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

Submission to the UN Committee on the Rights of the Child

 **15 May 2019**

|  |  |
| --- | --- |
| P: +61 800 880 176 | E: enquiries@esafety.gov.au |

## Introduction

The Australian eSafety Commissioner (eSafety) welcomes the formulation of a General Comment on children's rights in relation to the digital environment by the Committee on the Rights of the Child. One in three internet users globally are children, children are early adopters of online products and technology, and children can be the most vulnerable to their potentially harmful impacts. More can and should be done to meet and address their rights in this space.

This submission, and further documentation referenced in it, sets out some of eSafety’s experiences in relation to several of the questions in the Concept Note, including:

* how children's views and experiences can be expressed and taken into account when formulating policies and practices which affect their access to, and use of, digital technologies;
* how the practices of businesses operating in the digital environment should support the realisation of children's rights;
* how states can better realise their obligations to children's rights in relation to the digital environment.

This submission describes the role and functions of eSafety, but does not include details of our research, findings, and governing legislation. For details about eSafety’s programs, powers and operation are available through our [website](https://www.esafety.gov.au/about-the-office).

## Overview of eSafety

The Australian eSafety Commissioner was established in July 2015 under the *Enhancing Online Safety Act 2015* (Cth) (the Act). At the time, the Act gave eSafety a remit of enhancing online safety for children. While this remit was expanded in July 2017 to include promoting online safety for *all* Australians, we remain deeply committed to assisting children to navigate the particular issues and risks which can cause them harm or prevent them from experiencing the full benefits of digital technology. The establishment of eSafety reflects the Australian Government's significant commitment to protecting children online, so they can safely access the opportunities that the digital environment provides. However, long-term, sustained social and cultural change to promote the rights of children online requires the coordinated efforts of the global community. The proposed General Comment may assist in the process of encouraging the development of similar offices or bodies in other countries that have ratified the Convention on the Rights of the Child (the Convention).

Under the Act, eSafety has a powerful combination of functions. These functions range from prevention through education, research and awareness raising, to early intervention and harm minimisation through three statutory schemes addressing Cyberbullying, Image-Based Abuse and Offensive and Illegal Online Content. In exercising these functions, the Act requires eSafety to have regard, as appropriate, to the Convention. This broad remit, coupled with the directive to consider the Convention, requires and enables eSafety to address children’s online issues in a multifaceted, holistic and proactive way.

Within the six-page limit, we have not been able to canvass all of the relevant issues, including the impacts of discrimination and accessibility on children's rights in the digital environment. For insight on these issues, we draw the Committee's attention to the submission of the National Children’s Commissioner, which has our full support.

## Functions and Powers of eSafety

### Research and Education

eSafety’s functions include supporting, conducting and evaluating educational programs and research about online safety. The available evidence,[[1]](#endnote-2) including eSafety’s own research,[[2]](#endnote-3) confirms that the digital environment is integral to the lives of children and carries both risks and opportunities for children's wellbeing and rights. It also demonstrates that these opportunities and risks are not experienced equally by all children. A complex intersection of personal identity, characteristics and vulnerable circumstances can create susceptibility to online risks and harms.

Our 2017 Youth Digital Participation Survey of more than 3,000 children in Australia aged 8-17 years highlighted that the most common negative online experiences related to receiving unwanted contact, contact with strangers and unwanted content (33%), followed by social exclusion, threats or abuse (21%). However, some experiences were more prevalent among particular groups of children. For example, 50% of children with disability and 44% of those from culturally or linguistically diverse backgrounds reported that they had spoken to a stranger online, and more girls than boys (24% vs 19%) reported experiencing online social exclusion. Our 2018 Youth Consultation for our Safety by Design work (see further details below and in appendix A), however, also demonstrates the important role that the digital environment plays in enabling children to i) communicate, providing them with a voice and sense of belonging, ii) research, providing them with an ability and the freedom to research anything they like regardless of the time of day and iii) access engaging and entertaining content, allowing them to relax, learn new things, avoid boredom and have fun.

