General Comment on children’s rights in relation to the digital environment

Feedback from eSafety Commissioner, Australia

**November 2020**

# Introduction

The Australian eSafety Commissioner (eSafety) thanks the Committee for its draft general comment on children's rights in relation to the digital environment. We welcome opportunity to provide feedback and engage in this global dialogue.

eSafety wishes to outline at the outset that it fully supports efforts to respect, protect and fulfil children's rights in the digital environment. We acknowledge the significance of the general comment in setting a global standard for States in meeting their obligations under the Convention and its Optional Protocols, and responsibilities to secure children’s rights to provision, protection and participation in the digital environment.

## eSafety’s comments on the general comment

**Introduction to the general comment**

eSafety welcomes the comprehensive description of the digital environment and acknowledgement that it is continually evolving and expanding. Accordingly, we recommend including reference to new products and platforms, so that it remains relevant in the context of technological advances and emerging practices (text additions/deletions underlined).

1. The digital environment is continually evolving and expanding. It includes the internet and mobile technologies; digital networks, content, services and applications; old and new systems of media, communication and information; connected devices and environments; virtual and augmented reality; artificial intelligence, including machine learning; robotics; automated systems and data analytics; and biometrics and biotechnology. Children’s rights should be upheld across the entire digital environment, including in the design of products and platforms in development or not yet developed.
2. The opportunities and the risks of harm for children are likely to increase, even where children do not actively access the internet, as societies progressively rely upon digital technologies for their functioning. Consideration must be given to children’s safety, privacy and security in the context of being both actively and passively connected, as the pervasiveness of AI, Internet of Things and autonomous technologies increase.

We consider it important to highlight in the introduction that there are individual, social and systemic factors that may impact a child’s ability to recognise online risks, use preventative measures to protect themselves from harm, or seek help. These may relate to gender, age, race, religion, disability, sexuality, cultural background or geographic location, and can also impact on a person’s ability to fully participate and reap the benefits of being online and connected. While these factors are drawn out in the general principles (right to non-discrimination), we recommend these are drawn out upfront.

**General principles**

eSafety supports highlighting the four general principles as a lens through which to view children's rights in a digital environment. We note that they map to the three distinct categories – rights of provision, protection and participation – that are used to provide structure to reflect and assess the extent to which existing instruments, policies and practices facilitate children’s rights in all contexts, including in the digital environment.[[1]](#footnote-2)

eSafety has provided some expansion to how online harms and risks are described:

1. States shall take all appropriate measures to protect children from the risk and threat to their right to life, survival and development in the digital environment. These include content, contact and conduct risks, and threats that can impact a child’s social, emotional, psychological, financial or even physical safety. These include bullying, gambling, sexual exploitation and abuse, persuasion, encouragement, promotion or incitement relating to suicide and other life-threatening activities including by criminals, armed groups and those designated as terrorist groups. States should identify and address emerging risks children face in diverse contexts by consulting them as children have an important insight into the particular and emerging risks they face.

We welcome the recognition of the earliest years of life as a time that requires specific attention in relation to the digital environment, which aligns with eSafety's research.[[2]](#footnote-3) While we acknowledge that a precautionary approach should be taken with very young children, we believe the general comment should go further in highlighting that it is never too early to start building good skills for engaging online. eSafety's early years program provides an evidence-based model and has been adapted for international use.[[3]](#footnote-4)

1. States should pay specific attention to the earliest years of life, when brain plasticity is maximal and the social environment, particularly the relationships with parents and caregivers, is crucial in shaping the child’s cognitive, emotional and social attitudes and skills. Accordingly, it is important to ensure that children and their parents and carers are being prepared from an earlier age to navigate these environments safely. This requires multi-level awareness raising and capacity building for parents and carers, early educators and young children themselves. Moreover, although there is insufficient evidence that early use of digital devices may increase the risk of later digital addiction, a precautionary and strengths-based approach should be taken also in this respect.

**Evolving capacities**

eSafety supports the description of evolving capacities. We suggest that the recommendation for digital providers to offer or make available services to children appropriate for their evolving capacities be clarified to explain that it is not necessarily about restriction or creating a 'walled garden' but rather identifying and mitigating risks, and building safety and children's rights into the design of digital services.

1. States should require digital providers to offer or make available services to children appropriate for their evolving capacities by employing safety-by-design, building in protections and mitigating risks for children in the design, development and deployment of all online services.

