



Children's Online Privacy Code

Submission by the Alannah & Madeline Foundation

June 2026

Contents

Executive summary	3
About us.....	4
Recommendations.....	5
A very wide range of online services handle children’s data	7
Commercial targeting and profiling of children leads to exploitation and harm.....	8
Children’s privacy is undermined by ‘dark patterns’	9
Children also face interpersonal privacy risks.....	10
Parents and carers cannot manage digital risks alone	10
Parents and carers strongly support the need for the Code and have many ideas.....	10
Children want a Code to protect their privacy.....	12
Children have rights to privacy protection.....	13
Very vulnerable children need systems-level protection the most	13
The Code should be backed by appropriate resources	13
‘Personal information’ should be defined expansively	14
The Code should be communicated clearly to industry and the public	14

Executive summary

The Alannah & Madeline Foundation (the Foundation) welcomes the opportunity to comment on the draft of the Children's Online Privacy Code (the Code) by the Office of the Australian Information Commissioner (OAIC).

The Code represents a once-in-a-generation opportunity to reshape the digital environment into one where children can thrive, rather than be exploited or exposed to harm. We strongly support the OAIC's approach and urge bold, decisive leadership in finalising the Code. It must provide the strongest protections possible within the existing legislation and the Australian Privacy Principles.

Children are engaging with digital technologies from a very young age – for example, 84% of Foundation / Prep students use tablets.¹ While most families encourage children's responsible device use, many find it difficult to navigate the digital environment with confidence. Only one in ten parents report being very aware of how handling of children's data is regulated.²

It is neither fair nor realistic to expect children to understand or manage complex commercial data-handling practices or design features that undermine privacy. Nor can parents and carers reasonably be expected to shoulder this burden alone in a digital environment which many adults find opaque and disempowering.

Children's personal information is being collected, stored, used and disclosed in ways families often cannot easily understand, challenge or control. These practices are frequently reinforced by manipulative design features. As a result, children are exposed to significant risks and harms including tracking and profiling for targeted advertising; 'dark patterns' that lead towards poor privacy choices; the use of children's images to feed generative AI; and unwanted contact with strangers via recommender systems, weak or non-existent default privacy settings and geolocation features. Strong regulation is long overdue.

A robust Code would help to prevent and mitigate these harms while aligning with clear community expectations. Children and their parents and carers express strong support for the need for a Code.³ There is strong public support for government regulation of how industry handles children's data, while trust in technology companies to self-regulate remains very low.⁴

The Foundation strongly supports the draft Code, especially the '**best interests of the child**' principle, anchored in the *United Nations Convention on the Rights of the Child*. We also welcome the focus on protecting children from commercial profiling and manipulative design practices, including 'dark patterns'.

Effective implementation of the Code requires appropriate resourcing. The regulator must be equipped to provide expert guidance to industry, inform children and adults about their rights, monitor industry compliance, foster accountability, intervene effectively and appropriately to address concerns, and assess the Code's impact, including through meaningful engagement with children.

The Foundation supports the 14 draft rules, while recommending further strengthening to ensure:

- **Coverage of all relevant online services** that handle children's personal information, alongside a broad and future-proofed definition of 'personal information' that reflects the diverse and evolving ways children's data is collected and used.
- **High privacy by default and design.** Any age assurance measures should only be triggered where a user seeks to reduce/lower their protections, and as such must be data-minimising, ethical, accessible and appropriately reliable.
- **Stronger protections from interpersonal privacy risks and harms** - which children themselves and their parents and carers consistently identified as a priority.

- **Clarity that consent does not displace the best interest of the child** – a child's agreement to data handling cannot override an online service's obligation to act in accordance with that principle: children cannot be asked to 'consent' their rights away.
- **A clear commitment to the full spectrum of children's rights**, including rights to education, information-seeking, and freedom of expression. The Code should protect children's privacy in digital environments, not exclude them from participating in those environments altogether.

Our advocacy is informed by engagement with primary students, secondary students, young adults, and parents and carers, undertaken between 2024 and 2026. The parent sections of this submission contain detailed feedback on the draft Code from parents and carers of primary-aged children.

This submission is accompanied by a separate, standalone 'child and youth voice' document so the OAIC can hear directly from those children and young people, in their own words and in full.

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.

