



Children's Online Privacy Code:

Child and Youth Voice Report

June 2026

Contents

Executive summary	3
Method	6
About us	7
Rule 1: Many online services will need to follow the rules in the Code	8
Rule 3: Online services can only collect, use, or share the bare minimum amount of personal information they need to run the app, game, or website unless you choose differently	10
Rule 4: What do children and young people think of the rule 'Online services need to be fair and take care of your personal information in a way that is best for you'?	13
Rule 5: Online services need to ask for your permission to do things with your personal information	15
Rule 6: If you are under 15-years-old, in some situations online services will need to involve both you and your parent or carer to get permission to change your privacy protections	16
Rule 7: Online services must not trick you into giving them permission	17
Rule 8: Online services must make sure that the permission they get from you (or your parent or carer) is 'good' permission	18
Rule 9: Online services must make sure you can access and understand what they do with your personal information	19
Rule 10: Online services must answer you within 30 days (in most cases) if you ask to see, change or delete your personal information	21
Rule 11: Online services must delete your personal information if you (or your parent or carer) ask for it to be permanently deleted	22
Rule 12: Online services must tell you when your physical location can be seen by other people and parental controls are being used	23
Rule 13: Online services must make it easy for you to ask questions and complain if there is a problem with your personal information	25
Rule 14: Online services will need to think and plan before they act	26
Conclusion	27
Appendix: student drawings about online privacy	28

Executive summary

This report responds to the draft Children's Online Privacy Code (the Code), released for consultation by the Office of the Australian Information Commissioner in 2026.

It brings forward the views of children and young people on how their privacy should be protected in the digital environments they rely on every day.

The Alannah & Madeline Foundation (the Foundation) led consultations with children and young people across a range of ages (7-25 years of age), with a particular focus on primary school students. This addresses both their extensive use of online services and the relative lack of past research capturing their experiences, concerns and expectations in relation to online privacy.

In total, we engaged **78 children and young people** specifically on the draft Code and drew on findings from earlier related consultations involving a further **510 children and young people**. Together, these insights provide a substantial evidence base to inform a Code that is not only effective in principle, but also meaningful in practice for the children it is intended to protect.

Children and young people welcomed the intent of the Code and were eager to have a voice in how their privacy and personal information is protected. They were clear that they want stronger protections, clearer rules and greater transparency about what happens to their personal information online. For them, privacy is not a technical or abstract issue. It is deeply connected to safety, trust, dignity and control.

As they told us:

- *'Consumers should have the right to expect that any data collected by the platforms will only be used for their interests, not those of the platforms'.*
- *'We are not safe online because we don't know who we are talking to'.*
- *'it feels a bit uncomfortable knowing that companies might know more about me than i know about myself'.¹*

Their responses send a clear message: children and young people expect privacy protections that are real, understandable and effective. They want online services to collect less data, explain their practices clearly, avoid manipulative design, and take genuine responsibility for acting in children's best interests.

Key insights are summarised as follows:

Rule 1: Many online services will need to follow the rules in the Code

- Upper primary students agreed the Code should apply to services which children use or which collect children's data.
- Primary students use a wide variety of online services, many of them not aimed specifically at children.
- Tech use diversifies with age, with secondary students using AI and various apps for health and wellbeing.

Rule 2: To protect your personal information, online services might have to either give everyone better privacy protections or check your age

- Upper primary students preferred high protections for everyone, while young people were divided.
- Probably due to debates about the social media age delay, many children and young people doubt the reliability of age assurance and see it as a restriction for children to 'get around'.
- Upper primary students tend to accept the general concept of age limits for using online services, while secondary students are sceptical about the efficacy and fairness of age limits.

- Children and young people commonly provide fake personal details online, believing this will protect their privacy or let them access the services they want. This has ramifications for any age assurance employed under the Code.

Rule 3: Online services can only collect, use or share the bare minimum amount of personal information they need to run the app, game or website unless you choose differently

- Upper primary students, secondary students and young adults supported the rule but had questions about how it would work in practice.
- Children and young people do not want to lose the benefits of online services and recognise that collection and use of their personal information benefits them in some situations.
- However, they feel uneasy with services collecting information that is not necessary for the child's online activities or the service's main purpose. Demands for their contact details especially worry them. Many like the idea of data minimisation.
- Primary students' greatest privacy concerns involve interpersonal risks and cybercrime. They want better inbuilt protections from these privacy threats.
- Children and young people receive mixed messages about allowing their data to be collected: this can be portrayed as dangerous (eg. scams), as compulsory and normal (eg. edtech), as protective (eg. age assurance), or as unavoidable (eg. teens on social media).

Rule 4: Online services need to be fair and take care of your personal information in a way that is best for you

- Upper primary students supported the rule in theory but questioned how it would work and doubted online services would stick to it.
- Upper primary students struggle with the concept of online services handling their data but tend to dislike the idea. They want better protections from interpersonal risks, security risks, and intrusive advertising. Their visions of a better internet resonate with the best interests of the child principle.
- Secondary students and young adults do not believe their best interests are upheld online. They want stronger data security and restrictions on advertising to children. They have concerns and mixed feelings about targeting.

Rules 5 & 6: Online services need to ask for your permission to do things with your personal information, and if you are under 15-years-old, in some situations online services will need to involve both you and your parent or carer, to get permission to change your privacy protections

- Children and young people are not used to being asked to make real choices about what happens to their data. Nor are they used to thinking about parental consent in relation to data-handling.
- Upper primary students were divided about the age for decision-making. Some supported 15, while others wanted the minimum age to be younger or older.
- Primary students tend to see parental permission as a normal or positive online safety measure. However, they queried which parent would give permission in cases of divorce and believed some children would 'get around it'.
- Secondary students and young adults supported the rules but queried how they would work in practice. By secondary school, parental permission models are less trusted.
- Secondary students and young adults suggested rules 5 and 6 might be combined for clarity.

Rules 7 & 8: Online services must not trick you into giving them permission, and online services must make sure that the permission they get from you (or your parent or carer) is 'good' permission

- Primary students worry about being tricked online and support these rules.
- However, primary students associate trickery with cybercrime, scams, 'dark patterns' and deceitful content, not with other ways online services might handle their data.
- Upper primary students like the idea of having multiple opportunities to decide about the handling of their data and being able to change their minds easily.

- Secondary students want more honesty from online services about data-handling, but many have experienced so much pressure and dishonesty online that they doubt things will change.
- Edtech complicates these rules, as students use it from a young age and often have little meaningful choice in relation to how their data is handled.

Rule 9: Online services must make sure you can access and understand what they do with your personal information

- Upper primary students, secondary students and young adults supported this rule.
- Children and young people want to make smart choices online and want clear, honest, relevant information that will help them to do this.
- However, the wrong information could backfire badly: causing students fear, confusion and distress or causing them to assume a service is much safer than it is.

Rules 10 & 11: Online services must answer you within 30 days (in most cases) if you ask to see, change or delete your personal information, and online services must delete your personal information if you (or your parent or carer) ask for it to be permanently deleted

- Upper primary students want to be able to see, change and delete data but think 30 days is too long.
- Secondary students and young adults want ways to see, change and delete their data which are simple and secure.
- Some young people spoke of wanting a 'right to be forgotten'.

Rule 12: Online services must tell you when your physical location can be seen by other people and parental controls are being used

- Upper primary students strongly supported the rule.
- Secondary students and young adults tended to support the rule but queried how it would work.
- Primary and secondary students worry about scary people finding their location. This rule could help build their skills and confidence.
- However, there is a risk that alerts could provoke confusion, fear and distress unless the situation is explained clearly and age-appropriately with child-friendly pathways to resolve any concerns.
- Primary students see tracking by parents and carers as protective or unremarkable.
- Children and young people voiced little interest in parental controls, seeing them as either protective, normal or irrelevant.

Rule 13: Online services must make it easy for you to ask questions and complain if there is a problem with your personal information

- Upper primary students want a reporting mechanism which responds swiftly or immediately, and which enables students to ask questions about privacy, alert their parents to a problem, or have someone thrown off an online service for threatening a child's privacy.
- Some primary students don't like the term 'complain', worrying that adults would not respond positively to complaints by children.
- Secondary students know of online reporting pathways but tend not to trust them. They would trust reporting systems more if the systems showed better transparency, consistency and closure.

Rule 14: Online services will need to think and plan before they act

- Upper primary students assumed this rule was a 'given'.
- While children like the idea of the Code, most have not heard of it before. They suggest informing students about it via app notifications, school-based education, pop-up ads in games, news and television.
- Secondary students and young adults are curious about how the Code will be implemented, querying how it will be enforced and whether it will apply to large international companies.

Method

This report presents findings from the following engagements with children and young people in 2026:

- Six small-group workshops engaging 24 primary students between Years 4-6 in six Victorian communities, metropolitan and regional. Workshops were commissioned by the Foundation from Lewers Research, who designed sessions derived from the OAIC consultation worksheets for Years 3-6 students. Complementary workshops were held with 38 parents and carers.
- Student consultations led by our eSmart team with 35 students from Years 2 and 3 at an independent primary school in Melbourne, seven students from Year 6 at a state primary school in Adelaide, and three students aged 10-13 undertaking home schooling in Victoria. Students discussed their use of online services, their concerns and rules for protecting privacy, what happens to personal information online, and what a private and positive online service could be like.
- A workshop with nine members of the Foundation's Youth Engagement Program (YEP) aged 16-25. Young people discussed their uses of technology, their thoughts on data-handling, what they would like to tell online services, and their responses to the draft Code's rules 2, 3, 5, 6, 9 and 12.

The report is also informed by the findings of other recent engagements led by the Foundation:

- A workshop about digital safety, online risks and an 'ideal internet' with 44 Year 6 students from 12 primary schools at a Student Leadership Conference in a Victorian outer metropolitan local government area in 2026.
- A consultation about Australia's Digital Duty of Care led by our eSmart team at a Catholic primary school in Melbourne in 2025 with 26 students from Grades 3 to 5.
- A 'Hackathon' in 2025 for 60 students of different ages from seven Victorian secondary schools, led by the Foundation for the Youth Advocacy Program. The program empowers secondary students to explore and act on digital issues that matter to them while building digital and media literacy, advocacy, creativity and leadership. Students explored and researched key issues and developed pitches to a creative agency for projects to address problems in the digital environment.
- Co-design workshops about digital technologies, online safety education and digital citizenship with 324 primary students from Foundation / Prep to Grade 3 in four schools in Victoria, Tasmania, South Australia in 2024 led by the eSmart team.
- Workshops with 56 primary students from Prep to Grade 6 across seven Victorian communities led by Lewers Research in 2025 to inform the Foundation's submission to the first consultation about the Children's Online Privacy Code.

All children under 18 had parental permission to take part, with information about the workshops provided in advance to parents and guardians. At the school workshops, educators were present and opportunities were taken to strengthen the educators' connection to their eSmart Advisors. Summaries of findings are provided to schools afterwards to help inform planning about digital literacy education.

At the Code consultations, the facilitators led discussions about the Code and its draft rules. They did not cover all the rules in each session, as we judged that a narrower approach would yield richer insights and that much groundwork would be needed before children and young people were ready to discuss the Code.

