alannah & madeline foundation

Draft Online Safety (Basic Online Safety Expectations) Determination 2021

A submission by the Alannah & Madeline Foundation

October 2021

Contents

Executive summary

The draft Online Safety (Basic Online Safety Expectations) Determination 2021 represents a welcome step towards a proactive, structural approach to improving the safety of Australians online. In our response to the draft Determination, we focus on its implications for children and young people aged 0-18.

Recently, the Child Online Safety Index (DQ Institute) compared Australia against 30 countries and found that while Australian children were, on the whole, doing well online, they continued to be at higher than average risk of a number of problems, notably cyber bullying victimisation and perpetration, exposure to violent and / or sexual content, and low levels of parental guidance of children's digital media use. The Online Safety Act has great potential to help shift these indicators for the better.[1]

The draft Determination proposes additional expectations to sit beneath the Online Safety Act and reasonable steps that online services could take to meet these expectations, in order to uphold the safety of Australians on their services. Our submission focuses on the additional expectations and reasonable steps that address:

- default privacy and safety settings for online services used by children
- training in online safety for employees and contractors of online services
- assessment of safety risks by online services
- collaboration between online services to address high-volume, cross-platform attacks
- communication of key user documents by online services (eg. terms of use)
- access to reporting and complaints mechanisms for users of online services
- actions to address unlawful or harmful behaviour online and store reports about this behaviour.

In our recommendations, we respond to each of these proposed expectations and steps. We also emphasise four overarching points.

Firstly, there should be a clear, enforced expectation that online services have a duty of care to children who use their services, and that online services should provide a standard of safety which is in line with community expectations and at least equivalent to that expected of in-person spaces where children live, learn and play. The best interests of the child should be a key guiding principle. (See especially Recommendations 1 - 4.)

To this end, we submit that high-privacy default settings for children should be a clear expectation of online services. Assessment of safety risks, and online safety training for employees, should also be clear expectations. Here, we call for a child safety 'lens', recognising that children and young people at different developmental stages have particular needs and vulnerabilities, and are entitled to particular protections.

Child safety training and planning should function to bring online services in line with the National Principles for Child Safe Organisations.[2] Risk assessments should identify and address risks to children associated with contact, content, conduct, transparency of system design and data collection and use, so that online services are designed for child safety. We believe that the system design should protect children and young people, rather than the historical approach of holding children and their parents individually responsible for avoiding risky and harmful experiences online.

Secondly, there should be a clear commitment to upholding the rights of the child, referring to the United Nations Committee on the Rights of the Child, General Comment No.25 on children's rights in relation to the digital environment. (See especially Recommendations 5 - 10.) In line with this, we urge:

- that children's views have a meaningful role in the assessment of safety risks and impacts by online services; in the development and communication of online services' key documents; and in the improvement of pathways for reporting and complaints

- that any collection, use, storage and sharing of data about children's experiences of harmful or unlawful behaviours online is proportionate and reasonable and focuses on upholding the best interests of the child

- that steps be taken to improve children's experience of reporting and complaints mechanisms of online services. These mechanisms should be safe, effective, accessible, confidential, age-appropriate, and trusted by children

- that responses to antisocial behaviour by children online recognise that children are still developing and deserve to be treated differently to adults, even when they behave harmfully. Every effort should be made to find and use effective alternatives to the criminal justice system. There should be a strong focus on rehabilitation and positive behavioural change.

Thirdly, we support Safety by Design in reference to eSafety's principles and initiatives, which guide online services in anticipating, detecting and eliminating harms before they occur. We anticipate that its guiding principles of service provider responsibility, user empowerment and autonomy, and transparency and accountability will guide the implementation of the Act and this Determination.

Finally, we call for investment in high-quality digital literacies education in schools and early childhood settings, aligned with developmentally appropriate education about respectful relationships and backed by meaningful partnerships between school communities and trusted providers of high-quality digital literacies education.

We also call for targeted interventions to build the strengths, skills and supports of professionals who work with vulnerable children and young people, and parents and carers in communities with high levels of digital exclusion and / or complex disadvantage.

This is in recognition of the fact that the legislative and structural changes heralded by the Online Safety Act should be supported and enhanced by initiatives to build strength in school communities, families and services. A particular focus on communities with high levels of digital exclusion and disadvantage is important due to the much higher risks that vulnerable children and young people experience online and their limited access to appropriate education and supports. (See especially Recommendation 11.)

While the Online Safety Act and its draft Determination have great potential to improve children's safety, no structural or legislative solution is perfect or instantaneous. Children and young people who have risky or harmful experiences online still turn, for the most part, to their families, friends and school communities for support. It is vital that we continue to build strength in those spaces.

About us

The Alannah & Madeline Foundation is the leading national not-for-profit organisation working to protect children from the effects of violence and bullying.

We care for children who have experienced or witnessed serious violence; reduce the incidence of bullying, cyber bullying and other cyber risks; and advocate for the safety and wellbeing of children.

Our programs are in close to one third of Australian schools and more than 80% of Australian public libraries. We also support 10,000 children in refuges or foster homes across the country every year through our Buddy Bags program.

We have reached more than 2.7 million children and their families nationwide since the Foundation started.

Recommendations:

1. Item 6(3b) - Ensure that online services have robust privacy and safety settings (including in relation to geolocation and profiling), set to the highest level by default, unless there is a compelling reason for a different default setting in order to uphold the best interests of the child. Adopting the highest standards of privacy as a default setting for children should be a clear expectation of online services, not just a reasonable step. This approach should apply to all online services that children use, not just child-specific services. In this context, children should be recognised as anyone under the age of 18. We refer to the approach towards high-privacy default settings articulated in the UK Children's Code or Age Appropriate Design Code.

