



alannah &
madeline
foundation



Children's Voices and the Digital Duty of Care

January 2026

For their right to be safe

Executive summary

This report responds to the 2025 consultation to inform the drafting of a Digital Duty of Care under the Online Safety Act 2021, led by the Department of Infrastructure, Transport, Regional Development, Communications, Sport and the Arts (the Department).

To ensure children's voices are heard, the Alannah & Madeline Foundation (the Foundation) gathered insights from primary school students – those who use digital technologies daily and are among the most vulnerable to risks and harms online.

Our insights are drawn from three consultation processes involving 406 students overall (see **Method** for details).

High-level findings may be summarised as follows:

- **Digital access is near universal** with almost all primary students using digital devices, most commonly tablets.
- **Gaming and watching videos** are the most popular online activities.
- **Social interaction is common** – many students connect with others online, often via the chat function in games.
- **Technology use grows with age** – older primary students describe using a wider range of digital products, including some designed for older audiences.
- **Children recognise risks despite positive views** – while most see technology as fun and helpful, they are aware of dangers such as contact with strangers, security breaches, exposure to 'scary' content, scams, loss of private information, impulsive or risky purchases, too much screentime, and bad behaviour like swearing.
- **Direct interaction drives risk** – most platforms flagged as unsafe by students allow for direct interaction between users.

While primary students tend to frame these risks in terms of bad people (scammers, stalkers, bullies, strangers) rather than system-level problems, they have strong ideas about what safer platforms should look like.

Children imagine digital spaces where safety is built in and by default, not left to them or to chance. Their vision includes platforms where:

- **privacy and security settings are strong and simple** for children to use
- **personal details stay private** – children's location and identifying details are protected
- **unwanted contact is blocked** – children cannot be seen or contacted by strangers
- **help is easy to access** – clear options to block, report concerns and ask for support
- **content and conduct are respectful** – no exposure to offensive language, bullying or anti-social behaviour
- **parents can supervise effectively** – especially around contacts and location
- **money is safe** – no pressure or tricks to spend, and no risky purchases
- **ads do not intrude** – children aren't forced to watch advertising.

Students see system-level risks as most unfair when they involve intrusive / unwanted contact from strangers or loss of control over money or personal information.

When things go wrong online, children turn first to the people and systems they trust. Most students said that their rules come from parents, teachers and the 'settings' on their devices. Most primary students welcome online safety education in school and view it positively.

Overall, students tend to be most familiar with online safety rules concerning stranger danger, cyber security, bad behaviour (eg. swearing) and time limits. Understanding varies by age: younger students'

understanding of the rules is limited, while older students understand them better, but remain vulnerable to risks and harms. Common rules include:

- don't add random people
- don't share phone numbers or personal details
- avoid swearing so you don't get banned
- follow app rules and age limits
- take breaks and stick to time limits
- no devices in bedrooms or behind closed doors.

Students also described practical strategies: reporting or blocking strangers, skipping ads, and checking reviews before downloading apps. Some even invent creative solutions like using fake details when asked for personal information.

Parental influence is critical. Children whose parents regularly talked to them about privacy and safety often mirror those attitudes and behaviours. For example, some students said their parents set up app restrictions or taught them to research apps before downloading. Others mentioned learning to spot scams or avoid risky links because of parental guidance.

Despite these efforts, students recognised that staying safe online can be hard. They want platforms to share responsibility by making safety simple and automatic – rather than leaving it entirely to children or their families.

Method

This report presents findings from a dedicated workshop about a Digital Duty of Care led by our eSmart team at a Catholic school in Melbourne.

Held in December 2025, the workshop engaged 26 students – eight in Grade 3, five in Grade 4, and 13 in Grade 5.

Our eSmart team designed interactive classroom activities to explore key topics raised by the Department, including:

- students' favourite online activities and platforms
- students' thoughts about online harms
- students' views on how platforms could be made safer and more responsible
- sources of support for online problems.

Students all had parental permission to participate, with information about the workshop provided in advance to parents and guardians. Staff, including the school principal, were present throughout. A summary document of the workshop's findings will be provided to the school to prompt wider discussion in the school community. The Foundation also used this opportunity to forge a stronger connection between the educators and their eSmart Advisor.