The report is structured thematically around the rules of the draft Code. Where children and young people responded directly to draft rules, we provide their responses. Our engagements also yielded many insights

from children and young people which did not respond narrowly to individual rules, but which are nonetheless relevant to the Code. We have linked those insights to the most pertinent rules.

We have kept original spelling and grammar to preserve authenticity and remind readers of the children and young people's varied ages and stages of development.

About us

The Alannah & Madeline Foundation was established in the aftermath of the Port Arthur tragedy by Walter Mikac AM in memory of his two young daughters, Alannah and Madeline. Today, our vision is that all children and young people are safe, strong and heard.

Over nearly three decades, our work has grown and evolved, but our purpose remains constant: to champion and strengthen the rights of children and young people to be safe wherever they live, learn and play.

Our work focuses on several connected areas.

Healing and recovery:

Reflecting our origins, we support children and young people experiencing trauma through integrated therapeutic and practical supports, while also strengthening the capacity of parents, carers, educators and communities to respond. This includes specialist trauma recovery and therapy services, as well as work with early childhood settings, kindergartens and primary schools to build trauma-informed capability and practice.

Online safety:

We support children and young people to have safe, inclusive and empowering digital experiences. Through eSmart, the Foundation works with schools, educators, families and communities across Australia to build the knowledge, skills and confidence children need to participate safely, responsibly and positively online. This work includes helping children and young people to develop digital and media literacy, while also working with families, educators, communities and governments to protect children's digital rights.

Bullying prevention:

In 2018, we partnered with Kate and Tick Everett to establish Dolly's Dream, following the tragic suicide of their daughter Dolly. Through Dolly's Dream, we work to prevent bullying and respond to its impacts by supporting children, young people, families, schools and communities with a particular focus on rural, regional and remote Australia. Its programs and services are tailored to the needs and contexts of those communities.

Children's rights, advocacy and systems change:

As a rights-based organisation, we work to transform the systems that shape children's safety and wellbeing. Since our inception, we have advocated for stronger firearms safety and continue to convene the Australian Gun Safety Alliance. We also advocate to ensure children's rights are upheld in digital environments and that trauma-informed approaches are embedded across the systems that support children, young people, families and educators. This includes engagement with government, regulators and sector partners. Across all of this work, we are guided by the voices of children and young people, by evidence and lived experience, and by a commitment to being trauma-informed, inclusive and strengths-based in everything we do.

Rule 1: Many online services will need to follow the rules in the Code

Positive response from upper primary students

This rule was tested in a consultation with upper primary students. They agreed it made sense that the Code should apply to any online services that they use, or that could collect personal information about them, such as health or education apps.²

Primary students use a wide variety of online services, many not specifically for children

Lower primary students told us they used digital technologies including:

- Devices: iPad / tablet, Xbox, PC, laptop, smartphones, Sony PlayStation 5, smart TV
- Gaming: Minecraft, Roblox, Snake Clash, Uno, Poki, Fortnite, Geometry Dash, Fork N Sausage
- Learning: Mathletics, Reading Eggs, Phonics Play, Typing Tournament, Minecraft Education, Wordle
- Social: chat function in games and YouTube, Instagram
- Entertainment: YouTube, YouTube Kids, Disney Channel, Netflix, Spotify, ABC iView
- Search: Google.³

Upper primary students told us they used digital technologies including:

- Devices: Chromebook, iPad / tablet, laptop, PC, iPhone / smartphone, PlayStation 5, TV, Nintendo Switch, smartwatch, smart keyboard, smart mouse, VR headset, headphones
- Social: Discord, Messenger Kids, TikTok, Snapchat, Messenger, WhatsApp, X, Bump, Instagram
- Learning: Bible App, Reading Eggs, VinciBot, Sunshine Online, Duolingo, Word
- Gaming: Minecraft, Roblox, Clash Royale, Zelda, Blockudoku, Sonic, Mario Kart, Pokemon, Block Blast, Fortnite, Temple Run
- Entertainment: YouTube, YouTube Kids, YouTube Music, Kayo Sports, Twitch, Netflix, Spotify
- Creativity: Canva, Gallery, Stop Motion, iMovie, Capcut, Pinterest, Google Photos
- Shop: Temu, Shein, Yelp
- Search: Google, Safari, Google Maps
- Other: Life 360, VicEmergency, Tinder. (It was our impression students had heard of the last app rather than used it, but educators to follow up.)⁴

Comments from students included:

- *'Juniors and Preps are using iPads and the older kids are using Chromebooks'*
- *'I'm allowed as much as I want. Apart from when, like, it's breakfast or dinner or lunch, then you're not allowed'*
- *'I watch Kids YouTube and listen to music'*
- *'I play by myself on my phone'*
- *'Most games I play are pg'*
- *'I am a Roblox hacker'.⁵*

Tech use diversifies with age, with young people using AI and apps for health and wellbeing

Secondary students and young adults told us they used digital technologies including:

- Social: Snapchat, Instagram, TikTok, Messenger, WhatsApp
- Learning: Canvas, Teams, Moodle, Gmail
- Entertainment: YouTube, Netflix
- Gaming: Minecraft, Roblox, Clash of Titans, Fortnite, Block Blast, 8Ball, Xbox
- AI: Gemini AI, ChatGPT, chatbots
- Health: Apple Health, Strava, AI notetaker at doctor, health trackers.⁶

Rule 2: To protect children's personal information, online services might have to either give everyone better privacy protections or check the age of users

Upper primary students preferred high protections for everyone, while young people were divided

This rule was tested in a consultation with upper primary students. They preferred the idea of high privacy protections for everyone. Many students had heard of the social media age delay and believed many children under 16 had succeeded in bypassing those age checks. As a result, many students did not view age verification as effective or accurate. Some also noted that age verification involves the collection of facial imagery and other personal data, which seemed counter to the purpose of the Code.

One student said *'people can just lie and get a photo of, like, say, for example, you're an older person, you can put a photo of, like, a younger person. And even if they do get your real face, they'll probably get your age wrong. And if you put your face on the Internet, it stays there.'*⁷

We also tested this rule with a group of secondary students and young adults. The responses were mixed: one strongly agreed, two agreed, three slightly disagreed or were neutral, and others did not table a response. Their comments indicated uncertainty about the intent and function of age assurance:

- *'what will be the process be behind age checks'*
- *'the privacy checks should be the same for adults and children regardless'*
- *'Why should there be a distinction in the protection of personal information between children and adult when children need parental/carer consent?'*
- *'Better privacy protection should be given to all users whether children or adults. In other words, a baseline for all but extra protection for children as decided by their parents and carers.'*
- *'if age checks are implemented willl children still get the same privacy protection as adults?'*⁸ [sic]

Upper primary students accept age limits as a general concept, while secondary students are sceptical

Many upper primary students support or accept age-based rules relating to the use of online services. When upper primary students were asked to describe their ideal internet or what they would do if they were CEO of a Big Tech company, students' replies included:

- *'Google – not searching up inappropriate stuff and age verification'*
- *'YouTube – age limit where they let you verify your age'*
- *'Roblox – only people of the same ages can play together'*
- *'My ideal internet – putting photo recognition for age'*
- *'Maybe we could make rules for age group like riding a bike or a scooter'*
- *'Putting people in age groups so they can see content made by their age'*
- *'Instagram for kids – Kid appropriate, do face verification, no people over 16'*
- *'14 and over'*
- *'Under 16 only.'*⁹

However, recently many upper primary students have come to believe that children 'get around' age assurance: *'Someone I know drew a moustache on their face and passed age assurance that way.'*¹⁰ Moreover, many students routinely 'protect' their privacy by giving fake personal information online.

Secondary students are sceptical about the efficacy and fairness of age assurance in general, commenting:

- *'young people can and do circumvent age gates'*
- *'we need to be a certain age but it doesn't stop us'*
- *'Alternative accounts are for people to forge being an older person so they don't get banned'*
- *'Kids will find a way to get around it anyway.'*¹¹

Rule 3: Online services can only collect, use, or share the bare minimum amount of personal information they need to run the app, game, or website unless you choose differently

Upper primary students, secondary students and young adults supported the rule but had questions

This rule was tested in a consultation with upper primary students. They had been taught about the importance of staying private online and, as a result, generally supported the rule. They liked the idea of having control over what information was shared about them and expressed concerns about apps asking for unnecessary data. They also liked the idea that they could have higher privacy protections without losing access to the online services they enjoyed using. Comments included:

- *'Because, like, if kids don't want all their information shared, they have the choice.'*
- *'I think it's really good because sometimes apps ask you for more than what they actually need. But, like, if they get the bare minimum, you'll have to share less and you can still play the game normally.'*
- *'Yes (there should be rules). But like, not, like, super strict. Like, rules that are appropriate... not like rules that people can't have any devices at all.'*¹²

We tested the rule with a group of secondary students and young adults. Five strongly agreed, one agreed moderately, and the others did not table responses. Their comments included:

- *'Yes this should be the standard as other information is not necessary unless permission is granted from user like if they wish for their algorithm to cater to them'*
- *'I believe the baseline should be no collection (eg. when users want to try out the service). There should be the arrangement for progressive informed collection commensurate with the service usage requirements.'*
- *'if a user choosers differently does this allow for algorhytm changes etc etc?'*
- *'what would the bare minumum amount of personal info be?'*¹³ [sic]

Primary students' greatest privacy concerns involve interpersonal risks and cybercrime

Lower primary students worried about online 'stranger danger' and cybercrime. Their warnings included:

- *'If someone hacks the platform they can get everyone's info'*
- *'they could steal your money and password'*
- *'Hack into my personal bank account'*
- *'Sometimes people still hack and ask people for their number and stuff'*
- *'if they do that [collect your personal information], they might take an embarrassing picture and threaten to take 1K from you.'*¹⁴

Upper primary students also worried about interpersonal privacy online: *'getting contacted by random people', 'your location being shared and tracked', 'someone can track you with your data.'*¹⁵

When upper primary students were asked how they would improve online services, their replies included:

- *'Snapchat ... verify you are adding people you know'*
- *'Roblox ... 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'*
- *'chats with unknown people get blocked'*
- *'Private server for friends'*
- *'a feature where you know who is who'*¹⁶

Primary students worry about sharing contact details and often provide fake ones

Many lower primary students feel it is not safe to provide contact details online. When asked to draw their ideas of a safe, fun online game, they drew things including:

- Parents allowing their child to share a name but not an address
- Personal details crossed out, blacked out, or written as 'XXXX'
- A message: *'This game collects no information'*
- Students giving fake names
- A student using an uncle's account with a fake name
- The phrase *'name is unsafe'* tilting into a hole.¹⁷

However, lower primary students also believe that providing contact details can be necessary for the functioning and security of online services eg. so students can access their apps, stay updated, be alerted when a login occurs, and purchase things online. Students commented:

- *'If you don't [give them your personal information], you might order something and it might go to another country'*
- *'On Amazon, you have to tell them where you live, they might not give you the package and come and threaten you for money.'*¹⁸