**General measures of implementation by States**

The general measures of implementation by States propose concrete recommendations on how to uphold and promote children's rights in the digital environment.

In Australia, eSafety is mandated to lead and coordinate online safety efforts across government departments and agencies. eSafety collaborates with governments and organisations globally to shape the development of safer and more responsible online environments. As countries join Australia in establishing online safety regulators, it is imperative that legislation, governance and national online safety strategies are internationally aligned and that a high standard for online content regulation is set. eSafety recommends including recognition of the need to coordinate and collaborate globally, both bilaterally, regionally and internationally.

1. States should identify a government body that is mandated to coordinate policies and programmes related to children’s rights in the digital environment among central government departments and different levels of government. It should also cooperate with businesses, civil society and other organizations to realize children’s rights in relation to the digital environment at cross-sectoral, national, regional and local levels. It is equally important to collaborate with other governments and international organisations, to promote global interoperability and a high bar for digital policies. Such a body should be able to draw on technological and other relevant expertise within and beyond government as needed. It should be independently evaluated for its effectiveness in meeting its obligations.

eSafety recommends privacy and ethical considerations be included in relation to the collection of data.

1. Data collection and research are vitally important as a means of mapping and understanding the implications of the digital environment for children’s rights, and for evaluating its impact on children, and the effectiveness of State interventions. States should ensure the production of robust, comprehensive data that is adequately resourced, ensuring that privacy, capacity to consent and the best interests of the child drive data collection and storage. Such data and research, including research conducted with and by children, should inform regulation, policy and practice and should be in the public domain.

With regard to the dissemination of information, awareness-raising and training, eSafety supports an approach that broadens the provision of online safety education so that it is empowering, builds resilience and effects positive culture change, while also promoting the development of safe and appropriate long term behaviours.

1. States should disseminate information and conduct awareness raising campaigns on the rights of the child in the digital environment, which start when children are young, and which are scaffolded and appropriately staged from the early years through to the final years of school and beyond. States should facilitate educational programs for children, parents and caregivers, as well as the general public and policy makers, to enhance their knowledge of children’s rights and develop their digital literacy and skills. This should include how children can benefit from digital services, how to minimize risks and how to recognize a child victim of online harm and respond appropriately. Implementation of curriculum and programs should be monitored and reviewed and a child’s knowledge and skills should be checked through assessment. Children should be involved in the review process to make sure programs meet their needs.
2. Professionals working for and with children in all settings, including in health and mental health facilities, in social work, alternative care institutions, law enforcement, the justice system as a whole, and the business sector including the technology industry, should receive training that includes how the digital environment impacts the rights of the child in the multiple contexts and ways in which children access and use technologies. States should ensure that pre-service and in-service training relating to the digital environment is provided for educators working in nurseries, schools and other learning settings to support them to develop knowledge, skills, capacity and confidence to cover this content. They must also be supported to understand that their role within online safety education may include facilitating youth-centred perspectives around online life rather than playing the traditional role of content expert.

eSafety agrees that States should require businesses to prevent their networks or online services from being misused for purposes that threaten children’s safety and well-being, and ensure that appropriate sanctions are in place for non-compliance.

1. States should require businesses to prevent their networks or online services from being misused for purposes that threaten children’s safety and well-being, and to provide parents, caregivers and children with timely safety advice and prompt and effective remedy, and that they ensure that appropriate sanctions are in place for non-compliance.

Furthermore, eSafety recommends including recognition of the further challenges that may arise due to children not reporting negative incidents, due to fear of having access curtailed or that nothing will be done. States should ensure that remedies acknowledge the right to provision and participation alongside protection, and the conflict between these rights in relation to remedial responses.

1. Children whose rights relating to the digital environment have been violated face particular challenges in accessing justice due to difficulties in obtaining evidence and identifying perpetrators, or because they lack knowledge of their rights or what constitutes a violation of their rights in the digital environment. Further challenges may arise due to the sensitivity of the issues that include disclosing children’s online activities and fears of reprisals by peers or of social exclusion. Children may also fear disclosing experiences of online harms of abuse to their parents or caregivers for fear of having their access limited or curtailed, or because of a belief that nothing will be done.
2. States should ensure that appropriate and effective remedial judicial and non-judicial mechanisms for the violations of children’s rights relating to the digital environment are prompt, available and accessible to children and their representatives. Such mechanisms should include free, widely-known, safe, confidential and child-friendly complaint and reporting mechanisms to the relevant authorities. These authorities should look to implement mechanisms to receive reports of digital child abuse, and to take down child sexual abuse material and other forms of illegal content that harms children. States should also provide for collective complaints, including class action and public interest litigation. States should provide for legal or other appropriate assistance to children whose rights have been violated through the digital environment.