Further perspectives have been drawn from two recent consultations and can be found under the 'What else have students told us?' section. These additional insights came from:

- **small group sessions** with 56 primary students (Prep to Grade 6) across seven Victorian communities led by Lewers Research for the Foundation in May 2025 to inform the Privacy Commissioner's plans for a Children's Online Privacy Code.
- **co-design workshops** with 324 lower primary students (Foundation / Prep to Grade 3) in four schools across Victoria, Tasmania, South Australia in 2024 led by the eSmart team to explore student's ideas about positive digital citizens and technology use.

About us

As a leading national not-for-profit charity dedicated to keeping children and young people free from violence and trauma, the Alannah & Madeline Foundation supports young Australians to recover and heal from trauma and empowers them to become positive digital citizens.

Our eSmart Program offers learning tools and resources, aligned to the curriculum and free for all Australian schools, to help students build online safety and digital and media literacy skills and behaviours to thrive online.

We also advocate for children's rights in legislation, regulation, systems and policy, notably in the digital environment.

Our vision is that all children and young people are safe and inspired with the freedom to flourish.

What do primary students do online?

School workshop findings

Students were asked to imagine that they had a 'digital backpack': what kinds of digital things did they use or play with in a normal week?

Responses were arranged into technology type, and the most popular devices were identified.*

Type	Product
Communication	Discord, Messenger Kids, TikTok, Snapchat, Messenger, WhatsApp / Messages, YouTube (not YouTube Kids), X
Education	Bible App, Reading Eggs, Vinci Bot (coding), Sunshine Online
Creativity	Canva, Gallery (photos), Stop Motion, Dragon Flame 25, iMovie (not to post, just to save to gallery)
Games	Minecraft, Roblox, Clash Royale, Zelda, Blockaduku, Sonic, Mario Kart, Pokemon
Streaming	Spotify, YouTube Music, Kayo Sports, Twitch
Shopping	Temu, Shein
Other	Google, Safari, Yelp, Bump, Tinder

Devices	Devices – most used
Chromebook	iPad x 6
Laptop or PC	iPhone x 5
PS5	TV x 4
Nintendo Switch	Laptop
iPad	PS5
Phone – iPhone	
Smart keyboard and smart mouse	
Tablet	
VR headset	

One student reflected on devices used within the school settings: *'Juniors and Preps are using iPads and the older kids are using Chromebooks.'*¹

* Note: some apps listed would be highly inappropriate for primary students to use. It was the eSmart team's impression that students mentioned these apps because they had heard of them, rather than used them personally. The classroom discussion did not allow for detailed discussion, but educators, including the principal, were present and undertook to follow up on relevant matters raised.

What else have students told us?

Through co-design sessions, 324 lower primary students told us:

- digital tech use is high. For example, all Years 1-3 students had used a tablet.
- students' feelings about tech are mostly positive. 77% agreed *'The internet is fun and we like going online'*.
- gaming is the most popular activity. All Years 1-3 students had played a game online and 77% of Foundation / Prep students said they knew where and how to download games.
- Minecraft and Roblox were mentioned often.
- many students interact with other people in games. One in three Foundation / Prep students said they had used the chat function in a game, and many students said they had lots of friends in Roblox.
- YouTube is also very popular. 78% of Foundation / Prep students had watched a YouTube video and 36% had commented on a video.²

Through small group consultations, primary students told us:

- children go online regularly. Amount of time online tends to increase with age.
- most students have access to a tablet and occasionally to parents' smartphones.
- younger students watch smart TV or YouTube Kids or play simple games on tablets.
- older students play games, chat with friends, watch content, play educational games, and do research for homework.
- Grades 3 and 4 are key times for increased tech use.
- Grades 4, 5 and 6 students may have smartwatches or their own phones. This often coincides with being allowed to walk home alone or go to the park unsupervised. Parents being able to track location is an important driver of purchasing the device.³

A survey of 1,000 Australian parents and carers of primary aged children confirmed that digital device use is almost ubiquitous – for example, 84% of Prep students used tablets, 45% used smartphones (their own or someone else's), 34% used gaming consoles, and 34% used laptops.⁴

Foundation / Prep, Year 1 and Year 2 students told us:

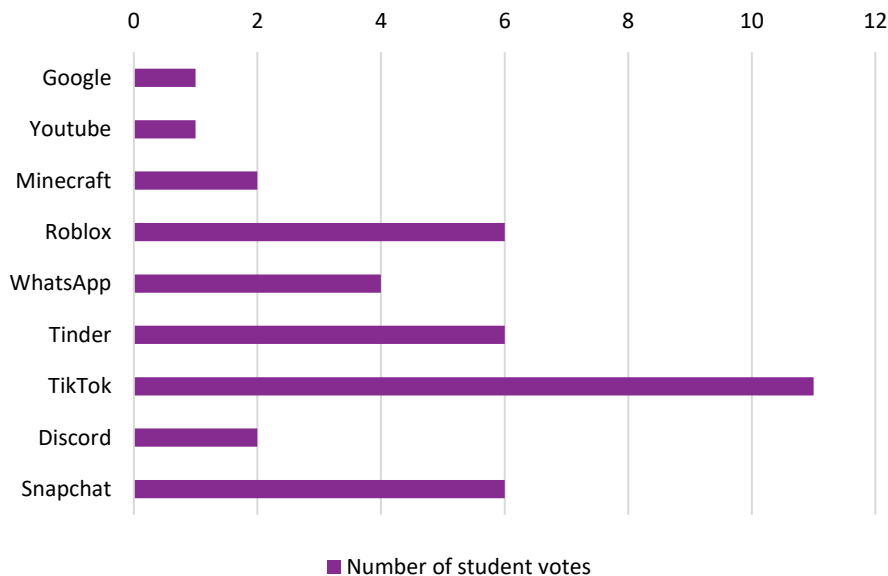
- *'Games are really fun.'*
- *'I watch Kids YouTube and listen to music.'*
- *'It [digital tech] helps you learn and is really fun.'*
- *'So that I can text my parents.'*
- *'I am a Roblox hacker.'*
- *'I play by myself on my phone.'*
- *'Getting to play games with people you don't know and making friends.'*⁵

What risks and harms do primary students experience online?

School workshop findings

After mapping the digital technologies students used in a typical week, we asked them to vote on which platforms felt the least safe. The results were striking; many of the apps and sites students used most were also those they considered the riskiest.

What platforms and apps are least safe?



For example, some students discussed why and how students add strangers on WhatsApp, with comments including *'they hide from their parents'*, *'parents don't know'* and *'they have seen a number somewhere and added it'*.

When asked about the safest digital platforms, students' responses included:

- *'Canva as it is just you inside your own world.'*
- *'Messenger kids because you get a specific code, can write their [your friends / people you want to add] name down and you can block them.'*
- *'Kids Helpline – getting an answer from a specialised adult.'*¹⁶

What else have students told us?

Through co-design sessions:

- 24% of lower primary students agree 'Kids feel worried, scared or nervous going online'
- older students had greater understanding of online risk and harm than younger students
- risks listed by students included contact with strangers, security breaches, inappropriate or scary content, and giving out personal information.⁷

Grades 1 to 3 students told us:

- *'Games can be scary.'*
- *'People might be unkind.'*
- *'Someone might want to scam me or trick me.'*
- *'You have to be careful of people you don't know when playing online.'*⁸

Through small groups consultations, primary school students told us:

- students in Foundation / Prep and Grades 1 and 2 know some rules about stranger danger and avoiding bad behaviour like swearing. But their understanding is limited.
- by Grades 3 and 4, students know more. These older students mentioned scams, identity theft, risky purchases, too much screentime, and people who swear, behave badly, ask for contact details, or watch children online without permission.
- apps that students associate with stranger danger include YouTube, multi-player games like Roblox and Minecraft, and messaging services like Messenger Kids and WhatsApp.
- students also mentioned financial risks on shopping sites like Temu and Shein.
- most students think of online risk in terms of dangerous individuals eg. scammers, bullies, strangers. They have little awareness of systemic risks eg. targeted content, 'infinite scrolling'.⁹

Grades 5 and 6 students told us:

- *'I was on Fortnite with my friend... and then someone we didn't know came in and he just started swearing at us.'*
- *'I almost got scammed once. My dad stopped me last second. I was like seven. I was gonna click on a link because it said, get free Robux.'*
- *'Gemma went to school and she posted something on Snapchat and then all of her friends made fun of it.'*
- *'I was playing with my friend and there was this person who joined the game and he said he was the same age as us, and he said, oh, do you love dogs? And I'm like, yeah. And he's like, I love dogs too. We might be best friends. And he pretended to be my friend, but I knew he actually wasn't. And I knew he was like much older than me, like high school.'*¹⁰

Are there any features of digital platforms that primary students would like to change?