Many lower primary students assumed certain games were private and safe because they were educational or because parents had given permission to use them.¹⁹

Many lower and upper primary students believed using fake contact details was a good way to protect privacy. When we asked a group of upper primary students to draw their ideas for protecting privacy, one drew a game telling its users *'when creating account please do not use real name'*.²⁰

Primary students have limited knowledge of commercial data-handling but some worry about it

Understandably, lower primary students do not think about companies tracking or harvesting their data without their knowledge. One student described a favourite platform as 'safe' because *'you don't need to download anything ... all you do is search poki, press poki games online and your in.'*²¹ [sic]

Some upper primary students are beginning to think about companies handling their data. At one workshop, students told us they liked their personal information being online when it was relevant and useful to them eg. their sporting teams posting the young players' scores and rankings. However, they were uneasy about their data being used for things other than an online service's main purpose.²²

When asked to draw their ideas for protecting privacy, one upper primary student drew an app which told its users *'we will use your personal information to ourselves only and not give it to anyone'*. Another student drew Roblox telling its users *'your info will not be used for any other perpose but only for the use so we can contacte you if your account is hacked and so we know you are not putting real name.'*²³ [sic]

When upper primary students were asked what would make online services safer and fairer, some of their replies addressed data collection, including in relation to edtech, including:

- *'I think, like, if you're using a school app, the school should give you a login so you're not using your information'*
- *'List to make chatgpt safer: Deleting all photos and questions in previous and new chats, not keeping personal information ... not needing to sign in with your email and name.'*²⁴

At one workshop, we gave upper primary students scenarios involving online risks at a system level and asked them to vote on whether each scenario was fair. The majority of students voted 'unfair' for scenarios where a website won't let students play a game without sharing their birthdays and phone numbers, where students get contacted on a messaging service by people they don't know, and where a platform collects

students' ages, locations and hobbies and shares this data with companies which advertise products to the students without students realising what is happening. Students' comments included:

- *'Why we gotta share that info [birthday and phone number]?'*
- *'Instead of birthday and phone number, parents should sign their kids in and set age limit'*
- *'I would say change it [login details] to just your birthday so it's nothing really personal'*
- *'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'.²⁵*

Young people are concerned about commercial data-handling and feel disempowered

By secondary school, more students raise concerns about commercial data collection as well as interpersonal privacy. Young people told us they did not believe they had a choice to protect their data if they wanted to access online services. When asked if their rights were upheld online, their responses included:

- *'No, as our data is always being stolen on websites.'*
- *'No, there are just fake choices of accepting rights. If I need to use the metro WiFi I consent to them collecting information about me. There is no alternative.'*
- *'random AI following accounts and skimming account for pictures'*
- *'selfies or stolen data used for AI'*
- *'We are not safe online because we don't know who we are talking to'.²⁶*

We asked a group of secondary students and young adults to respond to the statement that by the time a child turns 13, online companies have collected approx. 72 million data points on the child. Replies included:

- *'it feels a bit uncomfortable knowing that companies might know more about me than i know about myself'*
- *'I truly feel disturbed that data regarding not only my life but mostly everyone is being sold to large business and organisations'*
- *'It feels a little uncomfortable to just know you don't have any privacy about yourself'*
- *'we dont know what they are collecting and where it is going'.²⁷ [sic]*

When asked what they would like to tell online services, young people commented:

- *'i think that they should be very clear about what information they are taking/make it very accessible and only take the bare minimum like what the new online privacy code says'*
- *'Consumers should have the right to expect that any data collected by the platforms will only be used for their interests, not those of the platforms. Consumers should be offered the option of paying for the service instead of effectively selling their data in return for free usage.'*
- *'TAKE only data that isnt personalised or potentially harming, and if you are taking personalised data inform them that they understand what are the implications'*
- *'Only collect data that is necessary for the app's fiction. Don't share or sell you users data to companies'.²⁸ [sic]*

Rule 4: What do children and young people think of the rule 'Online services need to be fair and take care of your personal information in a way that is best for you'?

Upper primary students supported the rule in theory but had questions and doubts

This rule was tested in a consultation with upper primary students. They supported it in theory but found the language vague. Many believed online services would try to avoid following it. Comments included:

- *'Yes, I think it's good. I think it is worded a little bit peculiarly, like best for all children. But mainly you get the point.'*
- *'I think it's very important because if they're putting ads on there and they shouldn't be able to put these ads on because they influence a child's perspective and what they should do. If it does that, then you should. Because it's basically taking advantage of the child's mind or what they think. So I think it's very important that they put rules in force so then that doesn't happen.'*
- *'You can't really trust that it would definitely be in your best interests.'*²⁹

Upper primary students imagine a digital environment where children's best interests come first

We asked a group of upper primary students what they believed the digital environment should be like. While they did not speak of 'the best interests of the child', their replies aligned well with that principle, including 'Safe', 'Trustworthy', 'Truthful', 'Integrity', 'Responsibility', 'Empathetic', 'Kind', 'Respect', 'Honesty', 'Learning', 'Doing the right things', 'Fun', 'Creative', 'Appropriate', 'Gratitude', 'Teamwork', 'Social interaction'.³⁰

Upper primary students grapple with the idea of commercial data-handling but voice concerns about it

When asked, upper primary students tended to dislike the idea of online services handling their data. Some feared this could lead to interpersonal or criminal risks. A smaller number worried about targeting. Comments included:

- *'Playing a game, and get a targeted TEMU ad for something I bought recently- "it's all connected" '*
- *'chatgpt...stop sucking people in with asking questions with their algorithm.'*³¹

Upper primary students listed ways they would like online services to be improved eg. inbuilt security measures, apps and games that don't handle data, no commercial tracking, no ads when children go online, better blocking and filtering functions. However, some students assume the handling of their data is necessary for them to access services, and some recognise that targeting brings them content they like.³²

Moreover, some data-handling risks can seem distant and confusing. At one workshop, we gave upper primary students scenarios involving online risks at a system level and asked them to vote on whether each scenario was fair. Students couldn't agree about scenarios where a company uses children's photographs to train their AI, or where a student is bombarded with silly videos after liking one. In the first scenario, seven students voted 'fair', three 'unfair' and 15 'middle'; in the second, 13 voted 'unfair' and 12 'fair'. Some students gave responses like *'limit the silly vidios they show after you like one'*, while others responded *'they [the student] shouldn't have watched it in the first place, they could have watched something else'*.³³

Secondary students and young adults do not believe their best interests are upheld online

Secondary students and young adults tend to believe the digital environment does not uphold their best interests. They told us:

- *'Our rights to protection from harm and data collection and privacy aren't in place'*
- *'A lot of the conditions they [services] have shouldn't be legal and contradict our rights'*.³⁴
- *'really anxious and nervous about the future and my privacy and safety on digital apps'*
- *'It makes me feel like I have no anonymity'*
- *'scared for what they could potentially do with the data'*.³⁵ [sic]

Secondary students worried that having to share personal information online could expose them to identity theft or hacking. They objected to intrusive advertising, noting they were regularly shown social media ads for gambling and dating apps despite being underage. Students also observed that some online services are designed to maximise engagement, despite the risks to users' wellbeing: *'when you start you can't stop'*.³⁶

The secondary students wanted stronger protection of personal data, less exploitation of user data, and restrictions on advertising to children eg. fewer ads, no ads, or age-appropriate ads only.³⁷

Other secondary students and young adults discussed why online services handle individuals' data and engage in targeting:

- *'To sell it [data], to understand and build your algorithm, to target ads for you'*
- *'to fill your inbox and feed with exactly what you want to see'*
- *'because they want to use this information to advertise products'*
- *'to know what we like and to keep us on the app for longer'*.³⁸

Students recognised some positives: data-handling and targeting could make online services more convenient and enjoyable. However, they also warned these processes could make online services invasive, annoying or addictive: *'it kind of makes me feel like every move i make is being watched by some sort of algorithm which makes me a little uncomfortable / icky'*.³⁹

Rule 5: Online services need to ask for your permission to do things with your personal information

Upper primary students were divided about the age for decision-making

This rule was tested in a consultation with upper primary students. They had mixed views on the appropriate age for children to make decisions about their data. Some considered 15 appropriate; some wanted the early teens, and some wanted 16 or 18.

One student commented *'I think it's a good rule because, like, when you're usually 15, like, you usually, like, know everything. Like, you know what to say yes to and what to say no to and, like, how to take care of your personal information.'*⁴⁰

Secondary students and young adults supported the rule but had questions and doubts

We tested this rule with a small group of secondary students and young adults. Four agreed strongly, one agreed moderately, and the others did not table responses. They queried how it would work, commenting:

- *'How will apps actually verify that it is the parent is the one giving permission'*
- *'Lots of young people under 15 fake parental consent as well, a better way to force parental consent could be a voice or face recording of consent given'.*
- *'how will they make sure its a parent doing the permission and not a younger person?'*⁴¹ [sic]

One young person argued *'I think the real issue to be addressed is full transparency in the collection and usage of personal data, rather than an arbitrary age threshold. The platforms should facilitate parents/carers and children to come to a consensus and provide parents/carers with ongoing information on the collection and usage of personal data of their children to give the former the peace of mind'*.⁴² [sic]

Most primary students are comfortable with parental permission as a general approach

Primary students were not used to thinking about parental consent in relation to data protection. However, many were used to needing parental approval for other online activities eg. before downloading apps or playing new games.⁴³ As one lower primary student said about gaming, *'They [children] can ask an adult, and then when the adult says yes, they can play.'*⁴⁴

A few upper primary students wanted less adult supervision online (*'NO parental controls!'*), but most saw parental permission as a normal safety measure – although they were not used to associating it with data-handling. Their ideas for a better internet included:

- *'Nintendo – app connected to parents' phone where they can see what you are doing'*
- *'Can only get a friend with mums approve'*
- *'Parental controls'*
- *'Parentle approval'*
- *'you need parents permission for social media sign in.'*⁴⁵ [sic]

By secondary school, parental permission models are less trusted

Some secondary students and older primary students no longer believed their parents understood digital technologies well enough to make appropriate choices. Several raised concerns about parents entering information about their children into generative AI. One student said *'my mum thinks of Chat GPT as a person and as a friend'* and drew a student (*'young but educated'*) saying to the mother *'bro it's not even real who knows whos gonna look at your chat.'*⁴⁶

Rule 6: If you are under 15-years-old, in some situations online services will need to involve both you and your parent or carer to get permission to change your privacy protections

Upper primary students and young people supported the rule but worried it would not work in all cases

This rule was tested in a consultation with upper primary students. Involvement of parents in online decision-making was a familiar concept to them, as many had parental controls on their devices and were used to needing parental permission to download new games, especially with a paid component.

Most were comfortable with the rule and did not have concerns about parents having oversight and veto over certain activities.