2. Item 6(3c) - Ensure that employees and contractors of online services receive high-quality training in child safe practice by reputable providers, in line with the National Principles for Child Safe Organisations, which were developed in response to the Royal Commission into Institutional Responses to Child Sexual Abuse. There may be a need to fund the development of training that is specific and relevant to online services. Training in creating and maintaining safe online environments for children should be an expectation of online services which are used by children, not just a reasonable step.

3. Item 6(3c) - Consider training employees and contractors of online services in understanding children's and young people's lives online - eg. via the Trusted eSafety Provider Program - and in understanding child and adolescent development, capacity-building and decision-making, perhaps through an introduction to the research of bodies like the Royal Children's Hospital (Melbourne).

4. Item 6(3e) - Ensure that all online services likely to be accessed by children assess child safety risks and impacts on children and implement child safety review processes at all stages of the service. This should be an expectation for online services, not just a reasonable step. It should be understood as part of a duty of care of online services towards children in their services. Child risk assessments should consider risks associated with contact, content, conduct, system design and data collection and use. The process should involve scoping the service's impact on children, gathering evidence, consulting, analysing risks, planning and implementing responses, reporting publicly on the response, and monitoring and reviewing the impacts of the response. There should be clarity about the minimum standards for child risk assessments, with the best interests of the child as the primary consideration.

5. Item 6(3e) - When assessing safety risks and impacts, online services should engage meaningfully with consumers, especially children under 18, their parents and caregivers. Such engagement could be done through partnerships with research institutes and services which have expertise in trauma-informed and child-rights practice, to support ethical and genuine engagement.

6. Item 6(2) - Build a clear, community-wide understanding of what is meant by materials and activities on online services which are, or may be, unlawful or harmful. If online services are expected to focus primarily on the concerns listed under Item 11 (cyber bullying of children, image-based abuse, Class 1 content, etc.), additional work may be needed to communicate this clearly across online services and the wider community. Alternatively, if it is anticipated that online services will develop their own definitions of harm, their approach should have a primary focus on the best interests of the child and be guided by United Nations Committee on the Rights of the Child, General Comment No.25 on children's rights in relation to the digital environment. Definitions should be developed through meaningful engagement with children under 18, their parents, caregivers, research institutes, early childhood settings, schools and services with expertise in trauma-informed and child-rights practice.

7. Item 10(2) - Ensure that if online services collaborate to detect high-volume, cross-platform attacks and share information with each other about material or activity that is, or might be, unlawful or harmful, they are guided by the approach to children's data articulated by the United Nations Committee on the Rights of the Child, General Comment No.25. In particular, any interference with a child's privacy must be lawful, proportionate, intended to serve a legitimate purpose, and uphold the

   principle of data minimisation. We also endorse the position of the UK Children's Code, which states that online services should not disclose children's data to third parties unless they can demonstrate a compelling reason to do so (eg. preventing crimes against children), taking account of the best interests of the child. Before sharing children's data with third parties, online services should undertake due diligence to help ensure the data will not be used in ways detrimental to children's wellbeing.

8. Items 14, 17 and 18 - We support these additional expectations, but urge that there should be an additional, specific requirement that online services make their key documents (terms of use etc.) clear, meaningful and accessible to children and young people at different stages of development. This is in recognition of young users' developmental needs and vulnerabilities. To this end, we submit that online services should:

   - meaningfully engage children under 18, their parents and caregivers in the development, review and communication of key user documents

   - ensure these documents are communicated to children, young people, their parents and caregivers in ways which are clear, accessible, accurate, prominent, concise, and appropriate for children at different stages of development. This includes using plain English, and, where possible, professionally translated. The UK Children's Code provides insights into what this communication could look like.

9. Items 15 and 16 - We support these additional expectations, but urge that there should be an additional, specific requirement that online services make their reporting and complaints mechanisms accessible and meaningful to children and young people. This is in recognition of the developmental needs and vulnerability of young users and their low uptake of reporting mechanisms. We encourage online services to review their reporting mechanisms through meaningful engagement with children, young people, parents and caregivers, ideally through partnerships with research institutes and support services. Improvement of reporting mechanisms should have a primary focus on the best interests of the child. We refer to the United Nations Committee on the Rights of the Child, General Comment No.25, which states that reporting and complaints mechanisms for children should be safe, confidential, free, responsive, child-friendly, and available in accessible formats. The UK Children's Code also outlines good practice approaches.

10. Items 11 and 19 - We call for recognition that any actions to address unlawful or harmful behaviour by children online, and to store information about this behaviour, should be guided by the United Nations Committee on the Rights of the Child, General Comment No.25. This specifies that state policymakers should consider the effects of cybercrime laws on children, focus on prevention, and make every effort to create and use alternatives to a criminal justice response. This approach recognises that children are still growing up and should be treated differently to adults, even when they behave antisocially. (Many children who behave antisocially online are also vulnerable themselves.) We call for investment in expert supports with a focus on rehabilitation and positive behavioural change, and structures to connect children who behave antisocially online with these interventions.

11. Additional steps – Invest in initiatives to build strength in early childhood settings, school communities, families and support services. There should be a focus on Australia's most digitally excluded and disadvantaged children and young people. In particular, we encourage investment in:

- high-quality digital literacies education, aligned with developmentally appropriate education about respectful relationships, with expert support for educators to prevent and address antisocial behaviours online and offline
- high-quality social and emotional learning initiatives, structures and programs
- meaningful partnerships for early childhood settings and schools with trusted providers of high-quality digital literacies education
- targeted interventions to build the skills and supports of professionals who work with vulnerable children and young people to address their needs, strengths and concerns online and offline
- targeted interventions to build the strengths, skills and support networks of parents and carers in communities with low levels of digital inclusion, to better enable them to support children and young people online. These interventions should be responsive to local circumstances, culturally appropriate, and built on trusting relationships.