School workshop findings

Students were asked *'If you were the CEO of a Big Tech company, such as TikTok what would your rules be from your first day?'* Their responses were:

- *'Google – not searching up inappropriate stuff and age verification.'*
- *'TikTok – not rude or bullying.'*
- *'Nintendo – app connected to parents' phone where they can see what you are doing.'*
- *'YouTube – age limit where they let you verify your age.'*
- *'Delete swears – doesn't show on other people's chats.'*
- *'Temu – wouldn't let you buy anything with your mum's credit card.'*
- *'Snapchat – remove the map feature, verify you are adding people you know.'*
- *'Parental controls.'*
- *'Roblox – only people of the same ages can play together, if you are younger you should only be able to play with younger people and if you are older you should be able to play with older people, and if you want to play with an older person as a younger person, your parents should verify you know them in real life.'*
- *'Roblox – chat to people you know and swears equal ban.'*

Other anecdotes from students:

- *'I would like there to be no ads, once my dad saw a weird ad on my iPad when I wasn't on it.'* (Emphasised use of the word 'weird'.)
- *'We don't know if it is a friend or family member contacting us.'*
- *'If you watch too many swearing videos, you might get addicted to swearing as well.'*
- *'My friend had enough Robux, but it made him use real money.'*
- One student spoke about how their friend is in a long-distance relationship and social media enables them to maintain that connection

One of eSmart team members observed that students frequently used terms such as 'age verification' and 'parental controls' to describe what safety looks like on apps and digital platforms. This language, not commonly used terms a year ago, now appears to be widely adopted - though it remains unclear whether students fully understand what these measures involve or how they are actually work to keep them safe.

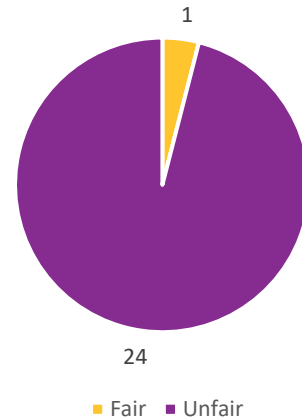
Students then took part in an activity called 'Fair or Unfair?' They were given scenarios involving system level online risks and asked to vote on whether each situation was 'Fair', 'Unfair' or 'Middle'. Some added comments to explain their views. (Original spelling retained.)

Our team noted a clear pattern: students were most likely to view a scenario as systemically unfair when it involved intrusive contact from strangers or loss of control over money or personal information – concerns that echo their broader worries about stranger danger and cyber security.

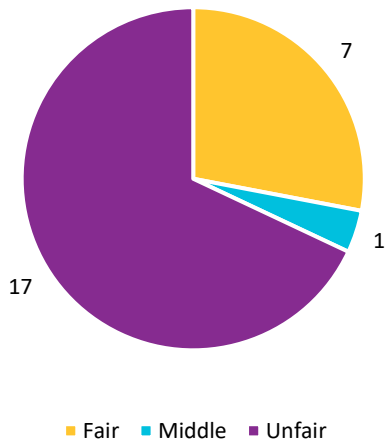
Conversely students seemed less likely to view a scenario as systemically unfair if the risks were more distant or difficult to predict such as those involving algorithms or AI training, or if harm had resulted partly from an individual's own actions.¹¹

For their right to be safe

A student is on an online platform. They don't realise it, but the platform knows their age, location & hobbies and shares it to companies to advertise products to that student. (Number of votes)



A student loves gaming but sometimes feels pressured or tricked into paying extra for things inside the game they didn't mean to pay for at the start.



'It was unfair because the video game never told him he had to pay to play... you can tell your mum that it's making you pay'

'When you play then you have to pay and it's kind of annoying cause you just want to keep playing'

'It is unfair because he already payed for it... You could tell the owner about it and tell him what happed and play a different game and deleat it'

'If kids have to pay for stuff they already have, the price should be low'

'Keep paying for the game'

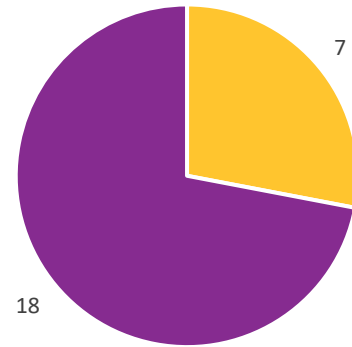
For their right to be safe

'Why we gotta share that info?'