However, some argued that other children might not want parents' involvement or might forge parental consent. Some queried what would happen to parental permissions if parents were divorced. Comments included:

- *'Some kids are really sort of... They don't really listen to their parents and they're more independent, I guess you could say. And they could forge a signature if they're influenced badly. And you can't really do anything about that if they do.'*
- *'How would they know that it's definitely your parent? Because you could just pretend that you're the parent, do yours and pretend that you're your parent and do their signature.'*
- *'I feel like this is good but I feel like they something like if they needed both parents. Some people have divorced parents and they can't have both parents.'*
- *'So mum's put a control on my iPad so I'm not putting anything on inappropriate things or doing the wrong things on it, but when I want a game it says, come up with the Apple load thing. Saying, are you allowed this game? And then you have to send it to your mum.'⁴⁷*

We also tested this rule with a small group of secondary students and young adults. Their responses trended positive: one strongly agreed, three agreed, two slightly agreed or were neutral, and the others did not table a response. Comments included:

- *'rule 5 and 6 seem really similar. maybe could become one rule?'*
- *'How are we making sure that the parent is the one allowing permission, that the rule is being bypassed'.⁴⁸*

Rule 7: Online services must not trick you into giving them permission

Upper primary students strongly supported this idea

This rule was tested in a consultation with upper primary students. It resonated strongly with them, as they gave many examples of feeling tricked or pressured online eg. being signed up for paid services without realising it, finding it difficult to unsubscribe or exit from games, ads and services, and being explicitly pressured to do certain things. Their understanding of 'tricks' was broad, encompassing commercial dark patterns, criminal scams, and unwelcome content. Comments included:

- *'I almost pressed yes and then cancel but the cancel button was very small and in the corner. It should be big and in the center.'*
- *'I had this game called Tokaboka. And it was supposed to have multiple games for free. And then you could only do like three without a subscription. And then it said, do it for free, but it didn't tell me it was going to start making my mum pay \$30 a month. So it started charging my mum \$30 a month. And then she got so annoyed at me, she was like, why am I getting charged?'*
- *'While you're scrolling, you can see videos of people saying if you don't subscribe, your family will die and stuff. And then you get pressured into doing it and... And like little kids believe it and they have to subscribe.'*⁴⁹

Primary students worry about being tricked online but rarely associate this with legal data-handling

Lower and upper primary students spoke of the need to be vigilant against online tricks by criminals: *'Getting scammed', 'Someone might want to scam me or trick me', 'No hacking', 'Do not click pop ups or links', 'Keep passwords safe', 'My friend had enough Robux, but it made him use real money'*. Upper primary students recalled many mistakes and near-misses eg. clicking on links, receiving strange messages.⁵⁰

Upper primary students also worried about making unintentional purchases online eg. on sites like Temu and Shein. When asked how online services could be improved, one student wished *'Temu – wouldn't let you buy anything with your mum's credit card'*.⁵¹

We presented one group of upper primary students with a scenario where a student feels pressured or tricked into making unintended purchases inside an online game. Most students (17 out of 25) thought this was unfair. Their comments included *'It was unfair because the video game never told him he had to pay to play', 'When you play then you have to pay and it's kind of annoying cause you just want to keep playing'*.⁵²

However, very few primary students thought about trickery in relation to reputable online services handling individuals' data. Only a small number had begun to worry that some services were not being honest with them – *'Eg-when camera or location is being used but you were sure you said no'*.⁵³

Secondary students want more honesty from online services but doubt it will happen

By secondary school, more students believed online services were tricking them into agreeing to the handling of their personal information. Students recognised they were more likely to give their data away because they could not understand complex T&Cs, commenting:

- *'terms and conditions are written in a way that is not easy to understand'*
- *'data is taken when signing up to social media'*.⁵⁴

However, secondary students worry about many types of trickery online: hacking, scams, identity theft, misinformation, manipulative people, intrusive advertising, and pressured in-app purchases. In this context, some feel apathetic or overwhelmed, unable to imagine having real choices.⁵⁵

Rule 8: Online services must make sure that the permission they get from you (or your parent or carer) is 'good' permission

Upper primary students supported this idea

This rule was tested in a consultation with upper primary students. They agreed broadly with the six components of 'good' permission, but two really stood out for them. They liked the idea that they would be asked to give permission more than once, so they could be reminded and stay up to date with where they had given permissions. They also liked the idea of being able to withdraw their permission at any time if they made a mistake or changed their mind. Comments included:

- *'I personally really like the keeping up to date. So because you could get an app and it just does a bunch of wish stuff once you've actually started playing it and then it's like, do we still have your permission? And you can say no. Then it's so much easier.'*
- *'I think it's good because, like, you can take all your permission at any time because so sometimes you might agree but then you like, might disagree.'⁵⁶*

Edtech complicates understandings of permission

When using educational technologies at school, primary and secondary students are often prompted or instructed to provide personal information like a name, DOB and email address, often without their parents' specific, informed, time-limited approval. Of course, high-quality edtech can bring many benefits for students. However, the current approach complicates students' experiences of 'good' permission.⁵⁷

Rule 9: Online services must make sure you can access and understand what they do with your personal information

Upper primary students supported this idea

This rule was tested in a consultation with upper primary students. They could relate to the idea of shorter and simpler privacy policies, as they often found them too long and complex and would skip over the details. The students supported the idea of being able to easily find, read and change privacy policies and permissions. A pop-up screen was seen to be a simple way to bring things to their attention.

- *'They should like explain it very well and like say, are you sure what it is?... Because some people might not understand.'*
- *'If each of the terms were like one sentence, like even maybe shorter than a sentence, like I read them, I normally just skip through them because if I try and even go on to them, it's like 10,000 words.'*⁵⁸

Secondary students and young adults supported this idea

We tested this rule with a group of secondary students and young adults. Three strongly agreed, two agreed moderately, and the others did not table a response.

One young person commented *'Definitely one of the most important rules and ensures data transparency and young people feeling safe when they know how their data is being used'*.

Another young person suggested ways of communicating with young users: *'mandatory/unskipable videos explaining, pre setting up the app/service'*.⁵⁹ [sic]

Young people agreed that many online services did not provide good information about data-handling. One commented *'I feel overwhelmed by the fine print which is not in plain English for easy read appropriate to children, teens and even young adults. Therefore, any consent given is not really informed.'*⁶⁰

Children want help to make smart choices online

Upper primary students often described their responsibility to make good choices online, including:

- *'Keeping personal information private'*
- *'Don't share phone numbers to random people'*
- *'Don't add random people'*
- *'Don't post photos that have personal info, like where you live and your school'*
- *'Keep passwords and personal info tied to you and don't tell randoms online'*
- *'Remember Yappy; the most important rule; don't YAP about your personal information online or anywhere.'*⁶¹

High-quality information could help students to build those skills. Some upper primary students wanted online services to provide proactive, consistent, simple information to encourage good choices:

- *'Should be clear instructions when you download apps and tutorials for how to change settings'*
- *'Add consistent reminders of what to do right'*
- *'it should be the same on every app'*
- *'it should be a simple tick box.'*⁶²

However, the wrong information could make things worse for primary students

Primary students think about privacy mainly in interpersonal terms. A notification that their personal information is being collected, stored or shared could cause worry or distress, as they fear it means scary individuals will find them.⁶³

Some upper primary students alerted us to another complication: when children hear that an online service has 'child-friendly' information, they might assume this means the whole service is child-friendly ie. safe and suitable for children. Some students assumed a service that provided child-friendly information would also be free from problems like gore content and swearing.⁶⁴ The potential for misunderstandings and subsequent loss of trust is significant.

Secondary students want clear, honest, accessible information

By secondary school, students are more aware that unclear privacy policies and T&Cs contribute to online risks. They want to see online services make changes including:

- *'There should be a legal requirement to provide a summary of terms and conditions'*
- *'Be clear about what data is being tracked specifically rather than just saying "cookies" because young people don't always know terminology'*
- *'Examples should be in Plain English or at least 7th grade level reading'*
- *'Make it known that information is being collected because some apps don't state that they collect data which is immoral to their users'*
- *'outline risks of allowing data collection so users can make an informed decision'*
- *'Have clear and easy to access language for T&Cs'.⁶⁵*

Rule 10: Online services must answer you within 30 days (in most cases) if you ask to see, change or delete your personal information

Upper primary students want to be able to see, change and delete data but think 30 days is too long

This rule was tested in a consultation with upper primary students. The students were in favour of being able to request that online services be responsive to requests to see, change or delete personal data.

However, the students felt 30 days was too long a time period for these requests to be actioned. Two weeks was more aligned with expectations. Comments included:

- *'I think it's really good because sometimes, like, you might... You might have gotten, like, tricked or something, and then they just don't reply, you know?'*
- *'Pretty good... I just think it should be shorter. Maybe like 15 days.'*⁶⁶

Young people want ways to see, change and delete their data which are simple and secure

Several young people told us they wanted ways of seeing, changing and deleting their data which were simpler and more secure. Their comments included:

- *'making it easier to change what data you give to companies (make it in the app instead of having to go to like a different website that is really hard to navigate)'*
- *'Personal data should only be stored at a storage location specified by a consumer who can encrypt, monitor, access, edit, remove and transfer such data at will to maximise protection'*
- *'I think there should a right to be forgotten in relation to personal data collected'*
- *'i feel like there should be a rule maybe that says it should be super easy to see what information is being accessed (not having to go on like 2 seperate websites just to see/change something)'.⁶⁷ [sic]*

Rule 11: Online services must delete your personal information if you (or your parent or carer) ask for it to be permanently deleted

Upper primary students supported the rule

This rule was tested in a consultation with upper primary students. They were in favour of having the ability to request that their data be permanently deleted and to be notified that this action has been taken. This rule has potential to reduce stress for children, as they know they can take greater control of their data at any time. Comments included:

- *'It would make me feel, like, better and calmer and would make you feel, like, not stressed (if I could request my data be deleted).'*
- *'I think I agree with that rule because it's, like, really safe and it makes sure that they can't gather information about you.'*⁶⁸

Rule 12: Online services must tell you when your physical location can be seen by other people and parental controls are being used

Upper primary students strongly supported the rule

This rule was tested in a consultation with upper primary students. They were in favour of the rule and appreciated the transparency and safety aspects. The rule was seen as valid and important, especially for younger children.

- *'Because, like, sometimes people that you don't want to see, like, your own location can be seeing your location.'*
- *'That's a good one. It could make you feel unsafe.'*⁶⁹

However, some students expressed concerns about feeling unsafe or distressed if they knew they were being tracked and there were mixed feelings about the emotional impact of being notified.