12. Additional steps - Invest in robust research, analysis and evaluation to assess the short- and long-term impacts of the Online Safety Act for children, young people, parents and caregivers, including in relation to digital literacy and wellbeing outcomes. Findings should be shared with the community.

Strong default privacy and safety settings

Under item 6(2), the draft Determination states the additional expectation that online services will proactively minimise the extent to which materials or activities on their service are, or may be, unlawful or harmful.

(Note: it is unclear exactly how such material and activities are defined. Presumably it is intended that online services will focus on the priority concerns outlined under item 11 of the draft Determination: cyber bullying, image-based abuse, abhorrent violent content etc. However, greater clarity would be welcome. Material and activities which 'may be harmful' could, in theory, be subject to broad and contested definitions.)

In order to realise the above aims, item 6(3b) of the draft Determination proposes that a reasonable step would be for services to ensure their default privacy and safety settings are robust and set to the most restrictive level if their service or a component of their service is targeted at, or being used by, children.

We support the approach of ensuring privacy and safety settings are set by default to the highest level for online services that children use, unless there is a compelling reason for a different default setting in order to uphold the best interests of the child.

However, we believe the approach of high-privacy default settings should be strengthened:

- It should be an expectation of online services, not just a reasonable step.
- It should apply to all online services that children use, not just services aimed at children.
- It should recognise that a child is anyone under the age of 18.

We refer to the definition of high-privacy default settings adopted by the UK Children's Code or Age Appropriate Design Code. The Code states that high-privacy default settings should make it as easy as possible for children to maintain and revert to a high standard of privacy. Elements of good practice should include:

- online services do not collect any more personal data about children than they need in order to provide the service. Any use of a child's data to personalise the service must be activated by the child
- online services do not make children's data visible to other users unless the child amends their settings to allow this
- online services do not 'nudge' children to choose low privacy options
- if children choose to change their settings, they should have the option of doing so temporarily and reverting to high-privacy default settings at the end of the session
- high-privacy defaults should be retained following software updates.[3]

High-privacy default settings should apply across all online services that children use, not just services aimed at children. Children use many online services which were not made specifically for them. For example, a recent survey by the Cyberbullying Research Centre found that large numbers of children aged 9-12 were using services designed for older users. 67% watched YouTube, 31% played Fortnite, 30% used TikTok, 16% used Snapchat, and 15% used Instagram.[4] Similarly, a survey of Australian teens by eSafety found that their most popular social media platforms were YouTube, Instagram, Facebook and Snapchat, none of which are specifically for children.[5]

As the 5Rights Foundation have argued, default settings should function to give children a 'floor of protection' in digital spaces, instead of placing responsibility onto individual children and their parents.[6] Many parents have low levels of digital literacy and confidence themselves. A survey by the Australian Centre to Counter Child Exploitation found that parents commonly reported feeling overwhelmed and struggling to keep up with their children online.[7] At our online safety workshops, many parents have told us that they would welcome stronger built-in safeguards for their children's privacy online.

Online users commonly stick with the privacy settings they are given by default, which are often set to the lowest levels in order to maximise data collection and increase users' time and activity online. When users do opt to change their privacy settings, they often meet barriers designed to discourage them.[8] Results for children can be risky or harmful. In a recent research project, the 5Rights Foundation created avatar child profiles on social media and found that within days these accounts were being followed by strangers and receiving unsolicited messages and pornography from unknown users, as well as being prompted towards harmful content (eg. eating disorders, suicide) based on any signs of interest from the child.[9]

Ensuring high-privacy default settings for all online services used by children would align with Australia's Safety by Design approach. The Safety by Design principles of service provider responsibility and user empowerment and autonomy state that the burden of safety should never fall solely on the individual user. They suggest that online services be set to the most secure privacy and safety settings by default.[10]

Training in online safety for employees of online services

Under item 6(2), the draft Determination states the additional expectation that online services will proactively minimise the extent to which materials or activities on their service are, or may be, unlawful or harmful.

To this end, under item 6(3c), the draft Determination proposes that a reasonable step would be for services to ensure their employees or contractors are trained in and expected to implement and promote online safety.

We support this approach but believe it could be strengthened. We would like to see all online services which are used by children ensure that their employees receive high-quality training in child safety, delivered by

reputable providers, in alignment with the National Principles for Child Safe Organisations. Resources might need to be set aside to develop training that is relevant to online services.

We believe training employees in creating and maintaining safe online environments for children should be an expectation of online services, not just a 'reasonable step'.

The National Principles, while not mandatory, can be used by businesses which provide services to, and work with, children and young people.[11] It would make sense for online services to engage with the National Principles, in the spirit of ensuring children enjoy the same standards of safety online as they do offline.

It is also worth recognising that some states and territories have progressed further in legislating for child safety. In Victoria, for example, businesses must comply with the state's Child Safe Standards if they provide cultural, recreation, entertainment, play and photography services specifically for children.[12] To our knowledge, this has not yet been tested in online spaces. However, in theory, at least, it would surely be relevant to services such as YouTube Kids and Facebook Messenger Kids.

We would also like to see employees of online services receive high-quality training in understanding children's lives online, eg. by using the Trusted eSafety Provider Program.

It would also be beneficial for relevant employees of online services to be trained in understanding child and adolescent development (eg. by an expert provider such as the Royal Children's Hospital), to provide a clear context for children's and young people's experiences and behaviours online.