Similarly, we recommend greater attention be given to establishing frameworks and referral of cases and effective support for when children engage in harmful online behaviours that violate the rights of other children, and that this approach should be educative, rather than punitive.

1. States should establish, coordinate, and on a regular basis monitor and evaluate the framework for the referral of cases and provision of effective support to child victims. This includes measures for the identification, therapy and follow-up care and social reintegration of child victims. Specific attention should be given to developing a framework and effective resources to support children who display harmful online behaviours. Responses to these behaviours should be educative, rather than punitive, recognising the social and contextual factors that may have contributed to the situation. Measures within this framework should be multi-agency and child-friendly to prevent the child’s re-victimization and secondary victimization in investigative and judicial processes.

**Civil rights and freedoms**

Access to information and digital technologies and a child’s rights to freedom of expression, thought and association are critical for children to be able to reap the benefits that digital environments offer. eSafety recommends that principles of empowerment, autonomy, inclusion and children’s evolving capacities be explicitly referenced.

1. States should ensure that digital providers comply with relevant guidelines, standards and codes, enforce their own community content rules and provide sufficient content moderation to meet their published terms. The content controls, including parental control tools and school filtering systems, restrictions on the operation of any internet-based, electronic or other information dissemination systems should not be used to restrict children’s access to the digital environment, but only to prevent the flow of harmful material to children. Principles of empowerment, autonomy and evolving capacity should govern the administration and operation of content controls, and such controls should balance protection against children’s rights, notably their rights to freedom of expression and privacy.

**Freedom of expression**

1. A child’s right to freedom of expression includes freedom to seek, receive and impart information and ideas of all kinds, using any media of their choice. Children report that these technologies offer significant scope to express their ideas, opinion, and political views. For children in disadvantaged or vulnerable situations, online participation with others who share their experiences can help them to express themselves. For children who are same sex attracted, intersex or gender diverse, online participation can foster a sense of community, safety and connectedness as they explore their identities.

**Freedom of association and peaceful assembly**

1. Public visibility and networking opportunities in the digital environment can also support forms of child-led activism and empower children as advocates for their rights and the rights of others. The Committee recognises that the digital environment enables child human rights defenders, vulnerable children, children from diverse, at-risk or ~~including children with disabilities, children in street situations or from indigenous/minority communities~~ or disadvantaged groups to advocate for their rights, to communicate with each other and form associations. States should support them and ensure their safety.

**Right to privacy**

While encryption is a powerful tool for privacy, it also can assist in serious harms by hiding or exacerbating criminal activities, including online child sexual abuse. Encryption requires detailed consideration to minimise the potential for harm across communication channels, and to ensure there is a balance between security, privacy and safety.[[4]](#footnote-5) We recommend removing the section on end-to-end encryption. However, if it is to remain in the general comment, we recommend including a following additional text:

1. States shall take legislative and other measures to ensure that children’s privacy is respected and protected by all organizations and in all environments that process their data. Such legislation should include strong safeguards, independent oversight and access to remedy. States should encourage the adoption of privacy-by-design, such as end to end encryption, in services that impact on children. States should also ensure that the use and promotion of encrypted services is done in a manner that minimises the potential for harm across communication channels, and to ensure there is a balance between security, privacy and safety. States should regularly review such legislation and ensure that procedures and practices prevent deliberate infringements or accidental breaches of children’s privacy. States should ensure that consent to process a child’s data is informed and freely given by the child or, depending on the child’s age and maturity, by the parent or caregiver, and obtained prior to the processing.
2. Many children use online avatars or names that protect their identity, and such practices can be important to protect children’s privacy. For children who are same sex attracted, intersex or gender diverse, privacy and anonymity online can also provide protection from persecution as they explore their identities. States should take a safety-by-design approach to anonymity, to ensuring that anonymous practices are not routinely used to hide harmful or illegal behaviour, for example bullying or hate speech. Safety-by-design might include encouraging platforms to forbid such behaviours in their published terms and block users who fail to uphold their standards. Protecting a child’s privacy in the digital environment may be vital in circumstances when the parents or caregivers themselves pose a threat to the child’s safety or, for example, when they are in conflict over the child’s care (e.g. custody or access). Such cases may require interventions such as family counselling or other services to safeguard the child’s right to privacy.