The children we spoke to did not express any concerns about their parents being able to track their location. Several were using apps like Life360 within their families for safety. Comments included:

- *'I have Life 360 on my phone. Sometimes, like, my mum can get me to, like, check where my sister is or something. We even have my sister's boyfriend's on it in case my sister turns off her location.'*⁷⁰

Secondary students and young adults tend to support the rule but query how it will work

We tested this rule with a small group of secondary students and young adults. Their responses trended positive: three strongly agreed, two agreed, one slightly agreed or felt neutral, and others did not enter a response. They queried how such alerts would work, commenting:

- *'Great that they are thinking of physical location of individuals, and how important transparency is'*
- *'Yes this is good otherwise it is an invasion of privacy for the young person'*
- *'location transparency is good but in comparison to other safety features I personally don't think its as important'*
- *'how will it tell you?'*
- *'Will be these tracking notifications be constant reminders or only one time alerts?'*⁷¹

Tracking alerts could help primary students – or they could make things worse

When we spoke to lower primary students, they worried about 'stranger danger' online but did not bring up geolocation specifically. We suggest this reflects their junior level of digital literacy.⁷²

Upper primary students voiced stronger concerns about interpersonal privacy, worrying that bad people would see where they lived or went to school.⁷³ A few called for an end to location tracking in games and apps or clearer ways to make choices about this:

- *'Geo tracking – would be good to be asked every time location is being tracked'*
- *'Snapchat – remove the map feature'*
- *'Share your location? Yes, No'* [two tick-boxes shown neutrally and equally].⁷⁴

Alerting primary students when someone can see their location might help them to build their skills and confidence. However, if such functions were poorly designed, they could have the opposite effect: worsening students' uncertainty and fear. It is not reasonable to assume every child will ask a parent or carer with high digital literacy to resolve the matter.

Meanwhile, many parents gift smartphones or smartwatches to upper primary students partly as a safety measure to track their children's location. Some students commented that they were only allowed to walk

to school because of apps like Life360.⁷⁵ Thus, upper primary students have seen geolocation features presented as both protective and dangerous. Given the potential for confusion, clear, honest communication with children becomes even more important.

Tracking alerts could help secondary students but will not resolve every problem

Secondary students also worry about interpersonal privacy online.⁷⁶ Conceivably, a tracking alert could help to address these concerns. However, few secondary students raised geolocation as a standalone problem. They saw the whole digital environment as a place where privacy was hard to maintain and wanted better support overall.

There was little debate about parental controls

Parental control features excited little interest among the children and young people we consulted. Primary students tended to see parental controls as protective or unremarkable, while secondary students rarely mentioned them, doubting their parents' digital literacy and viewing online safety as their own responsibility.

Rule 13: Online services must make it easy for you to ask questions and complain if there is a problem with your personal information

Upper primary students want to be able to report easily and get a timely response

This rule was tested in a consultation with upper primary students. They were broadly in agreement with it, although some worried about the word 'complain', as adults often tell them not to complain.

However, the prospect of being able to easily ask questions and expect a timely response was viewed positively. One student commented *'I think it should be, like, easy to, like, make a complaint or, like, review a game or write it.'*⁷⁷

Primary and secondary students want better reporting options than those currently available

Some upper primary students said they would like the ability to call or message for help if their privacy was threatened – for example, they wanted mechanisms to alert their parents to a privacy problem or to have a person kicked out of a game or chat for threatening children's privacy.⁷⁸ It was our impression that the students envisaged getting an immediate or quick response.

Secondary students had more awareness that they could report concerns to online services. However, they did not have much trust in these options. Some found it confusing to report a concern because mechanisms varied between different platforms. Others said the feedback loops from online services following a complaint were weak, with few clear outcomes or closure: *'when you report it, there isn't a feedback unless you go to the eSafety website or the police.'*⁷⁹

Rule 14: Online services will need to think and plan before they act

Upper primary students thought this rule was a 'given'

This rule was tested in a consultation with upper primary students. They found the rule difficult to engage with, as it seemed a 'given' or a hygiene factor.⁸⁰

Upper primary students are keen to see the Code promoted to children

A consultation with upper primary students found that while they liked the idea of the Code, they had not heard of it before.⁸¹ They suggested ways to notify and educate children about the Code, including through app notifications, school-based education, pop-up ads in games, and using news or television. They also highlighted the need for information to be presented in a fun or interactive way to ensure engagement. Comments included:

- *'When you go into the app, like, there'll be this thing and saying there's new rules, and then you can click on it and it'll just say, like, kind of like the main things.'*
- *'Get someone your age to tell you about it.'*
- *'Put it up at schools, but in fun ways.'*⁸²

Secondary students and young adults want to see how the Code is implemented and enforced

When we spoke about the Code with a group of secondary students and young adults, they were curious and skeptical about how it would be brought to life. Their comments included:

- *'unsure if it will be effective and implemented properly'*
- *'What type of penalties will tech companies face?'*
- *'How to make sure this is being regulated'*
- *'Would the code be regulated to large scale international companies rather national Australians business and services.'*⁸³ [sic]

Conclusion

Taken together, the insights in this report make clear that children and young people want a digital environment where privacy is real, understandable and built in by default. Across age groups, they consistently called for stronger protections, less unnecessary data collection, clearer explanations, more meaningful choices, and online services that act honestly and in children's best interests.

While their experiences and levels of understanding vary, the message is consistent: children and young people do not want privacy to depend on luck, technical knowledge or constant vigilance. Their reflections also show that privacy cannot be treated as a narrow or abstract issue. For children and young people, privacy is deeply connected to safety, trust, autonomy and dignity. It shapes whether they feel secure from unwanted contact, scams and tracking; whether they understand what is happening to their information; and whether they believe online services are designed to respect them rather than exploit them.

They want systems that are simpler, fairer and more transparent and they want adults, regulators and industry to take responsibility for making those systems work.

The Code is therefore an important opportunity to set a higher standard for how children's personal information is handled online. To succeed, it must do more than state good intentions. It must deliver protections that are practical, enforceable and meaningful in the everyday lives of children and young people. Their views point to the same conclusion: children deserve privacy settings and digital environments that protect them by design, support them to make informed choices, and place their rights and best interests at the centre.

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

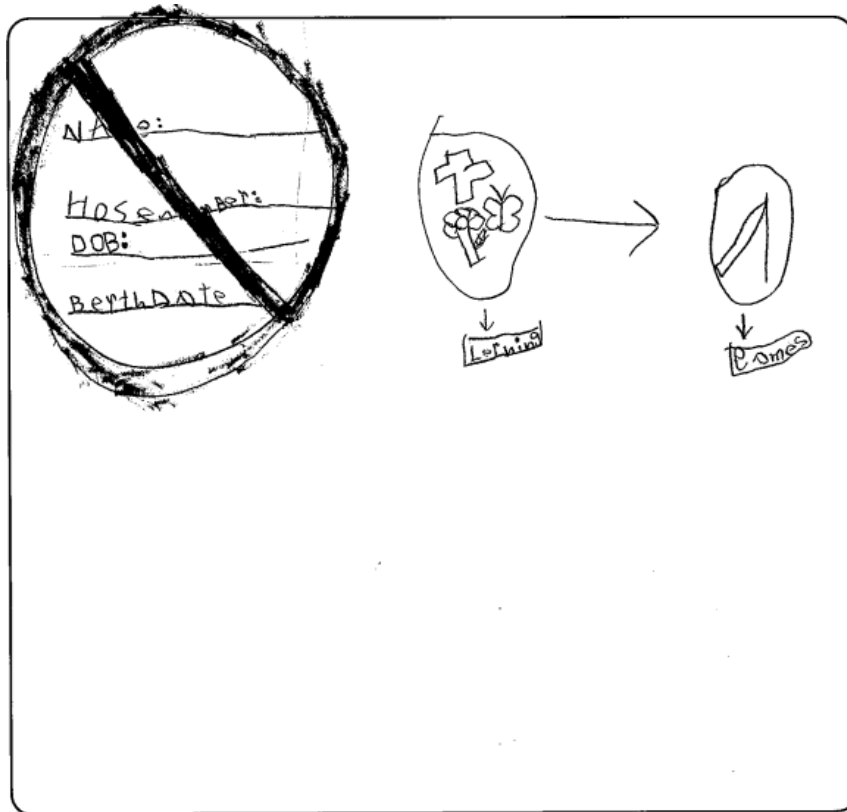
Ariana Kurzeme, Director, Policy & Prevention, ariana.kurzeme@amf.org.au
Dr Jessie Mitchell, Manager, Advocacy, jessie.mitchell@amf.org.au

Appendix: student drawings about online privacy

Year 2 and 3 students were asked: 'You are excited to play a new game "The King of Wizards"... What personal information do you think this new game will ask you? What do you think it is going to do with your information? Why do you think your grown up should download and play with you? Why is it safe?'

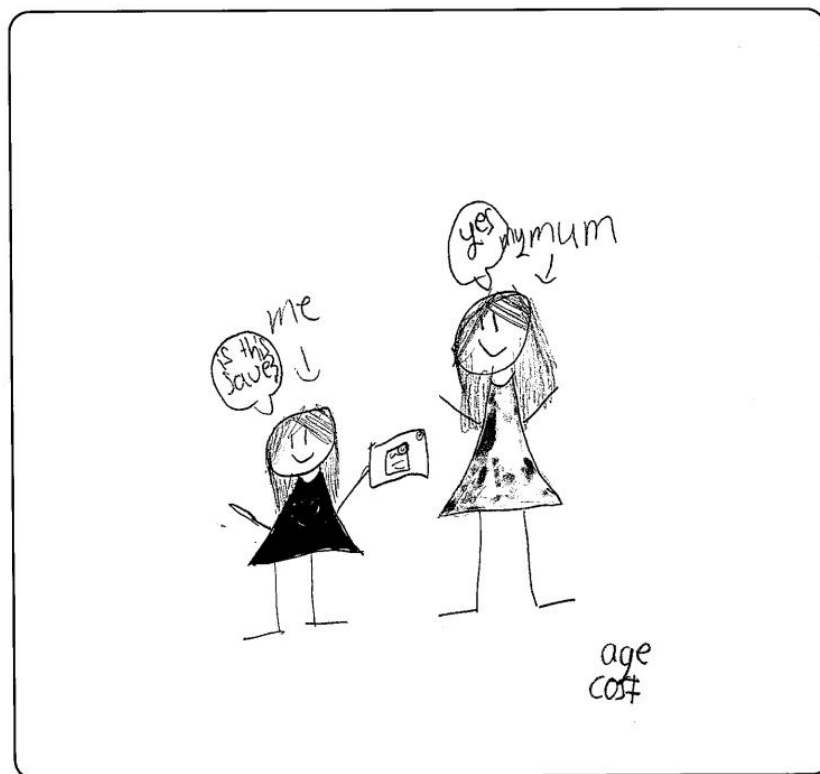


Above: The student felt it was OK to give some details but not all, and only with parental permission.



eSmart

Above: Personal information is crossed out, and games for learning are believed to be safe.