It is imperative that policies and programs to improve online safety for children are based on robust evidence of relevant risk and protective factors. They should also be built on a rights-based framework which takes into account children’s best interests and their other core rights of participation and non-discrimination, as well as their evolving capacities to understand and make informed decisions about their engagement in the digital environment. National research is an important component of eSafety's remit, and we know that international research projects, such as Global Kids Online, are going some way to generating cross-national evidence bases on children’s online rights, opportunities and risks. We encourage and support these efforts. Systematic and coordinated research and consultations with children are essential, both in terms of addressing any evidence gaps as well as in helping to shape, coordinate and maximise online safety efforts globally.

We note that there is not yet a strong evidence base regarding the age or developmental stage at which technologies or online services are suitable for children. We are also not aware of any independent evaluation of the capacity of children at various ages to make an informed decision to hand over personal data to an online service provider without the provider obtaining the consent of the child’s parents or carers. Australian Privacy Law does not specify an age after which individuals can make their own privacy decisions, but indicates that an entity may presume that an individual aged 15 or over has the capacity to consent, unless there is something to suggest otherwise. eSafety supports this position, and also endorses the Council of Europe's recommendation that decisions regarding children's capacity to consent to the processing of their personal data should take into consideration their rights, views, best interests and evolving capacities.[[3]](#endnote-4)

Our recent national survey of 3,520 parents shows that children in Australia are going online at earlier ages, with 42% of two-year-olds being given access to Internet-enabled devices and 94% of children going online by the age of four years.[[4]](#endnote-5) Accordingly, it is important to ensure that children and their support networks 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.

eSafety plays a key role in educating Australians to develop critical digital skills. We achieve this through outreach programs in schools and the community; online information for children, young people and parents; virtual classrooms; peer-led ‘digital leaders’ programs; lesson plans; face-to-face training; expert guidance; and supporting NGOs and experts to deliver their own online safety programs and presentations to schools. We are currently working on developing resources to support pre-school teachers to promote online safety. Details of all our programs can be found on our [website](https://www.esafety.gov.au/about-the-office/program-overviews).

### Reporting and Complaints Mechanisms

A significant component of eSafety's mandate is to administer three reporting and complaints schemes:

* The **Cyberbullying Scheme** came into force in 2015. It allows Australian children under 18 years who are experiencing cyberbullying—or their parents, carers or authorised persons—to make a complaint to eSafety if social media sites fail to remove cyberbullying material from their sites within 48 hours of being alerted to it. The scheme serves as a safety net for children who have been cyberbullied on a relevant service and have not been able to resolve the issue via social media services' reporting functions.

eSafety triages complaints based on the severity of the situation and the complainant's self-reported distress level, endeavouring to provide a response as soon as possible and connecting the complainant with relevant counselling and support services in the interim. Since its commencement, eSafety has assisted more than 1,100 children and families with cyberbullying issues and has had success in working collaboratively with social media services to have material removed very quickly. Schools have reported to us that when eSafety acts to address a complaint from a student, bullying dissipates in the school community.

* The **Image-Based Abuse Scheme** came into force in 2018. It allows Australians of all ages to report to eSafety if their intimate image has been posted, or a threat has been made to post, on a relevant service without their consent. The intent of the legislation is to send a clear message to the community that the non-consensual sharing, or threatened sharing, of intimate images is unacceptable.

There are two aspects to the scheme: first, a legal framework for the removal of image-based abuse content through enforceable removal notices, and second, options for taking action against the person responsible for the image-based abuse. We take a graduated approach to enforcement action and have a wide range of informal and formal options available. We may give removal notices to hosts or individuals responsible for sharing (or threatening to share) the material, for which failure to comply may attract civil penalties of up to $105,000 AUD for individuals and up to $525,000 AUD for corporations. These penalties serve as a deterrent whilst also providing a significant incentive to individuals who have engaged in image-based abuse and relevant services to remove material quickly, minimising harm to victims.

To date, we have received 784 reports concerning over 1,700 URLs. Approximately 30% of our image-based abuse reports involve a person who was under 18 years of age in the intimate image.eSafety takes a holistic approach to ensure victims are well-supported and to minimise risk of further harm. Our reporting portal helps victims regain control by providing reporting options, referrals to support services and helpful resources.  We have strong collaborative arrangements in place with social media services to facilitate rapid removal of intimate images, providing quick relief to victims. eSafety has taken action against persons responsible for image-based abuse on five occasions and has successfully removed images reported to us in over 80% of cases.When the individual responsible for image-based abuse is a child, we generally take a remedial and educative approach, combined with removal action. If material is indicative of child sexual abuse, it is addressed through our Online Content Scheme.