We believe this approach would align with Australia's Safety by Design principles of service provider responsibility, and transparency and accountability. These state that every attempt must be made to ensure that online harms are understood, assessed and addressed in the design and provision of online platforms and services. Services should embed user safety considerations, training and practices into the roles, functions and working practices of all individuals who work with, for, or on behalf of the product or service.[13]

Assessing safety risks and impacts

Under item 6(2), the draft Determination states the additional expectation that online services will proactively minimise the extent to which materials or activities on their service are, or may be, unlawful or harmful.

To this end, under item 6(3e), the draft Determination proposes that a reasonable step would be for online services to ensure that assessments of safety risks and impacts are undertaken and safety review processes implemented throughout the design, development, deployment and post-deployment stages for the service.

We support this approach. However, we believe that assessing safety risks and impacts for children and implementing child safety review processes at all stages of the service should be an expectation of online services, not just a 'reasonable step'. Acting on and mitigating identified risks to children should also be mandatory.

We refer to the United Nations Committee on the Rights of the Child (General Comment No.25 on children's rights in relation to the digital environment), which specifies that state parties should require the business sector to undertake child rights due diligence, in particular to carry out child rights impact assessments and disclose them to the public, with special consideration given to the differentiated and, at times, severe impacts of the digital environment on children.[14]

As the 5Rights Foundation have noted, child risk assessments, if done well, identify parts of an online service which may need to be redesigned, disabled or given risk warnings in order to keep children safe. A child risk assessment should consider risks associated with contact, conduct, system design and data collection and use, as well as content. The assessment should involve:

- knowing the customer ie. Children
- scoping the service's impact on children
- gathering evidence about risks to children's safety
- consulting, including with children themselves
- assessing and analysing risks that are likely to require mitigation strategies
- planning how the service will respond to these findings
- reporting publicly on the actions the service will take
- monitoring and reviewing the impact of these actions, including unintended consequences, and new risks emerging.[15]

This risk assessment approach should be understood as part of a service's duty of care towards children on their site. There should be clarity about the scope and minimum standards for child risk assessments for all online services likely to be accessed by children, guided by the best interests of the child as the primary consideration.

We believe this approach would align with Australia's Safety by Design principle of service provider responsibility, which states that online services should assess the potential risks of online interactions upfront and take active steps to engineer out potential misuse, reducing people's exposure to harms. Online services should prepare documented risk management and impact assessments to assess and remediate any potential online harms that could be enabled or facilitated by the product or service.[16]

When assessing safety risks and impacts, it is important that online services engage meaningfully with children, young people, and their parents and caregivers, and respond to their insights. Hearing directly from young users and the adults who support them would help online services to gain a clearer understanding of risks and impacts, design more effective interventions, and evaluate the outcomes of these interventions with greater accuracy and insight.

Such engagement could be done through partnerships with research institutes and services which have expertise in trauma-informed and child-rights practice, in order to support ethical and genuine engagement.

Findings should be shared (in a safe and de-identified way) to help build public accountability and trust, and to support other online services to better assess and respond to safety risks and impacts.

This approach would align with General Comment No.25 on children's rights in relation to the digital environment (United Nations Committee on the Rights of the Child) which specifies that states parties should ensure that digital service providers actively engage with children, applying appropriate safeguards, and give children's views due consideration when developing products and services.[17]

Addressing unlawful or harmful behaviour across multiple platforms

Under item 10(1), the draft Determination states the additional expectation that online services will take reasonable steps to consult and cooperate with providers of other services to promote the ability of end-users to use all of those services in a safe manner.

To this end, under item 10(2), the draft Determination proposes that reasonable steps could involve online services working with other services to detect high volume, cross-platform attacks and sharing information with other online services about material or activity on the service that is, or may be, unlawful or harmful for the purpose of preventing such material or activity.

There are compelling reasons why such steps might be needed. However, it is also vital that children's personal data is handled ethically and responsibly. Concerns about misuse of children's data could potentially arise in situations where online services collect and share information about a child as a victim and/or perpetrator of unlawful or harmful behaviour across multiple platforms.

Any approach to collecting and sharing children's data should be guided by the United Nations Committee on the Rights of the Child, General Comment No.25. General Comment No.25 states that privacy is vital to children's agency, dignity and safety and for the exercise of their rights. Therefore, any interference with a child's privacy must be lawful, proportionate, intended to serve a legitimate purpose, and uphold the principle of data minimisation. The best interests of the child should be the primary consideration.[18]

We support the approach to data sharing outlined in the UK Children's Code or Age Appropriate Design Code, which urges that:

- online services are guided by the best interests of the child whenever they consider sharing children's personal data
- online services do not disclose children's data to third parties unless they can demonstrate a compelling reason to do so, taking account of the best interests of the child. For example, data sharing might be legitimate for safeguarding purposes, such as preventing crimes against children
- if online services share children's data with third parties, they undertake due diligence and obtain assurances that it will not be used in ways which are detrimental to children's wellbeing.[19]

Consideration should be given to the needs and vulnerability of children at their various stages of development, with safeguards put in place to mitigate any negative impacts that data collection and sharing might have on them.

Online service documents and how they are communicated

Under item 14, the draft Determination states the additional expectation that online services will ensure they have terms of use; standards of conduct for end-users; and policies and procedures in relation to the safety of end-users, dealing with reports and complaints, moderation of conduct and enforcement of standards.

Under item 17, the draft Determination states the additional expectation that online services will ensure that these documents are readily accessible to end-users at all points in the end-user experience. The information should be written in plain language and reviewed and updated regularly.

Under item 18, the draft Determination states the additional expectation that online services will ensure that end-users receive regular reminders about the documents above and updates about any changes.

We support this approach. However, we urge that these additional expectations include a requirement that online services make the above documents meaningful and accessible to children, young people and their parents and caregivers, in light of young users' developmental needs and vulnerabilities.