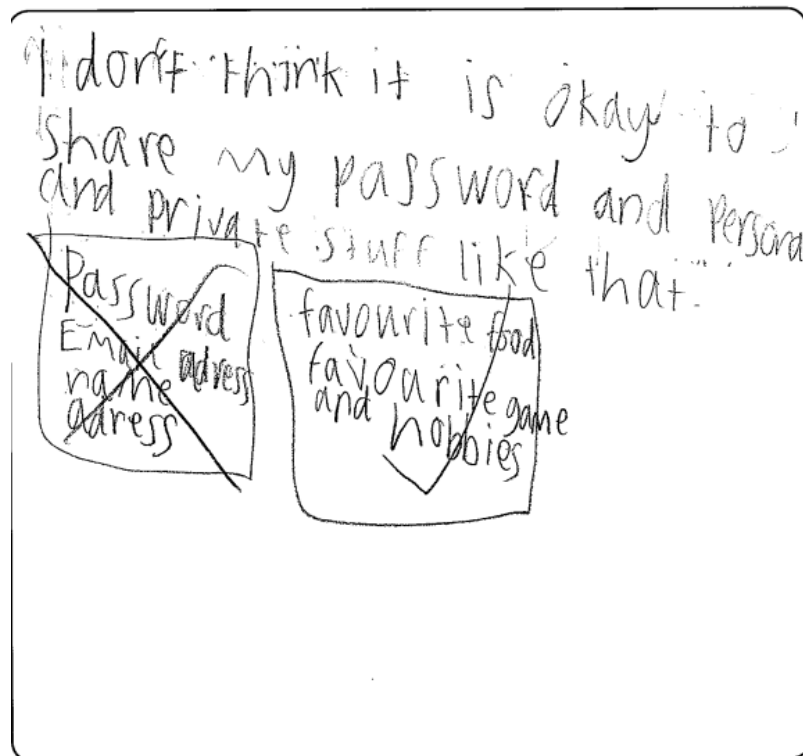
eSmart

Above: Online services are assumed to be safe if parents have given permission to use them.



eSmart

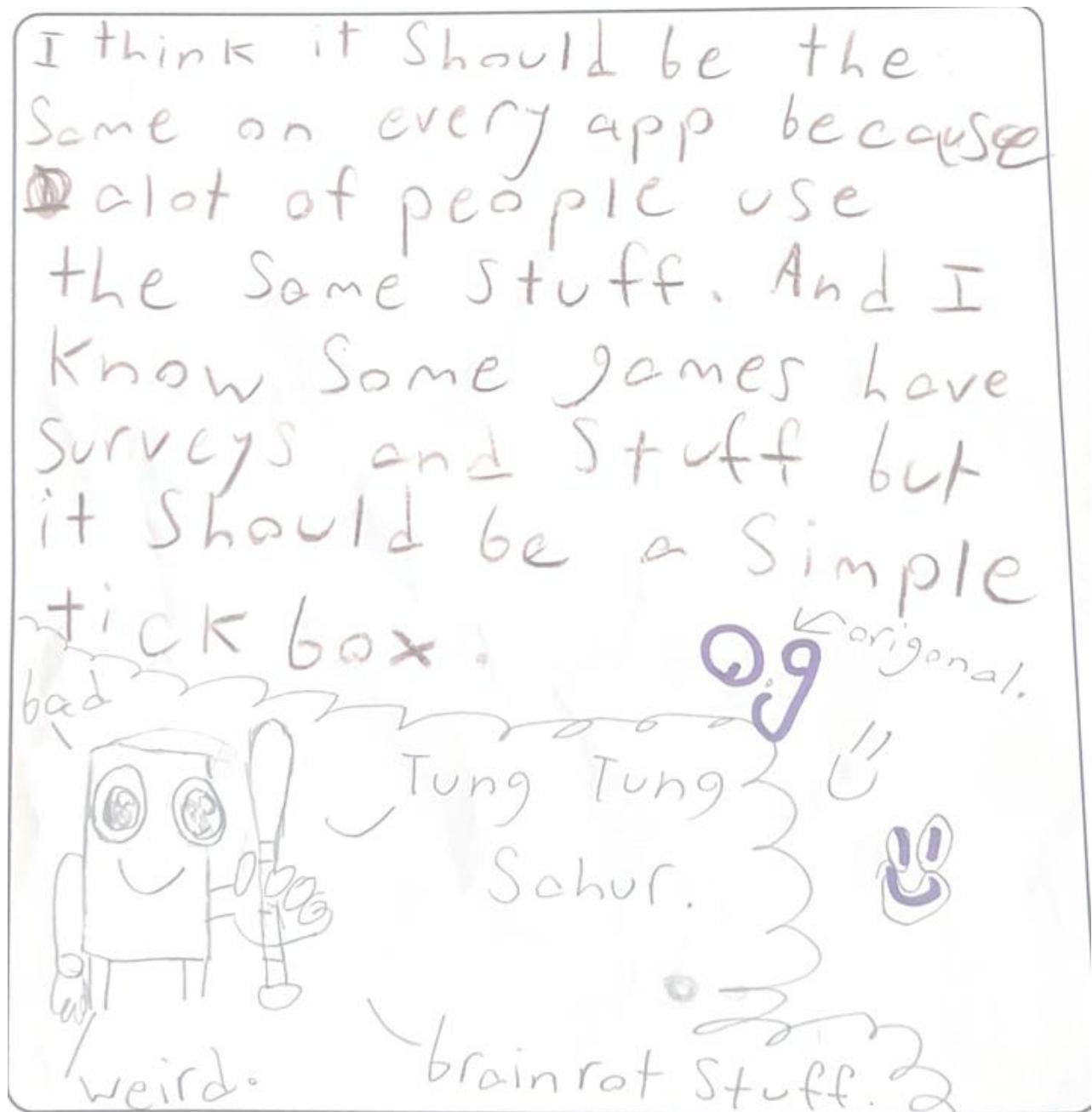
Above: To be safe, a student's parents stopped a relative putting her photo into AI.

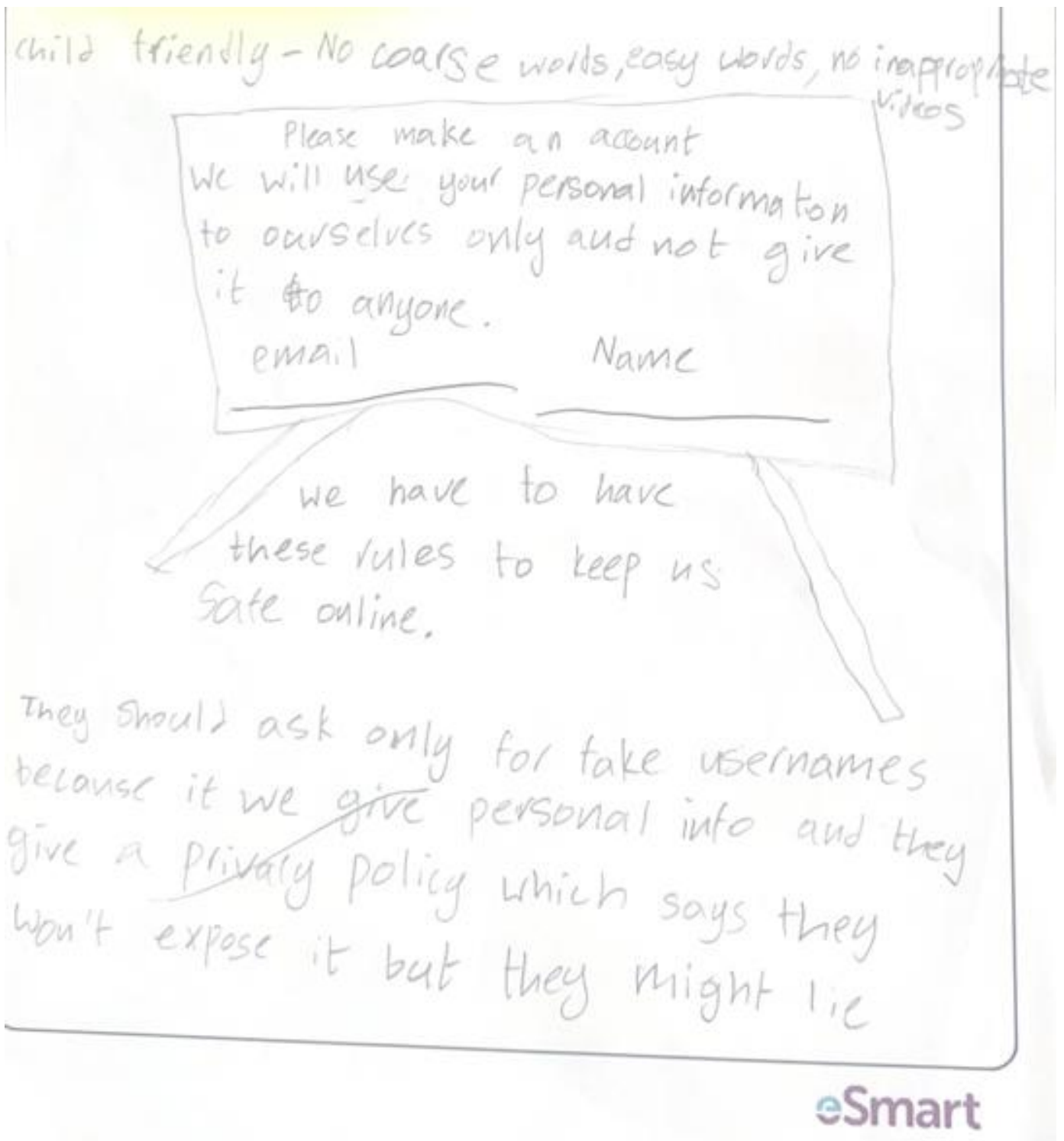


eSmart

Above: A student saw some information like hobbies and interests as safe to share online but contact details as unsafe to share.

Upper primary students were asked "Draw or write about how an online platform could make it easy for you and your grown up to access and understand what they will do with your personal information".



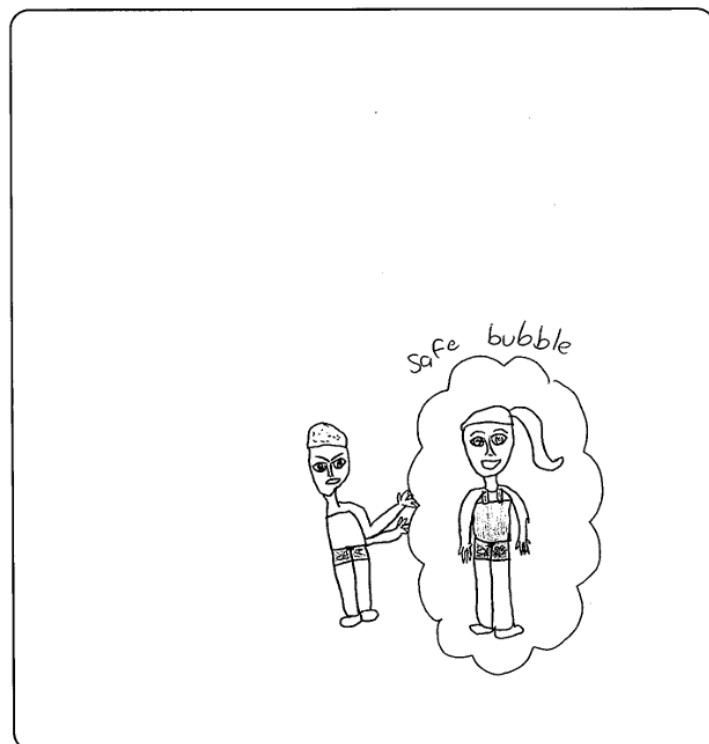


Above: The student envisaged 'child-friendly information' encompassing child-safe content on the service as well as clear privacy explanations. Fake names were associated with privacy. Mistrust in online services was expressed.