Recommendations

Implement the 14 rules of the draft Code, while strengthening the Code in the following ways:

1. Ensure the definition of 'personal information' is as expansive as it can be within the Privacy Act, including, to the extent possible, information about a child that has been inferred or generated.
2. Apply the Code to all businesses that affect children's privacy rights in relation to the digital environment, not limited to those which self-assess their primary purpose as being social media services, relevant electronic services or designated internet services. **(Rule 1)**
3. Apply the health service exemption only to online services which are appropriately accredited and regulated. **(Rule 1)**
4. Take the position that online services should provide all end-users with high privacy protection by default, estimating or verifying age only in the event that an end-user wishes to lower their protection. **(Rule 2)**
5. Specify that any mechanisms for age assurance or establishment of parental responsibility must demonstrate data-minimisation, show a high standard of ethics and accessibility, and show accuracy, reliability and robustness appropriate to the level of risk present. **(Rules 2 and 5)**
6. Communicate clearly to industry and the public that the purpose of any mechanisms for age assurance and/or parental consent adopted under the Code should be to ensure that children's personal information is protected appropriately within online services, not to exclude children from services that are legal for them to use. **(Rules 2 and 5)**
7. In line with the Online Safety Amendment (Social Media Minimum Age) Act 2024, require that online services may not collect government-issued identification material for purposes of age assurance or parental consent unless the service also provides reasonable alternative means. **(Rules 2 and 5)**
8. Clarify that children must be able to access online services that are legal for them to use while enjoying high privacy protections ie. access should not be contingent on losing privacy. **(Rule 3)**
9. In line with the UK Children's Code Standard 7, specify that the requirement for data minimisation and privacy by default must cover how children's personal data is handled in an interpersonal sense eg. the extent to which other end-users of an online service may see children's data and contact children – as well as the handling of children's data by the service itself and any third parties. **(Rule 3)**
10. Specify that online services should collect and retain only the minimum personal data needed to provide the elements of the service in which a child is actively and knowingly engaged, in line with the UK Children's Code, Standard 8. **(Rule 3)**
11. Require appropriate transparency reporting (potentially as part of an online registry of privacy impact assessments, see Rule 14) so that children, parents, carers and civil society can understand how entities assess and act upon the 'best interests of the child' principle in relation to children's data. **(Rule 4)**

12. End the profiling of children for targeted marketing, especially the targeted marketing of harmful and high-risk products to children. To the extent possible, restrict the functions of online services that currently serve to maximise children's exposure and receptiveness to targeted marketing, including targeting of content and contacts and 'sticky' design features. **(Rule 4)**
13. Clarify that any consent given by children or parents to children's data being collected, used or shared must not override the expectations that data-handling will be consistent with the best interests of the child and that children's privacy will not be unlawfully or arbitrarily invaded. **(Rules 5 and 6)**
14. Require that children, parents and carers be given information about data-handling and consent which is clear, honest, ethical, accessible to users with disabilities, age-appropriate, digestible, and timely. **(Rules 5, 6, 8 and 9)**
15. If possible, require standardisation of how the above information is presented to make it as accessible as possible for families who use multiple online services – see Proposal 10.3 of the Privacy Act Review Report, agreed to in principle by the Australian Government. **(Rules 5, 6, 8 and 9)**
16. Require the use of 'fair patterns' instead of 'dark patterns' when dealing with children's personal information. Fair patterns should include high-privacy and consumer-friendly options by default; easy, accessible pathways for users to lift their privacy protections; and easy, accessible ways for children, parents and carers to contact the company to find out more about their data rights. **(Rule 7)**
17. As in the UK Children's Code, Standard 13, encourage pro-privacy 'nudge' techniques where appropriate, taking into account the best interests of the child at different ages. **(Rule 7)**
18. Require entities to respond promptly upon receiving a request from a child or parent to see, change or delete the child's data. Children and parents told us that 30 days is too long to wait. Online services should also be required to provide an immediate receipt in clear, accessible language, explaining the process ahead and linking to external supports such as eSafety's reporting portal, Kids Helpline, the Australian Centre to Counter Child Exploitation, and Triple Zero in an emergency. Linking to support services swiftly is important because it is likely some requests will be triggered by a child experiencing online harm eg. stalking, doxxing, deepfakes. **(Rule 10)**
19. Require that any alerts which notify children of the presence of geolocation tracking must be clear, accessible, age-appropriate, and accompanied by simple, child-friendly pathways to stop unwanted people seeing the child's location and to seek help for any concerns. **(Rule 12)**
20. Require that reporting and complaint mechanisms must be free, safe, confidential, responsive, child-friendly, effective, accessible, prompt, and link to appropriate external support services. **(Rule 13)**
21. Require that, subject to appropriate safeguards, online services with high reach and/or risk may be required to share data with authorised independent researchers for the purpose of understanding the services' alignment with the Code and the outcomes of privacy impact assessments. **(Rule 14)**
22. Provide high-quality guidance to help online services to assess risks to children that may arise from their handling of children's data, to identify and act upon the best interests of the child, and to adopt reasonable, proportionate approaches to establishing age and parental consent.
23. Disseminate succinct, clear, accessible, relevant information about the Code to children, parents, carers and educators (school and early childhood), leveraging where possible the trusted roles of schools, regulators,