In particular, we believe it is important that online services:

- meaningfully engage children, young people, their parents and caregivers in the development, review and communication of terms of use, policies, procedures, standards of conduct etc, with the best interests of the child as the guiding principle throughout
- ensure this information is communicated to children, young people, their parents and caregivers in ways which are clear, accessible, accurate, prominent, concise, appealing, and appropriate for children at different stages of development.

By meaningfully engaging children and young people in the development of key documents, online services can gain insights into how to make their services safer. This approach would align with the United Nations Committee on the Rights of the Child, General Comment No.25, which explains that states parties should ensure that digital service providers actively engage with children and give children's views due consideration when developing products and services.[20]

This approach would also align with Australia's Safety by Design principle of user empowerment and autonomy. This principle states that online services' protocols and consequences for service violations should reflect the values and expectations of their users.

Once formulated, it is vital that online services' key documents are accessible and meaningful to children, young people, their parents and caregivers.

Historically, documents published by online services (eg. terms and conditions) have been long, legalistic, and hard to understand, favouring the commercial collection and use of individuals' data.[21] For example, one study by legal researchers examined 500 'Terms of Service' agreements and found that 498 failed to meet consumer readability standards.[22]

To address this problem, we submit that there should be a minimum standard for terms and conditions and related documents published by online services, covering what content these documents should include and how they should be presented.

The UK Children's Code provides a model that could be drawn upon here. It states that documents produced by online services for their users should be:

- clear, concise, prominent, and easy to find
- accurate, not promising protections that are not upheld regularly
- child-friendly and presented in a way that appeals to children of different age brackets. Communications could include diagrams, cartoons, graphics, video, audio, and / or gamified or interactive content
- incorporating mechanisms for children and parents to choose which version of the information they see eg. up-scaling or down-scaling according to their level of understanding
- supported by additional, specific, 'bite-sized' explanations about data use at the point when the child is activating that use.[23]

We submit that this approach would align with Australia's Safety by Design principle of transparency and accountability. The principle states that online services should ensure their user safety policies, terms and conditions, community guidelines and processes about user safety are accessible, easy to find, regularly updated and easy to understand. Users should be periodically reminded of these policies and proactively notified of changes or updates through targeted in-service communications.[24]

Empowering children to report concerns

Under item 15, the draft Determination states the additional expectation that online services will ensure they have clear and readily identifiable mechanisms that enable end-users to report, and make complaints about, breaches of the services' terms of use.

Under item 16, the draft Determination states the additional expectation that online services will ensure they make readily accessible to end-users' information and guidance on how to make a complaint to the eSafety Commissioner.

We support this approach. However, we urge that these additional expectations include a requirement that online services make their reporting mechanisms accessible and meaningful to children, young people, and their parents and caregivers. This is in recognition of the developmental needs and vulnerability of young users and their low uptake of reporting mechanisms.

At present, children and young people are unlikely to report concerns to an online service. Surveys of Australian, British and American teens showed that only 8 - 14% of those who'd had a negative experience online reported it to the site where it happened. Children and young people are much more likely to block the offending account, ignore the problem, and / or confide in friends or family.[25]

Some children and young people don't use online reporting options because they are not upset or have found another solution. However, others don't report because they don't believe reporting will do any good.

They may fear that the online service won't respond effectively, or that bullying will continue in other spaces and get worse.[26]

We encourage online services to review and improve their reporting mechanisms through meaningful engagement with children, young people, parents and caregivers. This work could be done through partnerships between online services, research institutes, and organisations with expertise in trauma-informed and child-rights practice.

The improvement of reporting mechanisms should be guided by a primary focus on the best interests of the child. More specifically, the United Nations Committee on the Rights of the Child, General Comment No.25, states that reporting and complaints mechanisms for children should be safe, confidential, free, responsive, child-friendly, and available in accessible formats.[27]

Other possible approaches which could be explored with children, young people, parents, caregivers and researchers could include:

- tailoring the communication of reporting options to different age groups of children and young people. The UK Children's Code provides examples of how to do this
- enhancing reporting mechanisms so that a child who makes a report also receives an age-appropriate prompt encouraging them to speak to a trusted adult or support service as needed
- developing 'feedback loops' for online services to let children and young people know what actions are being taken in response to their reports. (See Australia's Safety by Design principles.) [28]
- publishing information each year, in an ethical, de-identified, age-appropriate way, about the numbers of reports the online service received, what they did in response, and the outcomes for users. (See Australia's Safety by Design principles.) [29]

Addressing and recording unlawful and harmful conduct and content

Under item 11, the draft Determination reiterates a core expectation of the Online Safety Act that online services will take reasonable steps to minimise provision of certain material:

- Cyber-bullying material targeted at an Australian child
- Cyber-abuse material targeted at an Australian adult
- A non-consensual intimate image of a person
- Class 1 material

- Material that promotes abhorrent violent conduct
- Material that incites abhorrent violent conduct
- Material that instructs in abhorrent violent conduct
- Material that depicts abhorrent violent conduct.

The Online Safety Act allows for removal notices to be issued to individual users who post such material to take it down or cease hosting it, with the potential penalty of 500 points (equivalent $110,000) for non-compliance.[30]

Under item 19, the draft Determination states an additional expectation that online services will keep records of reports and complaints about the above-listed matters for five years after the report is made.

We welcome swifter action to prevent and address harm to children and young people. In particular, we were pleased to see a provision in the Online Safety Act to enable faster intervention by the eSafety Commissioner in cases of image-based abuse and serious cyber bullying of children. In our own work, we have seen how devastating these issues can be. Cyber bullying of children, for example, can be especially distressing due to its potential to continue 24/7 across multiple platforms in front of large audiences, and the anonymity and disinhibition that can be involved.[31]

Harmful online activities and materials pose a particular risk to children and young people who are already vulnerable offline. This includes children and young people who live in out-of-home care, have a disability, live with chronic illness or mental health problems, suffer from eating disorders, or are young carers. Vulnerable children and young people are more likely than their peers to be cyber bullied, experience image-based abuse, and view violent or extremist content, amongst other risks.[32]

However, we also recognise that a lot of antisocial behaviour directed at children online comes from other children, and that those responsible have their own vulnerabilities.

