alannah & madeline foundation

Ground Floor, 387 City Road
South Melbourne VIC 3205
Postal address
PO Box 5192
South Melbourne VIC 3205
Phone 03 9697 0666
Email info@amf.org.au
ABN 96 514 115 810
alannahandmadeline.org.au

'The internet needs fixing': Children and Young People's Vision for Australia's Digital Duty of Care, 2026

Children and young people have clear views about the digital world they want: one that is safe, trustworthy, truthful, respectful and designed to support learning, connection and enjoyment. The Alannah & Madeline Foundation shares their experiences and ideas to help shape a Digital Duty of Care for Australia.

This report draws on consultations about online safety and privacy with more than 800 primary, secondary and tertiary students between 2024-26. We focused particularly on primary students, whose insights are too often overlooked. Six recent sessions explored the Digital Duty of Care directly. Attributions and methodology available on request.

Children described using a wide range of online services, including generative AI, prolifically from a very young age. When primary students were asked what the internet should be like, their replies included *'Safe', 'Trustworthy', 'Truthful', 'Respect', 'Learning', 'Social interaction', 'Integrity', 'Responsibility'*. These values provide a child-centred test for the Digital Duty of Care: does the design of an online service help children experience the internet in these ways?

The experiences of children show a persistent and widening gap between that positive vision and the online environment they encounter. They value the opportunities to learn, play and connect, but also describe risks and harms created or intensified by design and operational features including chatbots, endless scrolling, recommender systems, deepfake tools, low-privacy settings, targeted advertising, weak enforcement of conduct rules, and safety tools they cannot trust.

Children and young people were direct about what is missing. One concluded *'Our rights to protection from harm and data collection and privacy aren't in place'*. A secondary student at a specialist school put it directly: *'The internet needs fixing'.* Their contributions did more than identify problems: they offered practical ideas for safer design, meaningful choice, accessible support and stronger accountability.

Children and young people's vision for a better digital world

Primary students want the digital environment to offer the protections and positive experiences they expect offline: peer friendships, age-appropriate entertainment, reasonable support and supervision from parents/ carers, protections from strangers, and enforcement of criminal law and clear rules against bullying and other harmful behaviour.

Secondary and tertiary students brought a more critical understanding of how platforms operate. They called for services to prevent and mitigate harm by design and to give young users genuine, clear choices about what they see, share and experience.

Across age groups, students identified six priorities for reforms:

1. **Design for positive childhood experiences.** Children want online services to be enjoyable, safe, age-appropriate and enhancing with boundaries that reflect those responsible adults set offline. (See exposure draft 25F, 25G)

2. **Protect children wherever they spend time online.** The duty should cover the wide range of services children use, including generative AI. (See exposure draft 25A)
3. **Address the full range of harms children experience.** Children describe harms across the domains of contact, content, conduct, contract and compulsion. (See exposure draft 25C, 25D)
4. **Make safer choices at the design stage.** Children identified risks in recommender systems, endless-feeds, low-privacy settings, contact with strangers, age-inappropriate advertising, and AI features that imitate people or misuse children's images or data. (See exposure draft 25F, 25G)
5. **Give children tools they can find, understand and trust**. Safety and reporting tools should be easily accessible (including for students with disabilities), respond quickly, explain processes and outcomes clearly, connect children to further support, include human oversight, and encourage help-seeking from trusted adults. Children cautioned against describing help-seeking as a 'complaint' and reported that trust in user tools is low. (See exposure draft 26)
6. **Explain reforms to the people they affect.** Children, young people**,** parents, carers and educators need clear information about what will change, and what protections cannot guarantee, so reforms build informed trust rather than complacency.

The digital services that are shaping children's lives

Children and young people told us they used digital technologies from a very young age. Lower primary students used devices including tablets, laptops and XBOX. Gaming was very popular, ranging from family-friendly games like Uno to age-inappropriate ones like Fortnite, with some students using chat functions. Students used search engines, educational apps and YouTube.

Upper primary students described expanded tech use, with many having received their first smart phones or smart watches. Gaming remained very popular eg. Minecraft, Roblox, Mario Kart. There was a rise in use of messaging services including Messenger Kids, iMessages, WhatsApp and Discord, social media like TikTok, Instagram and Snapchat, and live-streaming platforms like Twitch. Students used educational technologies, shopping platforms, music apps like Spotify, smart home systems, and location apps like Life360.

Generative AI was also used by upper primary students, who mentioned ChatGPT, Gemini, AI Overview (Google), My AI (Snapchat), AI character apps like PolyBuzz and Talkie, the Kmart shopping bot, a Fortnite chatbot, and a mental health chatbot.

Secondary and tertiary students adopted new educational and health/fitness technologies as well as gaming, messaging, social media and, frequently, AI eg. Gemini, ChatGPT, Claude, Grok, Character AI, Siri AI.

What children and young people experience as 'harm'

Many students had seen disturbing content. Upper primary students told us of their concern about *'inappropriate photos / videos'*, especially 'gore' videos: '*Extremely violent and bloody'*, '*Disturbing'*, '*Insides'*. Secondary students also worried about violence and gore and its long-term impacts on younger children.