government agencies, child safety organisations and independent experts like psychologists. Topics to cover include: which problems the Code does and does not address; whom the Code applies to (eg. not individual parents); and how the Code differs from the social media age delay.

24. Allocate appropriate resources for the implementation of the Code, responsive to the scale of the problem and informed by the findings of the UK Information Commissioner's Office in their interim impact review into their Children's Code.⁵
 - a. Prioritise early monitoring and enforcement on services with high reach and/or high risk to children, including those using profiling, recommender systems, geolocation or other practices that create heightened privacy and safety risks.
 - b. Implement the Code through a phased, risk-based rollout, beginning with an initial transition period supported by clear guidance, practical compliance tools and early engagement with industry.

A very wide range of online services handle children's data

Australian children use digital technologies from a very young age. For example, our survey of 1,000 parents and carers of primary students found that 84% of Prep / Foundation students used tablets, 45% used smartphones (their own or someone else's), 34% used gaming consoles, 34% used laptops, 13% used smart speakers, and 7% used wearables.⁶

When we spoke with 324 lower primary students in Victoria, Tasmania and South Australia in 2024, they told us all Years 1-3 students had used a tablet. Gaming was very popular; all Years 1-3 students had played a game online and 77% of Prep / Foundation students said they knew where and how to download games. YouTube was also popular: 78% of Prep / Foundation students had watched a YouTube video.⁷

As children grow, tech use increases and diversifies. For example, last year, we asked Years 3-5 students at a Melbourne primary school what digital technologies students used in a typical week. Their responses included shopping apps, streaming platforms, games, creative apps, edtech, messaging services, social media and search engines. Many of these services, if not most, were not aimed specifically at children.⁸

With many families facing cost-of-living pressures, children's use of digital technologies may increase further. Parents have told us that part of the appeal of online activities like gaming and streaming is that they are relatively cheap or 'free'.⁹

Meanwhile, technologies continue to emerge and evolve, sharing user data widely across multi-product ecosystems.¹⁰

As such, we welcomed the OAIC's proposal that the Code cover services likely to be accessed by children and services primarily concerned with the activities of children. The OAIC has recognised the reality that children's lives are affected by a wide range of technologies, many of which are not aimed solely at children as end-users.

In particular, we appreciate the OAIC's recognition of online services used in early childhood education and care services, a sensitive matter that requires close attention. Early Childhood Australia's recent 'Statement on young children and digital technologies' presents an opportunity for alignment, urging providers to develop policies and guidelines about the collection, use, retention and deletion of digital data held about young children and communicate these to families.¹¹

However, we have some concerns about limiting the Code to social media services, relevant electronic services and designated internet services. These categories are often assumed to refer to messaging services, gaming, social media, websites and apps,¹² which are not the only forms of technology that handle children's data. We gather that

the categories may prove broader for the purposes of the Code, possibly encompassing things like app distribution services and AI providers that produce connected toys. This would be very positive. However, we are concerned that problems will arise if companies are left to self-assess the categories of their online services based on primary purpose. A more objective, robust approach to categorisation is needed.

A comprehensive scope would also fit better with the vision of the Privacy Act review, which proposed that the Code should align to the extent possible with the UK Children's Code, which has a broad scope including search engine services, online marketplaces, and connected toys and devices.¹³

Meanwhile, entities providing a health service are exempt from the draft Code. There are valid reasons for this, but we trust this exemption will be applied with caution, given the proliferation of commercial for-profit online services which claim to enhance users' health and wellbeing. Many of these are used by children and many may not be appropriately regulated as regards data-handling.