For example, children and young people are at higher risk of cyber bullying others if they have social and psychological problems, such as poor relationships, loneliness, impulsive behaviour, low self-esteem, anger issues, and anti-social conduct offline.[33] Most young people who have behaved negatively towards others online (eg. calling names, spreading rumours, leaving someone out of things) say that they have also been treated negatively online themselves.[34] Furthermore, we know that risky and harmful experiences online tend to co-occur - eg. a young person who cyber bullies others is also more likely than their peers to be sharing nudes - so in some cases there are multiple concerns that need to be addressed.[35]

Therefore, we submit that antisocial behaviour by children online is unlikely to be resolved effectively by a heavily punitive approach that focuses only on an individual instance of harmful behaviour. We also urge caution in relation to storing and using data about antisocial behaviours by children online.

Historically, it has been a norm that children's actions should not follow them through their adult lives - for example, this is evident in the practice of expunging juvenile justice records. The Foundation supports the 'Raise the Age' campaign which is gaining momentum around Australia to lift the age of criminal responsibility to 14 years, rather than 10. A key principle behind this campaign is that children are still developing their cognitive, social, moral and emotional capabilities. As such, they should be treated differently to adults, even when their behaviour is antisocial or harmful. It is important to focus on rehabilitation, address the drivers of the behaviour, and set the child up to make positive, pro-social choices in the future.

If the Online Safety Act is to provide children with the same level of protection online that they enjoy offline, equivalent protections should also apply to children who have behaved antisocially online.

When children behave very antisocially online, we wish to see them linked to interventions that can support behavioural change and responsibility, address the child's circumstances holistically, and strengthen protective factors such as positive relationships, responsible adult supervision, fair and consistent educational setting rules, resilience, and self-efficacy. There must be structures and expert services in place to support this.

There is more work to be done to define what these approaches should look like. In the first instance, we urge that online services be guided by the best interests of the child as their primary focus, and by the United Nations Committee on the Rights of the Child, General Comment No.25, which states that:

- children may be alleged to have, accused of, or recognized as having infringed cybercrime laws. Parties should ensure that policymakers consider the effects of such laws on children, focus on prevention, and make every effort to create and use alternatives to a criminal justice response

- interference with a child's privacy is only permissible if it is neither arbitrary nor unlawful. Any such interference should be provided for by law, intended to serve a legitimate purpose, uphold the principle of data minimization, be proportionate and designed to observe the best interests of the child

- parties should protect children from cyberaggression and threats, censorship, data breaches and digital surveillance. Children should not be prosecuted for expressing their opinions in the digital environment, unless they violate restrictions provided by criminal legislation which are compatible with article 13 of the Convention on the Rights of the Child. (Article 13 states that children's right to freedom of expression may be subject to certain restrictions provided for by law which are necessary to protect other people's rights and reputations, and to protect national security, public order, and public health and morals.)[36]

Complementary actions to ensure positive outcomes for children

To ensure the best possible outcomes for children and young people, legislative and structural changes should be complemented by initiatives to build strength in early childhood settings, school communities, families, and support services. There should be a focus on Australia's most digitally excluded and disadvantaged families.

Antisocial behaviours online often occur between children and young people who know each other in person, typically at school. This leads many parents to go straight to the school expecting swift, effective action, which places great stress on both schools and families. Through our eSmart programs, Connect workshops, and our proud partnership with Dolly's Dream, we engage with thousands of students, parents and teachers each year. In our experience, families and educators are keen to learn more about other options for accessing support beyond the school (eg. reporting to eSafety). But many parents don't know much about these options and look to trusted educators to talk them through it. Moreover, school communities need the skills, resources and capacity to address the behavioural and relational issues between the students involved.

It is important to invest in ongoing support for school communities, including:

- high-quality educational resources which build students' digital literacies. For example, the Alannah & Madeline Foundation, informed by the Media Literacy Advisory Group, developed the Media Literacy Lab, an innovative, gamified education resource, which helps teach children how to think critically about their media experiences, create content responsibly, and be effective voices and active citizens online

- effective approaches to social and emotional learning which enable students to build empathy skills, recognise and respond to problems early, de-escalate situations where possible, and appropriately support peers who have experienced antisocial behaviour. (We recognise that young people often turn

to friends for support. The Youth Mental Health First Aid model might provide valuable lessons in how to build strength responsibly and appropriately.)

- meaningful partnerships between school communities and trusted providers of high-quality digital literacies education. (One-off information sessions and online resources, however valuable, are not enough.) It is our observation that schools which have positive long-term relationships with trusted providers are more likely to be engaged with the work of eSafety and developments like the Online Safety Act. In our experience, many schools would welcome more information about the Act, and have raised questions about topics including the relationship between eSafety and the police, the way new civil penalty systems will work, how the Act might affect teachers who have experienced online abuse, and how content and conduct from overseas will be handled under the Act.