'I don't think they should collect their phone number because calling them is not OK but their birthday is OK?'

'Instead of birthday and phone number, parents should sign their kids in and set age limit'

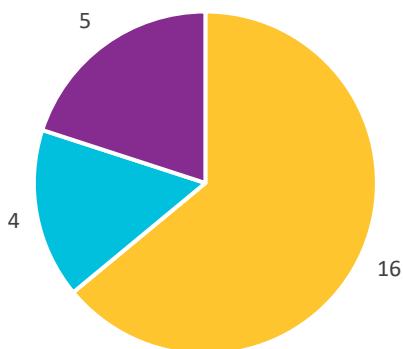
A website won't let a student keep playing a game unless they share their birthday and phone number.



Fair Unfair

'I would say to change it to just your birthday so its nothing really personal'

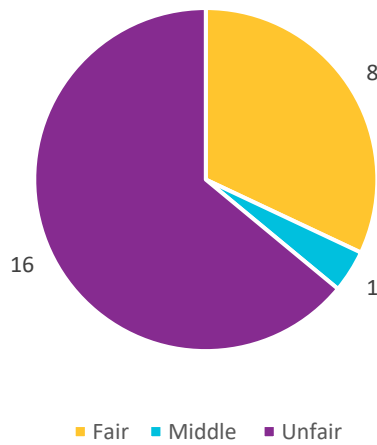
A student is looking for information for an assignment, but they are finding it hard to tell if what they are seeing is AI generated or not.



Fair Middle Unfair

'It should just say either AI generater or made by human'

A student has joined a messaging service to stay in touch with friends but keep getting messages and calls from people they don't know.

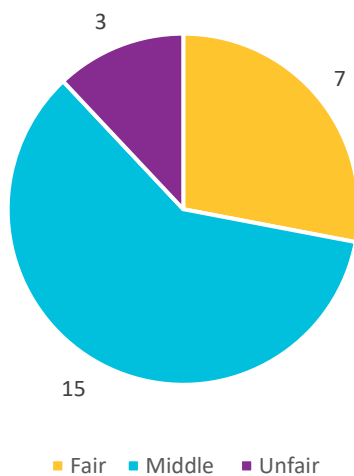


'I think it's unfair what on WhatsApp random stranger's can add you and talk to you. But they should add a rule where they have to prove they know them.'

'they can only chat to people they add'

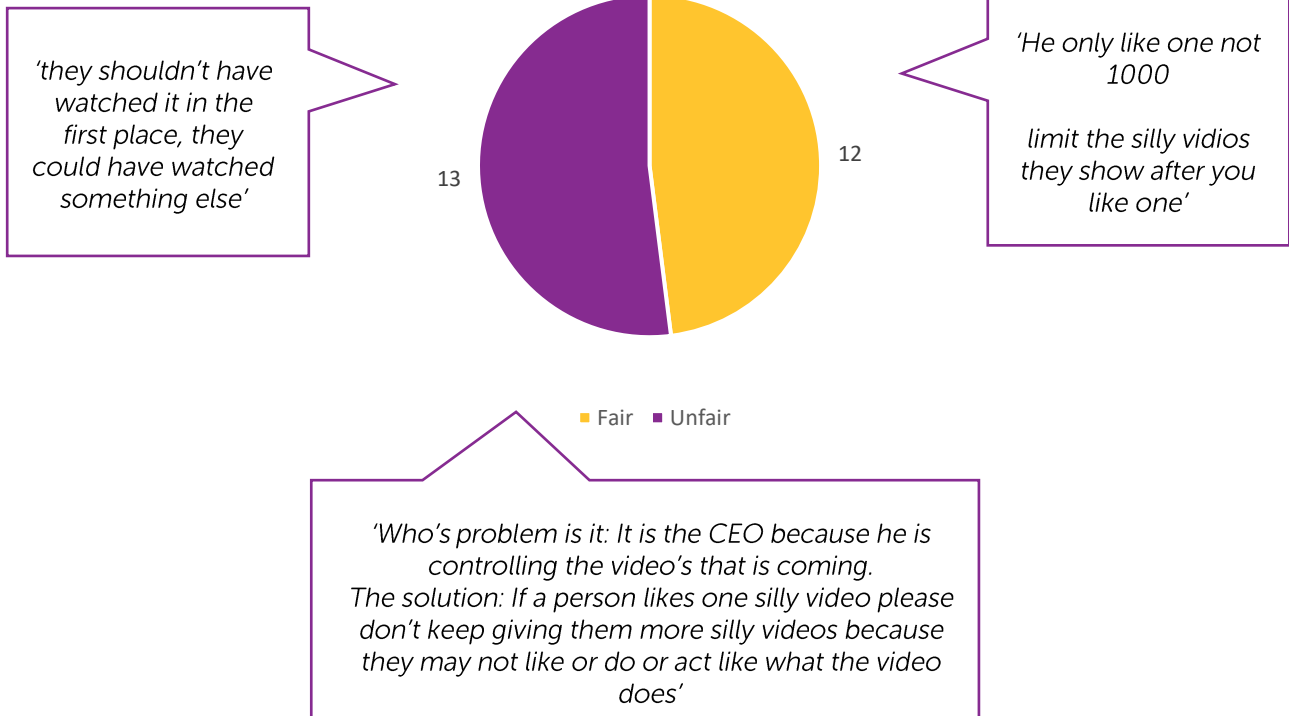
'I would find it unfair and my solution would be to make sure that I wouldn't speak to them and block them'