For example, almost a third of teenage sporting participants in Australia use apps for tracking their activity or training, while apps for monitoring infant health and development are common among new parents.¹⁴ Historically, regulation of such products has been thin. Concerns have been raised about products handling cognitive and neural data, sharing consumer data with third parties, targeting users with personalised advertising, 'bundling' data-handling consent, and having opaque privacy policies.¹⁵

Meanwhile, serious concerns have been raised about commercial 'companion AI' products impersonating the dynamics of mental health interventions, sometimes with dangerous results.¹⁶ One study found that 12% of teens who use AI companions use them for emotional or mental health support.¹⁷ Such common, high-risk technologies must not be permitted to slip through regulatory cracks.

Commercial targeting and profiling of children leads to exploitation and harm

For decades, advertisers have treated children as a lucrative market, due to children's relatively low impulse control, developing tastes, and limited understanding of commercial 'persuasion'. In today's digital environment, children are more vulnerable than ever. This is partly because marketing has become more compelling eg. gamified ads, 'unboxing' videos, social media contests, interactivity prompts, paid content, and promotion of products by influencers.¹⁸ Children's higher vulnerability nowadays is also due to targeting.

Targeted advertising is driven by the collection of children's data – including location, purchases, viewing history, contacts, preferences and responses – and the sharing of that data with third-party companies to develop user profiles. This process can threaten children's rights to privacy, freedom of thought, and protection from exploitation. Depending on the products promoted, targeting may also increase risks to children's health, behaviour and relationships.¹⁹

For example, whistleblowers have recalled social media companies telling advertisers they could increase sales by targeting products to teens at points when the teens' online behaviour suggested they were feeling vulnerable.²⁰ Platforms have been caught identifying for marketing purposes teens whose activities suggested receptiveness to gambling, alcohol, smoking, vaping, extreme weight loss, adult entertainment, and online dating.²¹ Meanwhile, some researchers have found that children are bombarded with junk food advertising online and that teens are shown advertising for alcohol and gambling on a daily basis.²² This poses risks to children's health, relationships and finances.

More broadly, we are concerned about companies targeting content and contacts to children in ways that serve to maximise children's exposure and receptiveness to marketing eg. by making online services distracting and compelling and encouraging emotions like anxiety and low self-esteem which advertisers can leverage.

When researchers set up avatar 'teen' accounts, they found that showing an interest in any topic led to many similar recommendations, with recommended content quickly becoming more extreme.²³ Teen boys were recommended pornographic content and contacts within hours of setting up an account.²⁴ Boys who showed an interest in gaming were recommended large amounts of firearm content; one account purporting to belong to a 14-year-old American boy was recommended 1,300 firearm-related videos in one month.²⁵ Meanwhile, girls who showed an interest in mental health issues were bombarded with depression, anxiety and self-harm content.²⁶ At the same time, design features which maximise engagement have left children feeling distracted, agitation, anxious, lonely, and affected by dopamine 'highs and lows'.²⁷

In response to such concerns, General Comment 25 of the United Nations Convention on the Rights of the Child urges, 'States parties should prohibit by law the profiling or targeting of children of any age for commercial purposes on the basis of a digital record of their actual or inferred characteristics, including group or collective data, targeting by association or affinity profiling.'²⁸

Recently, there have been attempts to protect children through age-gating of sites and apps which are inappropriate for children to use. This approach has benefits but can pose new threats to privacy if the age assurance mechanisms are of poor quality.²⁹ We find that age assurance is mistrusted by many children and young people.

For sites and apps which are legal for children to use, we think it is preferable for all users to be provided with high privacy protections by default, with age estimation or verification only activated in the event that a user wishes to lower their protection.

Children's privacy is undermined by 'dark patterns'

Children are vulnerable to 'dark patterns' online: a term used to describe design practices that trick or manipulate users into making choices which they would not otherwise make and which may not be in their best interests. These patterns hijack users' cognitive biases or weaknesses to 'steer' decision-making, usually for someone else's commercial gain.³⁰ Dark patterns can cause loss of money, time and/or privacy, cognitive burden, degraded online experiences, erosion of choice, and loss of consumer trust.³¹