Online safety education for children and parents, developed in dialogue with the eSafety Commissioner and delivered via a nationally consistent curriculum, would also align with Recommendation 6.0 of the Royal Commission into Institutional Responses to Child Sexual Abuse.[37]

Meanwhile, targeted interventions are needed to build the strengths, skills and support networks of our most digitally excluded and vulnerable families and the services that support them. It is the most vulnerable children and young people who are the most likely to have risky and harmful online experiences. They include children and young people living in out-of-home care, those dealing with eating disorders or physical or mental illness, those with disability, and young carers.[38] Vulnerable children and young people are less likely than their peers to have received cyber safety education that was useful to them; they are less likely to trust the guidance of adults; and they are more likely to have parents or carers with low digital skills.[39]

More work is needed to build the skills and supports of professionals who work with vulnerable children and teens, to address their needs, strengths and concerns online and offline. These professionals include youth workers, social workers, other allied health workers and school wellbeing staff.

We also encourage more investment in high-quality support for kinship carers, foster carers, and parents living in communities with low levels of digital inclusion, to better enable them to communicate regularly with children and young people about what's happening online; set clear, consistent and reasonable expectations; and support children and young people effectively if things go wrong. These interventions should be responsive to local circumstances, culturally appropriate, and built on trusting relationships.

Our partnership with Dolly's Dream, which works to change the culture of bullying through workshops, kindness activities, digital products and guidance to schools, parents and students, we have seen first-hand the particular need for appropriate support and strength-building in rural, regional and remote areas.

Finally, we stress that it is vital to measure and assess the impacts of the Online Safety Act for children, young people, parents and caregivers over the short and long term. The Online Safety Act represents significant and innovative steps to transform online safety standards; it will be vital to resource robust data collection, analysis and evaluation and share these findings with the whole community.

We would welcome the opportunity to discuss any of these matters further. Please contact Ariana Kurzeme, Director, Policy & Prevention, ariana.kurzeme@amf.org.au

[1] DQ Institute, '2020 Child Online Safety Index,' https://www.dqinstitute.org/child-online-safety-index/
[2] Australian Human Rights Commission and COAG, 'National Principles for Child Safe Organisations", 2018, https://childsafe.humanrights.gov.au/sites/default/files/2019-02/National_Principles_for_Child_Safe_Organisations2019.pdf
[3] Information Commissioner's Office, 'Age appropriate design: a code of practice for online services,' https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/age-appropriate-design-a-code-of-practice-for-online-services/7-default-settings/
[4] Justin Patchin, 'Tween Social Media and Gaming in 2020,' https://cyberbullying.org/tween-social-media-and-gaming-2020
[5] eSafety, 'Digital lives of Aussie teens', 2020, https://www.esafety.gov.au/about-us/research/digital-lives-aussie-teens
[6] 5Rights Foundation, 'Children Front and Centre: Fundamentals for a Child-Oriented Approach to Data Processing,' 2021, https://5rightsfoundation.com/uploads/5RightsDPCFundamentalsconsultationresponse.pdf
[7] Australian Centre to Counter Child Exploitation, 'Online Child Sexual Exploitation', Research Report, Feb 2020, https://www.accce.gov.au/resources/research-and-statistics/understanding-community-research
[8] 5Rights Foundation, 'Submission on Privacy and Children to the Special Rapporteur on the right to privacy', September 2020 , https://5rightsfoundation.com/uploads/5rights-submission-special-rapporteur-on-the-right-to-privacy.pdf
[9] 5Rights Foundation, 'Pathways: How digital design puts children at risk', 2021, https://5rightsfoundation.com/uploads/PathwaysSummary.pdf
[10] eSafety Commissioner, 'Safety By Design: Principles and Background', https://www.esafety.gov.au/about-us/safety-by-design/principles-and-background
[11] Australian Human Rights Commission, *National Principles for Child Safe Organisations*, 2019, https://childsafe.humanrights.gov.au/national-principles
[12] Victorian Children's Commissioner, 'Child Safe Standards: Who do the Standards apply to?' https://ccyp.vic.gov.au/child-safety/being-a-child-safe-organisation/the-child-safe-standards/who-do-the-standards-apply-to/
[13] eSafety Commissioner, 'Safety By Design: Principles and Background'
[14] United Nations Human Rights, Office of the High Commissioner, Committee on the Rights of the Children, 'General Comment on children's rights in relation to the digital environment,' 2021, https://www.ohchr.org/EN/HRBodies/CRC/Pages/GCChildrensRightsRelationDigitalEnvironment.aspx
[15] 5Rights Foundation, April 2021, Ambitions for the Online Safety Bill, https://5rightsfoundation.com/uploads/Ambitions_for_the_Online_Safety_Bill.pdf. Also 5Rights Foundation, 'Pathways: How digital design puts children at risk'
[16] eSafety Commissioner, 'Safety By Design: Principles and Background'
[17] United Nations Human Rights, Office of the High Commissioner, Committee on the Rights of the Children, 'General Comment on children's rights in relation to the digital environment'
[18] United Nations Human Rights, Office of the High Commissioner, Committee on the Rights of the Children, 'General Comment on children's rights in relation to the digital environment'
[19] The UK Children's Code or Age Appropriate Design Code, https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/age-appropriate-design-a-code-of-practice-for-online-services/
[20] United Nations Human Rights, Office of the High Commissioner, Committee on the Rights of the Children, 'General Comment on children's rights in relation to the digital environment'
[21] 5Rights Foundation, 'Ambitions for the Online Safety Bill'; 5Rights Foundation, 'Submission on Privacy and Children to the Special Rapporteur on the right to privacy', 2020, https://5rightsfoundation.com/uploads/5rights-submission-special-rapporteur-on-the-right-to-privacy.pdf
[22] CSA Group, 'Children's Safety and Privacy in the Digital Age,' 2020, https://www.csagroup.org/wp-content/uploads/CSA-Group-Research-Childrens-Safety-and-Privacy-in-the-Digital-Age.pdf
[23] The UK Children's Code or Age Appropriate Design Code
[24] eSafety Commissioner, 'Safety By Design: Principles and Background'
[25] Ofcom, 'Online Nation: 2021 Report, UK', 2021, https://www.ofcom.org.uk/__data/assets/pdf_file/0013/220414/online-nation-2021-report.pdf; Office of the eSafety Commissioner, 'State of Play: Youth, Kids and Digital Dangers,' 3 May 2018 https://www.esafety.gov.au/sites/default/files/2019-10/State%20of%20Play%20-