A student posts a photo of themselves on an online platform. An AI company (like Chat GPT) uses their photo to train itself so it can make more realistic photos of kids.



'it is their fault for putting it there'

A student “likes” a silly video. Now their feed is full of silly photos, they keep getting recommended videos that are sillier and sillier and nothing else is really coming up.



What else have students told us?

Small group consultation with Grades 3-6 students invited them to design an app that would protect their privacy. The students listed features including the following:

- simple privacy settings that are easy to use
- built-in firewall to block hackers and unauthorised access
- locking personal information in a 'loket' so only the individual can access it, like a PayPal for children's personal data
- opt-in data collection, and apps and games that don't require personal data to play
- blocking and filtering out rude language
- ability to report people who make you feel unsafe, remove them from a game or chat, or alert a parent
- notification to parents if a child wants to add a new friend to a chat service
- no tracking of location on games or apps but retain the ability for parents or trusted adults to see children's location
- no ads when children are using apps or games
- ability to block and report scam messages or calls
- ability to call or message for help if privacy is threatened
- built-in reminders to users not to share sensitive data
- built-in suggestions of games and apps which are safe and protect privacy.¹²

In our co-design sessions, lower primary students took part in an exercise where the students drew a superhero who would help people online. Key themes in the drawings related to stopping bad behaviours, being on standby to help, being happy and making others happy, helping people to be healthy, and being a friend.

Describing how these powerful figures would make the online world safer, students' comments included:

- *'It stops people from accidentally buying things.'*
- *'stop people talking to strangers online'*
- *'stops hacker's.'*
- *'can help me if I need help online. can read my mind if I need help'*
- *'flying. protecting laptops from viruses. He appears at night.'*¹³

How would students deal with a problem online?

School workshop findings

Students were asked 'Who gives you rules online, and what are they?'

Their responses were: parents, government, 'settings', teachers and principals.

Students described the rules about staying safe online as follows:

- *'Not to add random people'*
- *'Not swearing so you don't get banned'*
- *'Don't share phone numbers to random people'*
- *'Do all the things – school work and instrument first' [before going online]*
- *'Settings – break time [time restrictions], but they shouldn't let you cancel the break, they should leave it there so you have one'*
- *'Age and time limit'*
- *'Don't give out personal details'*
- *'Don't add random people'*
- *'Don't put lip balm on with your fingers and then put in your password – people will see it'*
- *'Don't let anyone scam you' – a student reflected this is hard because 'they might use a family photo and hack into your account'*
- *'Follow rules apps put on'*
- *'Don't post photos that have personal info, like where you live and your school'*
- *'Don't be a cyber bully, be an upstander'*
- *'No devices in the bedroom or on the toilet, behind closed door' – a student reflected this was challenging because 'you might be playing on your device around your sibling or cousin and they might be distracting' and another student reflected this is challenging because 'what if you have been at school or day and want to rest in bed'.¹⁴*

One of our eSmart team observed a concern being voiced at many schools: students use large numbers of apps and devices, all of which have different privacy and safety settings – settings which get updated intermittently. For example, choosing high safety settings on Roblox requires different steps to choosing high settings on WhatsApp. This makes 'staying on top' of settings difficult for students and their parents or carers, even when they want to make safe choices.