Dark patterns include pressuring users to 'choose' low-privacy options through repeated prompts, time pressure, emotional appeals, visual design, trick questions or pre-ticked boxes; defaulting to low-privacy options; making high-privacy options seem cumbersome or unattractive; obstructing access to information; overloading users with confusing information; collecting more data than necessary; and making accounts or subscriptions difficult to close or cancel.³²

Unfortunately, dark patterns are very common. One Canadian 'sweep' of 145 websites and apps found that 99% contained at least one indicator of deceptive design,³³ while an Australian survey found that 95% of adults who played online games had, in the past 12 months, encountered at least one dark pattern in a game.³⁴ Another project found that, on an average day, Australians would need to spend half an hour to find and adjust privacy settings to maximum protection on all the sites and apps used, plus 14 hours to read all the privacy policies.³⁵

Dark patterns seem to be especially common on sites and apps aimed at children.³⁶ The Canadian 'sweep' found that children's sites and apps were more likely than others to 'nag' users for personal information, 'confirm-shame' to discourage users from deleting accounts, and prioritise sign-up options over options to continue without an account.³⁷

As such, it is unsurprising that most Australian adults and children do not usually read or understand policies about privacy and data use.³⁸ When asked what stopped them from understanding the handling of their children's data, a third of Australian parents say they are unsure where to find the information and almost 3 in 10 say the information is too complicated and difficult to understand.³⁹ The majority of Australian parents and teens say they are confused or unclear about how to protect children's personal information online.⁴⁰

Children also face interpersonal privacy risks

Inappropriate design and data-handling by online services can also raise interpersonal risks to children's privacy. Primary students have told us repeatedly that their biggest privacy concerns are about contact risks: strangers, bullies, scammers, hackers, stalkers, people who behave badly.⁴¹

Such concerns are valid. eSafety found that 55% of children aged 8-17 had been in contact with someone they first met online.⁴² Approx. 1 in 12 children said their location had been tracked by someone without their permission.⁴³ Of children who played online games, almost 1 in 20 said someone had contacted them repeatedly in a game against the child's wishes.⁴⁴ A survey of American girls aged 11-15 found that only 18% believed location-sharing features on social media had a mostly positive effect.⁴⁵

Tragically, around 1 in 6 young Australians aged 16-24 say they were sexually solicited online by an adult during childhood; the vast majority of the perpetrators were strangers.⁴⁶ Use of digital technologies to track children's location also occurs in many cases of family and domestic violence.⁴⁷

At present, it is unclear to us whether the data minimisation approach articulated in Rule 3 of the draft Code also implies that interpersonal privacy measures must be set to their highest level by default for child end-users. We urge that such a requirement be articulated clearly, as in Standard 7 of the UK Children's Code.

We also think it urgent that any notifications alerting children to geolocation tracking should assist children to protect their privacy, too, and manage their concerns about the matter. It is not enough to tell children that a potential problem exists; as primary students explained to us, this might just cause further confusion, worry and fear. Children must be empowered with appropriate information and support pathways to resolve the problem.

Parents and carers cannot manage digital risks alone

Parents and carers tell us that while they try to keep their children safe online, many feel confused, tired and disempowered. Only 1 in 10 parents we surveyed said they were very aware of regulations governing children's data privacy, and 73% said they had less understanding than they would like about the data that online platforms might collect in relation to their children.⁴⁸

In a recent workshop, parents and carers of primary-aged children shared firsthand experiences of data breaches and 'near-misses' and lamented the difficulty of monitoring their children's online activity adequately.

One parent commented *'Kids need more protection, with usual households having both parents working with the cost of living, we sometimes tune out the online interactions that kids have.'*⁴⁹

Education for families, while important, is not enough in an environment where digital tech use is almost mandatory, data-handling is maximised by design, and meaningful consumer choice is limited. This situation can only be changed through systems reform.

Parents and carers strongly support the need for the Code and have many ideas

In 2025, we commissioned a survey of 1,000 parents and carers of primary-aged children and found they overwhelmingly wanted stronger regulation to protect children's data. More than 8 in 10 believed it was primarily government's responsibility to set legislation and industry standards about regulation and safeguarding of children's online privacy and data usage. There was little appetite for industry self-regulation. Almost two-thirds of parents felt low trust or no trust in tech companies.⁵⁰

This year, we commissioned in-depth qualitative sessions with 38 parents and carers of primary aged children to discuss the draft Code. They strongly supported the need for the Code and wanted it to apply comprehensively, to require online services to:

- collect minimal information from children
- permanently delete personal information when requested
- not trick, pressure or confuse children
- ask for permission before data is shared, from both the parent and child if appropriate
- not allow other users to see a child's location or contact a child without parental permission.⁵¹

Parents and carers supported the Code being led by the OAIC – seen as independent, credible and consistent – rather than by industry, whose interests may conflict with children's.