**Basic health and welfare**

eSafety supports the recommendation for States to regulate against known online harms and proactively consider emerging health evidence. Given the evidence to suggest that exposure to pornography can negatively impact a young person’s mental health and wellbeing, knowledge, attitudes and expectations about sex and gender, and their involvement in risky or harmful sexual practices or behaviours, eSafety suggests include an explicit recommendation for States to consider measures to prevent access to online pornography.

1. States should encourage the use of digital technologies to promote healthy lifestyles, including physical and social activity. States should regulate targeted or age-inappropriate advertising, marketing or service designed to prevent children’s exposure to the promotion of unhealthy food and beverages, alcohol, drugs, tobacco and other nicotine products. Such regulations relating to the digital environment should be compatible with and keep pace with regulation in the offline environment. States should consider measures to prevent children accessing harmful online pornography, while providing education and information about sex, sexuality and healthy relationships.

**Education, leisure and cultural activities**

eSafety supports the focus on using the digital environment to enable and enhance children's access to quality education. We recommend that the safe use of digital technologies in education be highlighted, as well as stressing the importance of supporting children to develop social and emotional skills to manage online relationships, alongside digital literacy and citizenship skills.[[5]](#footnote-6)

1. States should invest equitably in technological infrastructure in schools, ensuring the availability of sufficient number of computers, quality connectivity and electricity, teacher-training on the use of digital educational technologies, and timely maintenance of school technologies. States should ensure that the technologies provided to, and used in, schools meet the highest standards of safety, privacy and security. States should support the creation and dissemination of diverse digital educational resources of good quality and ensure that existing inequality is not exacerbated by problems regarding access to such resources.
2. States should ensure that schools teach digital literacy and social and emotional skills for engaging online, as part of the basic education curricula from the earliest years, and such teaching should be evaluated for its outcomes. This curricula should include the skills to handle a wide range of digital tools and resources and those related to content, creation, collaboration, participation and civic engagement. It should include the critical understanding needed to find trusted sources of information and to identify misinformation and other forms of biased or false content; sexual and reproductive health issues relevant to the digital environment; knowledge about human rights, including the rights of the child and of others in the digital environment, and available forms of support and remedy. Also, it should promote awareness of the risks of children’s exposure to potentially harmful content, contact and conduct, including cyberbullying and other forms of violence, help-seeking behaviours and coping strategies to reduce harm and build children’s resilience.
3. It is of increasing importance that children gain an understanding of the digital environment including its infrastructure, business practices, persuasive strategies, uses of automated processing and personal data and surveillance. All teachers, particularly those who undertake digital literacy education and~~, including~~ sexual and reproductive health education, should be trained ~~on providing digital literacy education and~~ on safeguarding and respectful online relationships as it relates to the digital environment.

**International and regional cooperation**

As the world’s only online safety regulator solely dedicated to leading and coordinating online safety efforts nationally and to helping keep its citizens safer online, we support the recommendations on international and regional cooperation (p. 127/128). We know that other countries are looking to Australia's model as they develop their own regulatory bodies, and we welcome the opportunity to collaborate.

1. Council of Europe (2018). Policy guidance on empowering, protecting and supporting children in the digital environment. Available at <https://rm.coe.int/it-guidelines-background-document-policy-guidance-on-empowering-protec/168093b644> [↑](#footnote-ref-2)
2. eSafety Commissioner (2018). Digital parenting. Available at <https://esafety.gov.au/about-the-office/research-library> [↑](#footnote-ref-3)
3. eSafety Commissioner (2020). Online safety advice for young children, parents and carers. Available at <https://www.esafety.gov.au/key-issues/tailored-advice/international/advice-parents> [↑](#footnote-ref-4)
4. eSafety Commissioner (2020). End-to-end encryption trends and challenges — position statement. Available at <https://www.esafety.gov.au/about-us/tech-trends-and-challenges/end-end-encryption-position-statement> [↑](#footnote-ref-5)
5. Walsh, K., Wallace, E., Ayling, N., and Sondergold, A. (2020). Best Practice Framework for Online Safety Education

   Report for the eSafety Commissioner. Available at <https://www.esafety.gov.au/sites/default/files/2020-06/Best%20Practice%20Framework%20for%20Online%20Safety%20Education_0.pdf> [↑](#footnote-ref-6)