Contact risks were also raised repeatedly. Lower primary students worried about 'stranger danger' online: '*We could talk to strangers which is not good'.* Upper primary students warned of *'getting contacted by random people', 'creeps looking at you', 'your location being shared and tracked'.*

By secondary school, contact with strangers online was described as a regular (eg. weekly) occurrence. Students described online pestering and sexual harassment as common, especially for girls. One student remarked *'In real life you can call the police but online there isn't anyone controlling'*.

Poor conduct by peers was raised as a concern, too. Upper primary students objected to swearing and to '*mean people'*, '*hate comments'*, '*BULLYING'.* Secondary students at a specialist school described '*Messages – cyber bullying*' and '*Threats online, like you are the next person to get blah blah blah*'. Secondary students also warned of a rise in people creating *'harmful AI videos'* to bully others.

Meanwhile, students of all ages worried about cybercrime, including scams, hacks and identity theft.

How children and young people experience risk

Some content risks reported by upper primary and secondary students related to design elements like endless-feed features and recommender systems. Their comments included:

- '*Like I was on YouTube before the under 16 ban was on and I searched up AFL highlights because I'm allowed on YouTube still, but only for sport highlights, my mum said. And then I searched up AFL and it came up with like, how to kill yourself and suicide stuff.*'
- '*While you're scrolling, you can see videos of people saying if you don't subscribe, your family will die and stuff.... And like little kids believe it and they have to subscribe.'*
- *'Videos that come up that I don't like – girl videos*'.

Some secondary students also raised content risks relating to high-volume age-inappropriate advertising, noting that they were regularly shown ads for gambling and dating services.

Risks are also attached to design features which encourage communication. Students described risky experiences on platforms which show children's profiles to other users or enable users to contact people anonymously without consent, send ephemeral messages, or use voice-changer tools. Some students used their parents' accounts, which could mean further interaction with adults. We asked three groups of upper primary students to respond to a scenario where a student joins a messaging app to talk to friends but starts getting messages and calls from strangers. The majority felt this situation was unfair.

Other design features function to maximise engagement. Some primary students told us of games and apps whose function was *'brainrot'*, while secondary students debated whether it was OK to spend hours scrolling short videos, gaming or messaging, as many did. We invited three groups of upper primary students to respond to scenarios where children are bombarded with content based on things they have 'liked' before. Students grappled with this, disagreeing over whether the situation was fair, unfair or 'middle'.

Secondary and tertiary students were better able to articulate the quandary: personalised design and targeting make online services convenient and enjoyable but also invasive and compulsive. Students liked being shown content that matched their interests but worried about being 'sucked in' by inauthentic content or drawn into echo chambers based on personal biases: *'don't trust the algorithm'*.

One student said *'I never had the intent to scroll on these platforms, it just becomes some sort of habitual behaviour that occurs without conscious awareness. I'll go on Instagram with the intent of texting my friend, 20 minutes later I'll still be scrolling.'* [sic]

Generative AI prompted debate, too. Primary, secondary and tertiary students find AI a very useful source of ideas, information, advice and study support. However, they also raised concerns about safety, wellbeing, accuracy, data security and environmental risks.

Some students warned of the loss of privacy: '*random AI following accounts and skimming account for pictures'*, '*selfies or stolen data used for AI'*. Others worried about peers becoming reliant on chatbots, warning that they were building relationships with AI and becoming isolated from other people.

Children and young people's ideas for safer design

While most students were comfortable with family and friends contacting them or seeing their location with permission, they wanted action to stop inappropriate contacts: '*Protection from child pred'*. One student drew her vision of a better internet: a happy girl inside a '*safe bubble'* and a creepy man locked out. Ideas included:

- *'chats with unknown people get blocked'.*
- *'Private server for friends'.*
- *'feature to block users based on age and gender'.*
- *'Roblox – only people of the same ages can play together.'*
- '*Snapchat – remove the map feature, verify you are adding people you know'.*
- *'All messenger apps are to make sure that you are only allowed to talk to people that you know'.*

- *'If you add someone, it sends a message to, like, the parents to ask, and then it also asks you if you want to add them, and it asks their parents if you want to add them.'*
- *'You cannot message people unless you have added them on the app/game'.*
- *'on certain games people can only join you if you have alowed them to.'* [sic]
- *'TikTok ... I would make a face scanner (like roblox) to put you into age groups in the app. This would prevent some hackers and old people you dont know from reaching you.'* [sic]

Other primary students imagined new online safety features which would bar people who have played '*scary horror games'* from playing on Roblox with children, require students to get parental approval to unblock someone, and show exact usernames only in searches to stop students accidentally adding the wrong people.