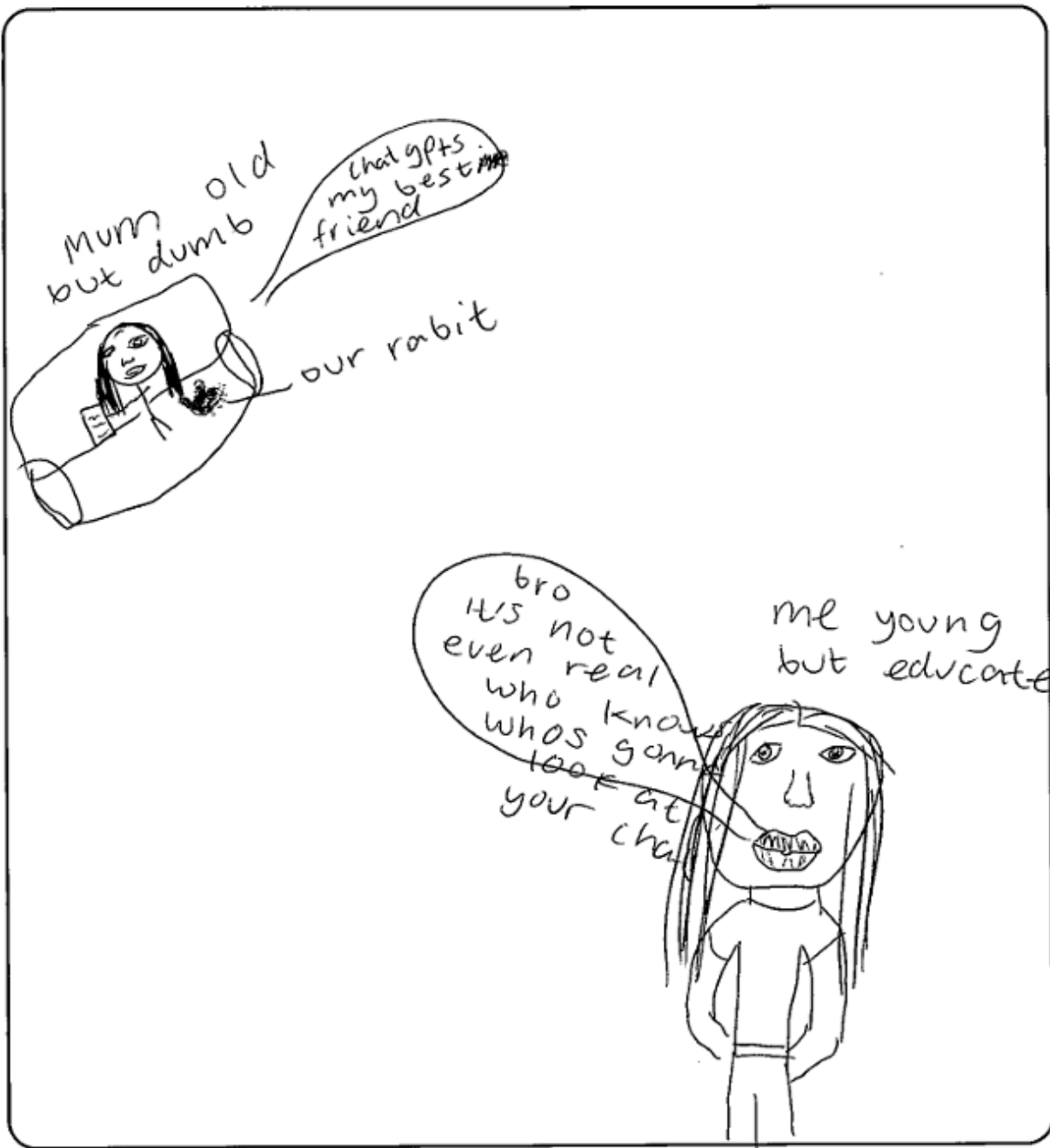
Upper primary students engaged in home schooling were asked 'Draw or write what it would be like if your privacy is NOT protected on an app or platform you use'. 'Now draw or write what the same app would look like if it is being fair and acting in your best interests to protect your privacy'.



eSmart



eSmart



eSmart

Above: A student worried that parents did not have the digital literacy to decide what AI did with their children's personal information.

¹ Alannah & Madeline Foundation, 'Youth Engagement Program workshop on the Children's Online Privacy Code', 2026

² Lewers Research for Alannah & Madeline Foundation, 'The Draft Children's Online Privacy Code: consultation with parents and carers and primary aged children - qualitative research report,' prepared by Lisa Lewers, Moira Callard and Lauren Campbell, 2026

³ eSmart, Alannah & Madeline Foundation, 'Children's Online Privacy Code consultation with Years 2 and 3 students', Melbourne independent primary school, 2026; eSmart, Alannah & Madeline Foundation, 'Safe Kids are eSmart Kids: lower primary school co-design results, external report,' August 2024; Lewers Research for Alannah & Madeline Foundation, 'Upholding children's right to privacy online: qualitative research report,' 2025

⁴ eSmart, Alannah & Madeline Foundation, 'Children's Online Privacy Code: consultation, state primary school, Adelaide', 2026; eSmart, Alannah & Madeline Foundation, 'Children's Online Privacy Code small-group workshop, home education students,' May 2026; eSmart, Alannah & Madeline Foundation, 'Children's voices and the digital duty of care', upper primary school workshop, Melbourne, December 2025; Lewers Research for Alannah & Madeline Foundation, 'Upholding children's right to privacy online: qualitative research report,' 2025

⁵ eSmart, Alannah & Madeline Foundation, 'Children's Online Privacy Code consultation with Years 2 and 3 students, Melbourne independent primary school', 2026; eSmart, Alannah & Madeline Foundation, 'Children's voices and the digital duty of care', upper primary school workshop, Melbourne, December 2025; eSmart, Alannah & Madeline Foundation, 'Safe Kids are eSmart Kids: lower primary school co-design results, external report,' August 2024; Lewers Research for Alannah & Madeline Foundation, 'Upholding children's right to privacy online: qualitative research report,' 2025

⁶ Alannah & Madeline Foundation, 'Youth advocacy program: insights report for Year 1 implementation 2025,' March 2026; Alannah & Madeline Foundation, 'Youth Engagement Program workshop on the Children's Online Privacy Code', 2026

⁷ Lewers Research for Alannah & Madeline Foundation, 'The Draft Children's Online Privacy Code: consultation with parents and carers and primary aged children – qualitative research report,' prepared by Lisa Lewers, Moira Callard and Lauren Campbell, 2026

⁸ Alannah & Madeline Foundation, 'Youth Engagement Program workshop on the Children's Online Privacy Code', 2026

⁹ eSmart, Alannah & Madeline Foundation, 'Children's voices and the digital duty of care', upper primary school workshop, Melbourne, December 2025; eSmart, Alannah & Madeline Foundation, 'Year 6 Student Leadership Conference, Victorian LGA', February 2026

¹⁰ eSmart, Alannah & Madeline Foundation, 'Children's Online Privacy Code: consultation, state primary school, Adelaide', 2026

¹¹ Alannah & Madeline Foundation, 'Youth advocacy program: insights report for Year 1 implementation 2025,' March 2026

¹² Lewers Research, 'The Draft Children's Online Privacy Code: consultation with parents and carers and primary aged children – qualitative research report,' prepared by Lisa Lewers, Moira Callard and Lauren Campbell, 2026

¹³ Alannah & Madeline Foundation, 'Youth Engagement Program workshop on the Children's Online Privacy Code', 2026

¹⁴ eSmart, Alannah & Madeline Foundation, 'Children's Online Privacy Code consultation with Years 2 and 3 students', Melbourne independent primary school, 2026

¹⁵ eSmart, Alannah & Madeline Foundation, 'Children's Online Privacy Code small-group workshop, home education students,' May 2026

¹⁶ eSmart, Alannah & Madeline Foundation, 'Children's Online Privacy Code: consultation, state primary school, Adelaide', 2026; eSmart, Alannah & Madeline Foundation, 'Children's Online Privacy Code small-group workshop, home education students,' May 2026; eSmart, Alannah & Madeline Foundation, 'Children's voices and the digital duty of care', upper primary school workshop, Melbourne, December 2025; eSmart, Alannah & Madeline Foundation, 'Year 6 Student Leadership Conference, Victorian LGA', February 2026; Lewers Research for Alannah & Madeline Foundation, 'The Draft Children's Online Privacy Code:

consultation with parents and carers and primary aged children - qualitative research report,' prepared by Lisa Lewers, Moira Callard and Lauren Campbell, 2026

¹⁷ eSmart, Alannah & Madeline Foundation, 'Children's Online Privacy Code consultation with Years 2 and 3 students', Melbourne independent primary school, 2026

¹⁸ eSmart, Alannah & Madeline Foundation, 'Children's Online Privacy Code consultation with Years 2 and 3 students', Melbourne independent primary school, 2026

¹⁹ eSmart, Alannah & Madeline Foundation, 'Children's Online Privacy Code consultation with Years 2 and 3 students', Melbourne independent primary school, 2026

²⁰ eSmart, Alannah & Madeline Foundation, 'Children's Online Privacy Code: consultation, state primary school, Adelaide', 2026

²¹ eSmart, Alannah & Madeline Foundation, 'Children's Online Privacy Code consultation with Years 2 and 3 students', Melbourne independent primary school, 2026; eSmart, Alannah & Madeline Foundation, 'Children's Online Privacy Code: consultation, state primary school, Adelaide', 2026

²² eSmart, Alannah & Madeline Foundation, 'Children's Online Privacy Code: consultation, state primary school, Adelaide', 2026

²³ eSmart, Alannah & Madeline Foundation, 'Children's Online Privacy Code: consultation, state primary school, Adelaide', 2026

²⁴ eSmart, Alannah & Madeline Foundation, 'Children's Online Privacy Code: consultation, state primary school, Adelaide', 2026; eSmart, Alannah & Madeline Foundation, 'Children's Online Privacy Code small-group workshop, home education students,' May 2026; eSmart, Alannah & Madeline Foundation, 'Children's voices and the digital duty of care', upper primary school workshop, Melbourne, December 2025; eSmart, Alannah & Madeline Foundation, 'Year 6 Student Leadership Conference, Victorian LGA', February 2026; Lewers Research for Alannah & Madeline Foundation, 'The Draft Children's Online Privacy Code: consultation with parents and carers and primary aged children - qualitative research report,' prepared by Lisa Lewers, Moira Callard and Lauren Campbell, 2026

²⁵ eSmart, Alannah & Madeline Foundation, 'Children's voices and the digital duty of care', upper primary school workshop, Melbourne, December 2025

²⁶ Alannah & Madeline Foundation, 'Youth advocacy program: insights report for Year 1 implementation 2025,' March 2026

²⁷ Alannah & Madeline Foundation, 'Youth Engagement Program workshop on the Children's Online Privacy Code', 2026

²⁸ Alannah & Madeline Foundation, 'Youth Engagement Program workshop on the Children's Online Privacy Code', 2026

²⁹ Lewers Research for Alannah & Madeline Foundation, 'The Draft Children's Online Privacy Code: consultation with parents and carers and primary aged children - qualitative research report,' prepared by Lisa Lewers, Moira Callard and Lauren Campbell, 2026