* The **Online Content Scheme** came into force in 1999 and, before the creation of eSafety, was administered by the Australian Communications and Media Authority. It allows Australians to report (including anonymously) certain illegal and offensive online content, including child sexual abuse material. eSafety deals with thousands of reports each year, with almost 75% of these concerning child sexual abuse material. eSafety is able to notify material to the Australian Federal Police for criminal investigation and onward referral to Interpol, and to facilitate the rapid removal of the vast majority of this material through our international networks.

Our experience in administering the Online Content Scheme, in particular, points to the value of international cooperation in regulating the online world. The vast majority of the offensive and illegal online content reported to eSafety is hosted overseas. In these instances, we do not have jurisdiction to issue a takedown notice. However, our membership of the International Association of Internet Hotlines (INHOPE) enables us to refer content directly to a relevant INHOPE member and have content removed expeditiously so as to prevent the spread of child sexual abuse material and the re-victimisation of the children who are the subject of these images. These types of partnerships and collaborative approaches are key to effective online regulation.

These three schemes offer Australians practical help in managing the impact of these types of abuses, but their real uniqueness lies in the fact that eSafety can formally direct certain online service providers to remove content from their services, providing and empowering victims of online abuse to take control and help reduce harm and re-victimisation. While the schemes are largely operating as a cooperative model between government and industry, the powers available to eSafety to compel the removal of material provide a critical safety net and drive industry to be proactive in addressing online harms.

As noted above, the Act requires eSafety to have regard, as appropriate, to the Convention in exercising its functions. In relation to our reporting and complaints schemes, this includes taking into account the Government's obligations:

* to consider the best interests of the child in all actions concerning them (article 3),
* to provide children with an opportunity to be heard in any judicial or administrative proceedings affecting them (article 12),
* to protect children from arbitrary or unlawful interference with their privacy (article 16),
* to take appropriate measures to protect children from all forms of violence (article 19) and sexual abuse (article 34), and
* to ensure that children who are alleged to have infringed the law are dealt with in a manner appropriate to their age and wellbeing and proportionate to their circumstances and the alleged infringement (article 40).

In the context of cyberbullying and image-based abuse complaints, this means that children who report concerns are taken seriously and connected with appropriate support, and that eSafety endeavours to have the material removed as quickly as possible to minimise harm to privacy and wellbeing. Where cyberbullying incidents involve students from the same school, eSafety will often obtain consent with the complainant to engage with the school so that the situation can be resolved in accordance with the school's bullying policies. This allows for children who are alleged to have engaged in illegal or inappropriate behaviour to be treated in a manner consistent with their age, maturity and circumstances.

While the Cyberbullying and Image-Based Abuse Schemes have come into force relatively recently, the Online Content Scheme has been running since 1999 and has not been substantially reformed since 2007. A recent independent review of the scheme draws attention to important lessons about the regulation of new technologies.[[5]](#endnote-6) For example, one of the most significant difficulties with the scheme consists of its rigid definitions and distinctions based on technologies which are now obsolete. Accordingly, it is essential to use technology-neutral terms which refer to the functional aspects of products and platforms so that definitions can be interpreted to accommodate technological advances and evolving consumer preferences. It is essential that as a global community, we are on the front foot in addressing emerging and fast changing online risks and harms, that we are being proactive rather than simply reacting to, or retrofitting solutions, after the harm has been done.

## Safety by Design

eSafety recognises the need to drive-up standards of user safety within the technology community, and to encourage and secure greater consistency and standardisation of user safety considerations. To reduce risks and counter threats online, a proactive approach is critical. We recognise the importance of proactively and consciously considering user safety as a standard risk mitigation and development process.

