world has risks, but at the same time, the benefits of online platforms for children and young people are undeniable.

Children (defined as under 18 by the UN-Convention on the Rights of the Child) have a right to safe access to online spaces. Digital rights requires that all children have equal and effective access to the digital environment in ways that are meaningful for them; child rights also include rights to participation, information and expression (United Nations, 2021).

Bravehearts believes that steps can be taken to safeguard children from potential risks and to enhance their feelings of safety and confidence while engaging online. This involves monitoring their online experiences, supporting them in acquiring relevant skills, utilising the safety features provided in games and applications, and creating a supportive atmosphere that encourages them to seek help when needed.

- Education and awareness: While it is unreasonable and unfair to hold children, young people and parents and caregivers individually responsible for avoiding and dealing with harms in the digital environment, it is critical that we equip these cohorts with the information and skills they need to lessen vulnerability against online harms. Children need to know the positives and negatives of the online world and be prepared to monitor and act when necessary. Importantly a considered and sizeable investment in digital literacy and good digital citizenship education is required to help develop skills that are needed to ensure positive and safe online behaviours and practices. Parents and caregivers should be equipped with the knowledge to engage in open dialogue around digital literacy, online safety skills and help-seeking.
- Safety by design: The concept of Safety by Design emphasises the importance of user safety and rights as fundamental elements in the design and development process of online products and services. Safety by Design operates under three key principles: (1) Service provider responsibility, (2) User empowerment and autonomy and (3)Transparency and accountability
- Digital duty of care: Social media platforms and apps are widely used because they promote opportunities for conversation and personal connection; and are created by for-profit companies. We need the technology sector to do more to monitor what is happening online, supported by government rules and regulations. The recently announced Digital Duty of Care, is a positive step towards companies being held responsible for users' safety, placing a duty of care onto digital platforms for the wellbeing of their users, and requires digital platforms to implement diligent risk assessments and risk mitigation plans to make their systems and processes safe for all Australians.
- Disruption through AI: The promise of artificial intelligence in predicting and preventing child sexual abuse is significant. AI-driven algorithms have the ability to identify and analyse potentially harmful online content, such as CSAM, grooming activities, and cyberbullying.
- Children's Digital Privacy Code: Bravehearts supports the development of a Code that protects the digital rights and privacy of children and young people.

References

Brown, R., Napier, S. & Smith, R. (2020). Australians who view live streaming of child sexual abuse: An analysis of financial transactions. *Trends & Issues in Crime and Criminal Justice*, no. 589. Canberra: Australian Institute of Criminology. doi.org/10.52922/ti04336

Crabbe M, Flood M, Adams K. (2024) Pornography exposure and access among young Australians: a cross-sectional study. *Australian and New Zealand Journal of Public Health, 11*. doi: 10.1016/j. PMID: 38508985

eSafety Commissioner (2025). *Behind the screen: The reality of age assurance and social media access for young Australians*. Sydney [NSW]: eSafety Commissioner

eSafety Commissioner (2019). *Safety by Design Overview*. Sydney [NSW]: eSafety Commissioner

Office of the Australian Information Commissioner (2023). *Australian Community Attitudes to Privacy Survey 2023*. Office of the Australian Information Commissioner, Australian Government.

Suojellaan Lapsia Protect Children (2024). *Tech Platforms Used by Online Child Sexual Abuse Offenders: Research Report with Actionable Recommendations for the Tech Industry*. Retrieved from: https://www.suojellaanlapsia.fi/en/post/tech-platforms-child-sexual-abuse

Thorn (2024). *Youth Perspectives on Online Safety, 2023*. Retrieved from: https://www.thorn.org/research/library/2023-youth-perspectives-on-online-safety/

United Nations (2021). General comment No. 25 (2021) on children's rights in relation to the digital environment. Retrieved from: https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-25-2021-childrens-rights-relation

Walsh, K., Mathews, B., Parvin, K., Smith, R., Burton, M., Nicholas, M., Napier, S., Cubitt, T., Erskine, H., Thomas, H.J., Finkelhor, D., Higgins, D.J., Scott, J.G., Flynn, A., Noll, J., Malacova, E., Le, H., and Tran, N. (2025). Prevalence and characteristics of online child sexual victimization: Findings from the Australian Child Maltreatment Study. *Child Abuse and Neglect, 160*, doi.org/10.1016/j.chiabu.2024.107186

Wolbers, H., Cubitt, T., Cahill, M., Ball, M., Hancock, J., Napier, S. & Broadhurst, R. (2024). Drivers and deterrents of child sexual offending: Analysis of offender interactions on the darknet. *Trends & issues in crime and criminal justic*e no. 703. Canberra: Australian Institute of Criminology. doi.org/10.52922/ti77659

Bravehearts Foundation Limited
ABN: 41 496 913 890 ACN: 607 315 917
PO Box 575, Arundel BC, Qld 4214
Phone 07 5552 3000 Email research@bravehearts.org.au
Information & Support Line 1800 272 831
bravehearts.org.au