What else have students told us?

Through small group consultations, primary school students told us that parental influence is key: students whose parents often talked to them about topics like online privacy had much deeper understanding of the issues and often adopted their parents' attitudes. This could lead to them mirroring parental behaviours online.¹⁵

Grades 4 and 5 students told us:

- *'My dad works his own business, so he knows a lot about this and is very protective about clicking on links and stuff. It collects your email address, contact details.'*
- *'Maybe checking reviews on apps to see if other people have experienced stuff or researching it before you download something. That's what my mum did with Temu. Google says that one in 25 people have experienced Scams on Temu.'*
- *'I'm playing on the iPad and I just downloaded this game and it says, what day were you born, how old you are, and what's your phone number? Okay, so I just made it up. So, like, because my dad, if there's something online and he has to sign it, like, pretend he's at the post office and he has to sign on the iPad, he just does a fake signature because it might go to someone.'*
- *'Like if I get a text from someone where I haven't added them, it'll be like, report, block, sender. I think my mum set up some stuff where, like if I'm trying to download an app, if it's like 15 plus, then it literally will not let me download that because it knows like that I'm 10.'*¹⁶

Meanwhile, co-design workshops with lower primary students told us that most students (73%) agreed 'It's fun to learn about online safety'.¹⁷ The students expressed general interest in learning about online safety because of their enjoyment and curiosity about the activities they engage in online. Some expressed a sense of responsibility, perhaps driven by parental approval or recognition of the importance of understanding unfamiliar or potentially harmful online environments. Older students were more likely than younger ones to appreciate the importance of learning about online safety.

Students from Foundation / Prep to Grade 2 told us about online safety education:

- *'Sometimes you need to do the hard things you don't know about.'*
- *'Makes me more responsible because my parents will like it.'*
- *'You can get even better and more confident.'*
- *'I learned to skip ads. Now it's more fun.'*¹⁸

We would welcome the opportunity to discuss any of these matters further. Please contact:

Ariana Kurzeme, Director, Policy & Prevention, ariana.kurzeme@amf.org.au
Dr Jessie Mitchell, Manager, Advocacy, jessie.mitchell@amf.org.au

¹ eSmart (Alannah & Madeline Foundation), Digital Duty of Care consultation, 17 December 2026, Presenter: Bianca Kendrick, Youth Programs and Policy Advisor

² eSmart at Alannah & Madeline Foundation, Smart Kids are eSmart Kids co-design reports, 2024

³ Lewers Research for Alannah & Madeline Foundation, 'Upholding children's right to privacy online: qualitative research report,' 2025, available on request

⁴ Lewers Research for Alannah & Madeline Foundation, 'Upholding children's right to privacy online: quantitative report'

⁵ eSmart at Alannah & Madeline Foundation, Smart Kids are eSmart Kids co-design reports, 2024

⁶ eSmart (Alannah & Madeline Foundation), Digital Duty of Care consultation

⁷ eSmart at Alannah & Madeline Foundation, Smart Kids are eSmart Kids co-design reports

⁸ eSmart at Alannah & Madeline Foundation, Smart Kids are eSmart Kids co-design reports

⁹ Lewers Research for Alannah & Madeline Foundation, 'Upholding children's right to privacy online: qualitative research report'

¹⁰ Lewers Research for Alannah & Madeline Foundation, 'Upholding children's right to privacy online: qualitative research report'

¹¹ eSmart (Alannah & Madeline Foundation), Digital Duty of Care consultation

¹² Lewers Research for Alannah & Madeline Foundation, 'Upholding children's right to privacy online: qualitative research report'

¹³ eSmart at Alannah & Madeline Foundation, Smart Kids are eSmart Kids co-design reports

¹⁴ eSmart (Alannah & Madeline Foundation), Digital Duty of Care consultation

¹⁵ Lewers Research for Alannah & Madeline Foundation, 'Upholding children's right to privacy online: qualitative research report'

¹⁶ Lewers Research for Alannah & Madeline Foundation, 'Upholding children's right to privacy online: qualitative research report'

¹⁷ eSmart at Alannah & Madeline Foundation, Smart Kids are eSmart Kids co-design reports

¹⁸ eSmart at Alannah & Madeline Foundation, Smart Kids are eSmart Kids co-design reports