In June 2018, eSafety laid out our intention to develop a Safety by Design Framework and set of Safety by Design Principles. At its core, Safety by Design (SbD) is about embedding the rights of users and user safety into the design, development and deployment of online and digital products and services. Consideration and care was taken to ensure that the SbD Principles and Framework balance an individual’s right to provision, participation and protection. In addition, the clear expectations on businesses to meet human rights responsibilities to children in the online world have been reflected in the SbD Principles.

SbD places user safety considerations at the centre of product development. It recognises and responds to the intersectionality of risk and harm in the online world and acknowledges the potential of advancements in technology, machine-learning and artificial intelligence to radically transform user safety and our online experiences. While personal information privacy and cyber security fall outside of eSafety's remit, SbD looks to the well-established processes surrounding privacy and security, and endeavours to elevate safety as the third design pillar in the developmental process.

It was vital to eSafety that the views and opinions of children were listened to, heard and actioned in the development of our SbD work. A five-day structured online forum was carried out with 123 children[[6]](#endnote-7) aged 14 to 17 of mixed gender, ethnicity, socio-economic background, schooling and location to guide the development of the SbD Principles. The forum explored participants' views about how they felt they could benefit from being online while being adequately protected. Children clearly articulated that they wanted greater control over, and more transparency from, the platforms and services they use. They wanted to be made more aware of safety features that exist or are being developed. They also wanted to manage their own safety more confidently. Lastly, they wanted to place their trust in industry. A summary of the findings from the consultation can be found in appendix A, and a vision statement which laid out what children want and expect from online industries to help users navigate the online world freely and safely is provided in full in appendix B.

Following an eight-month consultation process with industry, parents and carers and children, eSafety developed a set of SbD Principles that provide online and digital interactive services with a universal and consistent set of realistic, actionable and achievable measures to better protect and safeguard citizens' safety online. Three overarching principles were developed:

1. **Service Provider responsibilities**: This is premised on the fact that the burden of safety should never fall solely upon the end user. Preventative steps can be taken to help ensure that known and anticipated harms have been fully evaluated in the design and provisions of an online service, and steps taken to make services less likely to facilitate, inflame or encourage illegal and inappropriate behaviours.
2. **User empowerment and autonomy**: The dignity of users is of central importance, with users’ best interests a primary consideration. Human agency and autonomy can be supported, amplified and strengthened when designing services – allowing users greater control, governance and regulation of their own experiences, particularly at times when their safety is being, or is at risk of being, compromised.
3. **Transparency and accountability**: These are hallmarks of a robust approach to safety, that provide assurances that services are operating according to their published safety objectives, as well as educating and empowering the public about steps that can be taken to address safety concerns.

eSafety has been careful to articulate in the SbD Framework that the connections between privacy, security and safety are numerous, and the relationship between them is not binary. Indeed, many of the fundamental data protection and security principles are as much an imperative for user safety as they are for data protection, privacy and security. Our intention in the SbD Principles is to promote the rights and autonomy of citizens as they relate to user safety.

Our work on SbD is ongoing. With the core SbD Principles established, we will now create the SbD Framework of resources and work with industry to ensure user safety is embedded into the design, function and content of services. In the months ahead we will begin developing the guidance and resources that will assist industry in adopting SbD, working alongside key organisations and stakeholders.

## Conclusion

The digital environment poses new and broad-ranging challenges. One of the most significant is how parties to the Convention can meet their responsibilities in ensuring that respect for the rights of children are being met online. In particular, how they can ensure that online platforms and service providers are addressing children's rights in the provision of their services, the online protections that underpin their services and in guaranteeing children's online participation. Human rights standards—and particularly children's right to safety—should be at the centre of online design, content and functionality, as well as of regulatory and enforcement regimes.

The technological design and architecture of online services governs how users are able to interact and engage online. These aspects act as both a facilitator and amplifier for how humans interact, engage and behave. While technology may not drive behaviours, it is a medium through which these behaviours can manifest. As such, developers, engineers and vendors of online services play an incredibly important role in shaping online environments and users’ safety therein. Governments have an important role to protect children and drive up standards of user safety within the technology community, raising awareness and the capacity of the community to deal with risks, and putting in place safety nets to minimise harm when risks are realised.