Meanwhile, primary students wanted to have fun while being protected from age-inappropriate content and language. Their ideas included:

- *'Child friendly – no gore – no violence – no coarse language'*.
- *'Putting people in age groups so they can see content made by their age.*'
- *'Make sure content is right for the age. For scary content, require a password protection and two-factor authentication'.*
- *'Maybe we could make rules for age group like riding a bike or a scooter*.'
- *'Maybe we could make like a kid Youtube not like kids youtube but like middle since we are getting older'.*
- *'[On YouTube] I'd automatically get rid of any hate comments and inappropriate photos/videos.'* [sic]
- '*YouTube: make it be able to detect if there is something bad on a video. have a strict policy so no swear words.'* [sic]
- *'[On Snapchat] I would also add a feature for parents or all people in general to get content BANs and Restrict certain types of content so it is unaccessible to kids*'. [sic]

Primary students also wanted aggression and swearing at children to be reprimanded promptly or stopped before other people are affected. Their ideas included:

- *'bad words get deleted as soon as written'.*
- *'Instant ban for trash talking'.*
- *'if they say like, like a naughty, naughty word, like, it'll block it out kind of like on the Roblox chat'.*
- *'If I was in charge of Fortnite for a day I would make [it] ... so if you say something insulting or rude to another player you get banned for 2 days'*
- *'if you cheat Hack or be mean you are banned from the game or app forever'.*
- *'If someone or bot is being inprotate [inappropriate] or mean delete it straight away'.*
- *'Messenger Kids: When anyone messages you an inappropriate message or one that is rude the app (messenger kids) deletes it immediately. When you get a new friend request if that friend has messaged something rude to someone else the friend request tells you that, that friend has been mean to other people before.'*

Secondary and tertiary students wanted online services to make more responsible choices and give young users more options to improve their experiences. They commented:

- *'I think social media should implement a setting that disables the scroll feature of the platform'.*
- *'the ability to filter out content, or types of content, that you are seeing before you can see it'.*
- *'ability to opt out of content'.*
- *'a way to edit your own feed – if you do or don't want to see things about politics or lifestyle / diet etc'.*
- *'content descriptors are mandatory, regulated and can be blocked'.*
- *'could be beneficial to be able to tailor your own feed in a different way – this could help with the problem of doom scrolling'.*
- '*Warning young people about harmful post or audios before putting anything online*.'
- '*age ranges like YouTube Kids.'*
- *'a kid friendly version of each platform, and then the data is transferable when they age up'.*
- *'for people under 20, restricting comments to none or maybe having a bot filter out (not hide them but completely delete them) comments perceived as negative'.*
- *'the user has to complete a certificate on digital safety education'.*

Meanwhile, students of all ages expressed a strong appetite for stricter regulation of generative AI, which they believed should help and improve everyday life, not dominate or endanger it. Their ideas included:

- *'Make sure you know if you are using AI chatbots.'*
- *'don't let AI take images and data'.*
- *'list to make chatgpt safer: – deleting all photos and questions in previous and new chats – not keeping personal information – stop sucking people in with asking questions with their algorithm – not needing to sign in with your email and name'.*
- *'Roblox ... no ai vosi [AI voices]'.*
- *'block any ai content from being posted on social media'.*

Tools that children and young people can find, use and trust

Upper primary students told us that tools for safety, privacy and reporting should be easy to find and use, explain things briefly and clearly, receive a swift response, be overseen by people (not bots), and not frame students' help-seeking as a 'complaint', as students have been taught that complaining is bad behaviour. Some students also wanted inbuilt mechanisms which would alert their parents to a problem.

Secondary students, similarly, told us that reporting and safety tools should link to other sources of help and be accessible, trustworthy and easy, especially for students with disabilities, whose needs have often been overlooked. Students called for '*Block button – a clear one'*, '*Include speech to text'*, '*awareness of esafety commissioner website'.*

However, many students do not trust user safety tools. Upper primary students were sceptical about whether reporting to a platform was worthwhile, and secondary students tended to see reporting as ineffective, citing limited feedback, no clear outcomes, and different approaches between different platforms.

Students also had mixed experiences of online tools for parental supervision. Primary students tended to accept parental decision-making as a normal part of online safety eg. asking parents before playing a new game or using a new app. However, they also recognized that parents could not prevent all problems, citing differences between divorced parents and children not following parental rules or forging parental permission.

Secondary students wanted support and guidance from parents and carers, but they rarely mentioned parental tools; most seemed to assume that students would evade them or that parents would be unable to use them.

Children and young people warn: safer systems must not create false confidence

Listening to students revealed the strong, positive potential of a Digital Duty of Care and the importance of involving children and young people as reforms are designed, implemented and reviewed. Their experiences also warn against over-promising. The uneven start to the social media age delay has left many young people cynical about measures which rely on age assurance.

Conversely, there are risks of complacency eg. the risk that children and adults will assume online services are safe because the services have a legal duty of care or have made changes which 'feel' child-friendly. For example, some primary students assumed the presence of age assurance meant it was safe to interact with strangers in games: '*Age verification proves they are 9–10*.'

A Digital Duty of Care should be judged by whether children and young people experience meaningful improvements in safety, privacy, agency and enjoyment online. Their voices should continue to shape standards, guidance, implementation and evaluation. We would be delighted to discuss these insights further.

Please contact:
Sarah Davies AM, CEO, sarah.davies@amf.org.au
Ariana Kurzeme, Director, Policy & Prevention, ariana.kurzeme@amf.org.au
Dr Jessie Mitchell, Manager, Advocacy, jessie.mitchell@amf.org.au