%20Youth%20kids%20and%20digital%20dangers.pdf; Justin Patchin, 'Teens Talk: What Works to Stop Cyberbullying,' Cyberbullying Research Centre, https://cyberbullying.org/teens-talk-works-stop-cyberbullying
[26] For example Ofcom, 'Children's Media Lives - Wave 6', 2020, https://www.ofcom.org.uk/__data/assets/pdf_file/0021/190524/cml-year-6-findings.pdf
[27] United Nations Human Rights, Office of the High Commissioner, Committee on the Rights of the Children, 'General Comment on children's rights in relation to the digital environment'
[28] eSafety Commissioner, 'Safety By Design: Principles and Background''
[29] eSafety Commissioner, 'Safety By Design: Principles and Background'
[30] Commonwealth Government, Online Safety Act 2021, file:///C:/Users/jessie.mitchell/Downloads/C2021A00076%20(3).pdf . Penalties calculated using Australian Competition and Consumer Commission, 'Fines and penalties', https://www.accc.gov.au/business/business-rights-protections/fines-penalties and Australian Securities & Investments Commission, 'Fines and penalties', https://asic.gov.au/about-asic/asic-investigations-and-enforcement/fines-and-penalties/ . Figure of $110,000 confirmed by ABC, 'New laws introduced to protect people from extreme online abuse, trolls,' 15 June 2021, https://www.abc.net.au/news/2021-06-15/new-laws-esafety-online-abuse-penalties-trolling/100217376
[31] David Smahel, Hana Machackova,Giovanna Mascheroni, Lenka Dedkova, Elisabeth Staksrud, Kjartan Ólafsson,Sonia Livingstone and Uwe Hasebrink, 'EU Kids : Online 2020, Survey results from 19 countries,' 2020, https://www.lse.ac.uk/media-and-communications/assets/documents/research/eu-kids-online/reports/EU-Kids-Online-2020-10Feb2020.pdf
[32] Adrienne Katz and Dr Aiman El Asam, 'Refuge and Risk: Life Online for Vulnerable Young People', Internet Matters, 2021, https://www.internetmatters.org/about-us-3/refuge-and-risk-report/
[33] For example, Cyberbullying Research Centre, 'Cyberbullying Facts', https://cyberbullying.org/facts ; Sheryl Hemphill, Aneta Kotevski, Jessica A Heerde, 'Longitudinal associations between cyber-bullying perpetration and victimization and problem behavior and mental health problems in young Australians,' *International Journal of Public Health*, vol.60, no.2, Feb 2015; Sara Pabian and Heidi Vandebosch, 'An investigation of short-term longitudinal associations between social anxiety and victimization and perpetration of traditional Bullying and Cyberbullying,' *Journal of Youth and Adolescence*, vol.45, 2016; Y. Rodríguez-Castro, R. Martínez-Román, P. Alonso-Ruido, A. Adá-Lameiras, M.V. Carrera Fernández, 'Intimate Partner Cyberstalking, Sexism, Pornography, and Sexting in Adolescents: New Challenges for Sex Education,' *International Journal of Environmental Research and Public Health*, vol. 18, Iss. 4, 2021; Mariya Stoilova, Sonia Livingstone and Rana Khazbak, 'Investigating Risks and Opportunities for Children in a Digital World: A rapid review of the evidence on children's internet use and outcomes,' UNICEF Innocenti Discussion Paper 2020-03, 2021
[34] Office of the eSafety Commissioner, 'State of Play: Youth, Kids and Digital Dangers'
[35] Rodríguez-Castro et al, 'Intimate Partner Cyberstalking, Sexism, Pornography, and Sexting in Adolescents: New Challenges for Sex Education'; Adrienne Katz and Aiman El Asam, 'Look at me: Teens, sexting and risks', Internet Matters, 2020, https://www.internetmatters.org/about-us-3/sexting-report-look-at-me/ ; Stoilova et al, 'Investigating Risks and Opportunities for Children in a Digital World'; Becky Mars, David Gunnell, Lucy Biddle, Judi Kidger, Paul Moran, 'Prospective associations between internet use and poor mental health: A population-based study,' *PLoS One*, vol. 15, Iss. 7, Jul 2020; Johanna M F van Oosten, Laura Vandenbosch, 'Predicting the Willingness to Engage in Non-Consensual Forwarding of Sexts: The Role of Pornography and Instrumental Notions of Sex,' *Archives of Sexual Behavior*, Vol. 49, Iss. 4, May 2020
[36] United Nations Human Rights, Office of the High Commissioner, Committee on the Rights of the Children, 'General Comment on children's rights in relation to the digital environment'
[37] Royal Commission into Institutional Responses to Child Sexual Abuse, 'Final Report: Making Institutions Child Safe,' vol 6, Commonwealth of Australia, 2017, https://www.childabuseroyalcommission.gov.au/sites/default/files/final_report_-_volume_6_making_institutions_child_safe.pdf
[38] Katz and El Asam, 'Refuge and Risk: Life Online for Vulnerable Young People'
[39] Katz and El Asam, 'Look at me: Teens, sexting and risks'; Katz and El Asam, 'Refuge and Risk'; Adrienne Katz and Aiman El Asam, 'Vulnerable Children in a Digital World', Internet Matters 2019, https://www.internetmatters.org/wp-content/uploads/2019/04/Internet-Matters-Report-Vulnerable-Children-in-a-Digital-World.pdf