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, our experience shows that a three-pronged approach of regulation, enforcement and education, combined with a children's rights perspective, has enabled positive outcomes for children in Australia. We know that other countries are looking to our model as they develop their own regulatory bodies, and we will welcome the opportunity to collaborate with them in the future. Long-term, sustained social and cultural change in the digital environment, that promotes the rights of the child and their safety and wellbeing, requires the coordinated efforts of the global community to achieve the best outcomes.

**Appendix A: Summary of Safety by Design Youth Consultation Findings**

Overview

In 2018, eSafety held a five-day structured online forum with 123 young people aged 14 to 17 of mixed gender, ethnicity, socio-economic background, schooling and location. To participate, the young person had to be a current internet user who engages in online activities several times per week. The rational for selecting this age group was to ensure that those who participated in this process could provide insights based on their user experiences of various social media platforms and apps. The forum explored participants’ views about how they felt they could benefit from being online while being adequately protected against risks and harms.

*The important things about being online*

Young people were asked to imagine what their lives would be like if they were not allowed to use the internet for leisure. They identified seven online activities as most important:

1. *Communication*: The ability to communicate online through social media is the most important aspect of being online for young people. In particular, they stressed that it allowed them to reach out to a wider network domestically and abroad and provided them a voice and a sense of belonging.
2. *Freedom to research*: The ability and freedom to research anything they like online regardless of the time of day. Young people expressed the importance of being able to research topics such as life skills, current affairs and educational topics outside of the school curriculum.
3. *Entertainment:* The internet provided entertainment and streaming capability. YouTube was synonymous with the word ‘entertainment’ regardless of gender, providing them with the means of accessing engaging content that matches their interests, as well as helping them relax, learn new things, avoid boredom and have fun.
4. *News:* A source of unbiased news. The majority stated that they do not watch broadcast television. Instead they rely on the internet to stay informed on the latest news and current affairs.
5. *Gaming*: Gaming, regardless of gender, was highlighted as a way to relax, have fun and avoid boredom.
6. *Shopping:* While online shopping was not seen to be as important as communication, most viewed the ability to shop online as vital to their way of life.
7. *Music*: Access to music was also very important for young people and most could not picture living without music streaming services like Spotify.

Young people also highlighted that their internet use has allowed them to form new relationships, share ideas and their creativity, start online businesses, apply for jobs and express themselves.

*Online rights and perceived risks*

When discussing negative experiences online in the forum, 64% of young people admitted that their awareness of potentially negative online experiences affected the way they interacted online. Females were more likely to believe that these negative experiences could happen to young people online than their male counterparts.

Young people were divided (58% - Yes and 42% - No) in their views of whether existing safety features on platforms, apps and devices would mitigate online risks. For those who thought that existing features were sufficient, the efforts made by social media platforms and other app developers to i) ensure the privacy of their users and ii) provide users with control over how their information is used, were acknowledged. However, for those who thought that existing safety features were inadequate, they felt that they had very little control, and were at the mercy of the changes that app and platform developers make to their settings. Account hacking, the creation of fake accounts and unwanted exposure to violence or sexual content were the areas where current safety features were seen as inadequate.

A recurrent theme voiced by a significant proportion of young people was that users themselves played a significant role in shaping the online environment. Young people felt that there was often very little that developers could do to prevent negative peer-to-peer interactions related to bullying, the spreading of rumours and targeted discrimination. It is thus not surprising that young people flagged rules, community standards and guidance to the user base on acceptable behaviour as important.

When provided with an overview of the UNCRC, 59% of young people reported being aware that they had rights in the online world. Of those aware of their rights, 57% felt that these rights were being met and addressed online.

*Expectations*

While an overwhelming majority—91%—believed that the online industry has a duty to keep their young users safe online, they recognised that safety is a shared responsibility between users, parents, schools, the wider community, government and law enforcement.

Young people were asked to prepare a vision statement, to lay out what they want and expect of the Australian online industry to help users navigate the online world, freely and safely. Seventeen themes were drawn out from the discussions, with over a third of respondents highlighting the following as areas they felt were important:

1. Empowering users by giving them greater control of their own safety and experiences online.
2. Providing clear rules and guidance that are easy to read and highly visible.
3. Providing users with safety tools and features, namely ways to make reports and to block both people and content.
4. Imposing sanctions and consequences for violating the rules of the site.
5. Using scanning and filtering technology to ensure user safety is upheld on the site and users are not exposed to inappropriate or sensitive content.