³⁰ eSmart, Alannah & Madeline Foundation, 'Year 6 Student Leadership Conference, Victorian LGA', February 2026

³¹ eSmart, Alannah & Madeline Foundation, 'Children's Online Privacy Code small-group workshop, home education students,' May 2026

³² Lewers Research for Alannah & Madeline Foundation, 'Upholding children's right to privacy online: qualitative research report,' 2025; eSmart for Alannah & Madeline Foundation, consultation, state primary school in Adelaide, 2026

³³ eSmart, Alannah & Madeline Foundation, 'Children's voices and the digital duty of care', upper primary school workshop, Melbourne, December 2025

³⁴ Alannah & Madeline Foundation, 'Youth advocacy program: insights report for Year 1 implementation 2025,' March 2026

³⁵ Alannah & Madeline Foundation, 'Youth Engagement Program workshop on the Children's Online Privacy Code', 2026; Alannah & Madeline Foundation, 'Youth advocacy program: insights report for Year 1 implementation 2025,' March 2026

³⁶ Alannah & Madeline Foundation, 'Youth advocacy program: insights report for Year 1 implementation 2025,' March 2026

³⁷ Alannah & Madeline Foundation, 'Youth advocacy program: insights report for Year 1 implementation 2025,' March 2026

³⁸ Alannah & Madeline Foundation, 'Youth Engagement Program workshop on the Children's Online Privacy Code', 2026

-
- ³⁹ Alannah & Madeline Foundation, 'Youth Engagement Program workshop on the Children's Online Privacy Code', 2026
- ⁴⁰ Lewers Research for Alannah & Madeline Foundation, 'The Draft Children's Online Privacy Code: consultation with parents and carers and primary aged children - qualitative research report,' prepared by Lisa Lewers, Moira Callard and Lauren Campbell, 2026
- ⁴¹ Alannah & Madeline Foundation, 'Youth Engagement Program workshop on the Children's Online Privacy Code', 2026
- ⁴² Alannah & Madeline Foundation, 'Youth Engagement Program workshop on the Children's Online Privacy Code', 2026
- ⁴³ Lewers Research for Alannah & Madeline Foundation, 'Upholding children's right to privacy online: qualitative research report,' 2025
- ⁴⁴ eSmart, Alannah & Madeline Foundation, 'Safe Kids are eSmart Kids: lower primary school co-design results, external report,' August 2024
- ⁴⁵ eSmart, Alannah & Madeline Foundation, 'Children's voices and the digital duty of care', upper primary school workshop, Melbourne, December 2025; eSmart, Alannah & Madeline Foundation, 'Year 6 Student Leadership Conference, Victorian LGA', February 2026
- ⁴⁶ eSmart, Alannah & Madeline Foundation, 'Children's Online Privacy Code small-group workshop, home education students,' May 2026. Also eSmart, Alannah & Madeline Foundation, 'Children's Online Privacy Code: consultation, state primary school, Adelaide', 2026
- ⁴⁷ Lewers Research for Alannah & Madeline Foundation, 'The Draft Children's Online Privacy Code: consultation with parents and carers and primary aged children - qualitative research report,' prepared by Lisa Lewers, Moira Callard and Lauren Campbell, 2026
- ⁴⁸ Alannah & Madeline Foundation, 'Youth Engagement Program workshop on the Children's Online Privacy Code', 2026
- ⁴⁹ Lewers Research for Alannah & Madeline Foundation, 'The Draft Children's Online Privacy Code: consultation with parents and carers and primary aged children - qualitative research report,' prepared by Lisa Lewers, Moira Callard and Lauren Campbell, 2026
- ⁵⁰ eSmart, Alannah & Madeline Foundation, 'Children's voices and the digital duty of care', upper primary school workshop, Melbourne, December 2025; eSmart, Alannah & Madeline Foundation, 'Safe Kids are eSmart Kids: lower primary school co-design results, external report,' August 2024; eSmart, Alannah & Madeline Foundation, 'Year 6 Student Leadership Conference, Victorian LGA', February 2026; Lewers Research for Alannah & Madeline Foundation, 'Upholding children's right to privacy online: qualitative research report,' 2025
- ⁵¹ eSmart, Alannah & Madeline Foundation, 'Children's voices and the digital duty of care', upper primary school workshop, Melbourne, December 2025; Lewers Research for Alannah & Madeline Foundation, 'Upholding children's right to privacy online: qualitative research report,' 2025
- ⁵² eSmart, Alannah & Madeline Foundation, 'Children's voices and the digital duty of care', upper primary school workshop, Melbourne, December 2025
- ⁵³ eSmart, Alannah & Madeline Foundation, 'Children's Online Privacy Code small-group workshop, home education students,' May 2026
- ⁵⁴ Alannah & Madeline Foundation, 'Youth advocacy program: insights report for Year 1 implementation 2025,' March 2026
- ⁵⁵ Alannah & Madeline Foundation, 'Youth advocacy program: insights report for Year 1 implementation 2025,' March 2026
- ⁵⁶ Lewers Research for Alannah & Madeline Foundation, 'The Draft Children's Online Privacy Code: consultation with parents and carers and primary aged children - qualitative research report,' prepared by Lisa Lewers, Moira Callard and Lauren Campbell, 2026
- ⁵⁷ Lewers Research for Alannah & Madeline Foundation, 'Upholding children's right to privacy online: qualitative research report,' 2025
- ⁵⁸ Lewers Research for Alannah & Madeline Foundation, 'The Draft Children's Online Privacy Code: consultation with parents and carers and primary aged children - qualitative research report,' prepared by Lisa Lewers, Moira Callard and Lauren Campbell, 2026
- ⁵⁹ Alannah & Madeline Foundation, 'Youth Engagement Program workshop on the Children's Online Privacy Code', 2026
- ⁶⁰ Alannah & Madeline Foundation, 'Youth Engagement Program workshop on the Children's Online Privacy Code', 2026

⁶¹ eSmart, Alannah & Madeline Foundation, 'Children's voices and the digital duty of care', upper primary school workshop, Melbourne, December 2025; eSmart, Alannah & Madeline Foundation, 'Children's Online Privacy Code small-group workshop, home education students,' May 2026; eSmart, Alannah & Madeline Foundation, 'Year 6 Student Leadership Conference, Victorian LGA', February 2026

⁶² eSmart, Alannah & Madeline Foundation, 'Children's Online Privacy Code small-group workshop, home education students,' May 2026; eSmart, Alannah & Madeline Foundation, 'Year 6 Student Leadership Conference, Victorian LGA', February 2026

⁶³ Lewers Research for Alannah & Madeline Foundation, 'Upholding children's right to privacy online: qualitative research report,' 2025

⁶⁴ eSmart, Alannah & Madeline Foundation, 'Children's Online Privacy Code: consultation, state primary school, Adelaide', 2026

⁶⁵ Alannah & Madeline Foundation, 'Youth Engagement Program workshop on the Children's Online Privacy Code,' 2026

⁶⁶ Lewers Research for Alannah & Madeline Foundation, 'The Draft Children's Online Privacy Code: consultation with parents and carers and primary aged children - qualitative research report,' prepared by Lisa Lewers, Moira Callard and Lauren Campbell, 2026

⁶⁷ Alannah & Madeline Foundation, 'Youth Engagement Program workshop on the Children's Online Privacy Code,' 2026

⁶⁸ Lewers Research for Alannah & Madeline Foundation, 'The Draft Children's Online Privacy Code: consultation with parents and carers and primary aged children - qualitative research report,' prepared by Lisa Lewers, Moira Callard and Lauren Campbell, 2026

⁶⁹ Lewers Research for Alannah & Madeline Foundation, 'The Draft Children's Online Privacy Code: consultation with parents and carers and primary aged children - qualitative research report,' prepared by Lisa Lewers, Moira Callard and Lauren Campbell, 2026

⁷⁰ Lewers Research for Alannah & Madeline Foundation, 'The Draft Children's Online Privacy Code: consultation with parents and carers and primary aged children - qualitative research report,' prepared by Lisa Lewers, Moira Callard and Lauren Campbell, 2026

⁷¹ Alannah & Madeline Foundation, 'Youth Engagement Program workshop on the Children's Online Privacy Code,' 2026

⁷² eSmart, Alannah & Madeline Foundation, 'Safe Kids are eSmart Kids: lower primary school co-design results, external report,' August 2024

⁷³ eSmart, Alannah & Madeline Foundation, 'Children's Online Privacy Code small-group workshop, home education students,' May 2026; eSmart, Alannah & Madeline Foundation, 'Children's voices and the digital duty of care', upper primary school workshop, Melbourne, December 2025; eSmart, Alannah & Madeline Foundation, 'Year 6 Student Leadership Conference, Victorian LGA', February 2026

⁷⁴ eSmart, Alannah & Madeline Foundation, 'Children's Online Privacy Code: consultation, state primary school, Adelaide', 2026; eSmart, Alannah & Madeline Foundation, 'Children's Online Privacy Code small-group workshop, home education students,' May 2026; eSmart, Alannah & Madeline Foundation, 'Children's voices and the digital duty of care', upper primary school workshop, Melbourne, December 2025; Lewers Research for Alannah & Madeline Foundation, 'Upholding children's right to privacy online: qualitative research report,' 2025

⁷⁵ eSmart, Alannah & Madeline Foundation, 'Children's Online Privacy Code: consultation, state primary school, Adelaide', 2026; Lewers Research for Alannah & Madeline Foundation, 'Upholding children's right to privacy online: qualitative research report,' 2025

⁷⁶ Alannah & Madeline Foundation, 'Youth advocacy program: insights report for Year 1 implementation 2025,' March 2026

⁷⁷ Lewers Research for Alannah & Madeline Foundation, 'The Draft Children's Online Privacy Code: consultation with parents and carers and primary aged children - qualitative research report,' prepared by Lisa Lewers, Moira Callard and Lauren Campbell, 2026

⁷⁸ Lewers Research for Alannah & Madeline Foundation, 'Upholding children's right to privacy online: qualitative research report,' 2025

⁷⁹ Alannah & Madeline Foundation, 'Youth advocacy program: insights report for Year 1 implementation 2025,' March 2026

⁸⁰ Lewers Research for Alannah & Madeline Foundation, 'The Draft Children's Online Privacy Code: consultation with parents and carers and primary aged children - qualitative research report,' prepared by Lisa Lewers, Moira Callard and Lauren Campbell, 2026

⁸¹ Lewers Research for Alannah & Madeline Foundation, 'The Draft Children's Online Privacy Code: consultation with parents and carers and primary aged children - qualitative research report,' prepared by Lisa Lewers, Moira Callard and Lauren Campbell, 2026

⁸² Lewers Research for Alannah & Madeline Foundation, 'The Draft Children's Online Privacy Code: consultation with parents and carers and primary aged children - qualitative research report,' prepared by Lisa Lewers, Moira Callard and Lauren Campbell, 2026

⁸³ Alannah & Madeline Foundation, 'Youth Engagement Program workshop on the Children's Online Privacy Code', 2026