**Appendix B: Safety by Design Youth Vision Statement**

**Our Vision: Young People**

Our vision is that the Australian online industry:

* Enables users to **control** their online experiences and safety through the provision of tools and features that provide them with choices.
* Develops a strong set of easy-to-understand, highly visible, **ground rules** that have user safety at their core.
* Ensures users can easily **block and report** both people and content, placing control in the hands of the individual. This allows users to manage their online experiences and to help shape a more positive environment.
* Implements impactful **consequences and sanctions** for those who violate rules. This will reassure other users that their safety and security is a priority and sets clear expectations about how users should behave.
* Uses **developments in technology** to identify and minimise exposure to threats, risks, problems or content that is triggering, harmful or inappropriate. These precautions will help prevent harm or abuse, while also ensuring help is provided to those at risk.
* Provides users with **information and awareness** about safety features because knowledge leads to greater understanding, confidence, trust and, ultimately, use.
* Uses **human moderators**, alongside algorithms, to create a safe but not restrictive environment. Abuse and hatred should not be tolerated, and moderation would help prevent these from spreading.
* Provides users with **support**, and support networks, when they need it—especially when they are feeling low or do not feel safe. This will make users feel that they are not alone, that there are people and systems to help.
* Ensures **privacy settings** are comprehensive and set at the highest levels of protection by default. Also ensures that users know how to maintain and control their privacy, safety and security.
* Enforces some means of **verification** to make sure that people are real, are who they say they are and are accountable for their actions.
* Is aware of, and responsible for, the safety of users by valuing them above all else, **understanding the issues** they face and protecting their privacy and safety.
* **Empowers** users to interact freely online and to enjoy the benefits that the online world offers—without fear and without their rights or safety being put at risk.
1. Please refer to Third, A et al (2014). *Children's rights in the digital age, A download from children around the world*. Retrieved from https://www.westernsydney.edu.au/\_\_data/assets/pdf\_file/0003/753447/Childrens-rights-in-the-digital-age.pdf; Livingstone, S et al (2014). *EU kids online: Findings, methods, recommendations*. Retrieved from <http://lsedesignunit.com/EUKidsOnline/index.html?r=64>; UNICEF (2017). *Children in a Digital World: The State of the World’s Children 2017 report; Growing up In a digital age: An evidence review*. Retrieved from http://www.lse.ac.uk/media-and-communications/assets/documents/research/projects/childrens-privacy-online/Evidence-review-final.pdf. [↑](#endnote-ref-2)
2. eSafety Commissioner (2018). *State of Play—Youth, Kids and Digital Dangers*. Available at https://esafety.gov.au/about-the-office/research-library; eSafety Commissioner (2018). *Digital parenting*. Available at https://esafety.gov.au/about-the-office/research-library; eSafety Commissioner (forthcoming 2019). *Safety by Design*. [↑](#endnote-ref-3)
3. Council of Europe (2018). *Guidelines to respect, protect and fulfil the rights of the child in the digital environment*. Recommendation CM/Rec(2018)7 of the Committee of Ministers at p 16. Retrieved from https://rm.coe.int/guidelines-to-respect-protect-and-fulfil-the-rights-of-the-child-in-th/16808d881a. [↑](#endnote-ref-4)
4. eSafety Commissioner (2018). *Digital parenting*. Available at https://esafety.gov.au/about-the-office/research-library. [↑](#endnote-ref-5)
5. L Briggs (2018). *Report of the Statutory Review of the Enhancing Online Safety Act 2015 and the Review of Schedules 5 and 7 to the Broadcasting Services Act 1992 (Online Content Scheme).* Retrieved from https://communications.govcms.gov.au/publications/report-statutory-review-enhancing-online-safety-act-2015-and-review-schedules-5-and-7-broadcasting. [↑](#endnote-ref-6)
6. Please note that we have referred to 'children' throughout the submission, in line with the Convention's definition. However the detailed findings of our consultations with individuals aged 14-17 years in the appendices refer to participants as 'young people', in line with the terminology used throughout our Safety by Design project. [↑](#endnote-ref-7)