They envisaged the OAIC holding online services accountable, enforcing penalties, conducting audits and monitoring, responding quickly to concerns, reviewing and updating the Code, and educating the public.

The greatest privacy concerns for parents and carers were predators gaining access to their children, misuse of children's data, targeted advertising to children, and children's exposure to inappropriate content. (We realise the Code does not address the last one, but it serves as a reminder of what parents are navigating.)

Parents and carers were uncomfortable with collection of information about their children including photos and location, especially when this occurred without the family's clear understanding and consent. They were frustrated with the lack of transparency about what data is collected, stored and shared and parents' inability to make real decisions about this. They worried about data hacks, leaks, and targeted scams. And they felt uneasy about their children being shown targeted advertising and manipulated by algorithms.

In particular, parents and carers felt strongly that their children's personal information should not be visible or accessible to other service users and that other users should not be able to contact children without parental consent.

Comments from parents and carers included:

- *'I think this [the Code] is a great way to protect our children's privacy online. I definitely think it should have been implemented a lot earlier, especially because there are so many predators online that can access our children's information and use this to their own advantage.'*
- *'For me personally, anything and everything that leaves an online footprint (from their DOB, name, age, residence, living conditions etc.) should be dealt with caution and how those are used and/or misused.'*
- *'This is great that companies are now being held accountable for storing this data. Coming up with a plan like this makes sense. I think it's just a bit of a free for all at the moment.'*
- *'I believe that some of the personal information collected such as photos and videos of the child should not be allowed as there is a risk that this data could get hacked and misused inappropriately such as in the creation of AI generated child pornography.'*
- *'I think this is a fantastic idea that should have been implemented a long time ago. My eldest son once had his bank details taken after buying credits on Robux the next day when he checked his bank account \$60 had been taken from a person who had managed to hack his bank account.'*⁵²

Parents and carers had many questions about how the Code would be actioned and enforced and how online services would be held accountable. Concerns were raised about how children's data would be managed when stored or processed overseas and whether international companies would be effectively regulated.

In response to the rules of the draft Code, parents and carers told us:

- Rule 1: Parents and carers supported the Code applying to all platforms that collect children's data, not just child-facing apps, but queried how it would work and suspected some services would not comply.
- Rule 2: Most parents and carers wanted high default privacy settings for all, seeing this as simpler, safer and more inclusive, rather than age assurance, which they feared could be intrusive and unreliable.
- Rule 3: Parents and carers liked the idea of data minimisation and privacy by design, although they worried it could lead to children and parents having to make confusing choices about their settings.
- Rule 4: Parents and carers strongly supported prioritising children's interests but found the language vague ('best interests', 'fairness') and doubted that online services would do the right thing.
- Rule 5: While parents and carers saw the rule as positive overall, they debated the best age for children to make data decisions. Many wanted older (eg. 16 or 18), but some wanted younger (eg. 13).
- Rule 6: Most parents and carers supported the rule's promise of increased protection and involvement for both parties, but they worried about practical and logistical concerns.
- Rule 7: Parents and carers saw this rule as necessary and positive, stressing the need for clear, upfront communication and protection. They raised questions about implementation, enforcement and consistency between services.
- Rule 8: While parents and carers agreed this rule was important, they raised concerns about complexity and information overload.
- Rule 9: Parents and carers supported this rule, seeing it as sensible and necessary to inform both adults and children of their rights.
- Rule 10: While parents and carers broadly welcomed the promise of a guaranteed response 'window' for accountability and transparency, there was a strong consensus that 30 days was too long, especially for urgent cases.
- Rule 11: Most parents and carers supported this rule, believing it would give them and their children better control, consumer trust, and peace of mind.
- Rule 12: Parents and carers generally supported this rule for promoting transparency, safety and informed consent. They had some concerns about unwieldy notifications, confusion for younger children, and limiting of parental supervision.
- Rule 13: Parents and carers widely viewed this rule as positive but queried how it would function.
- Rule 15: Parents and carers saw this rule as necessary but self-evident.

Parents and carers thought the most important rules (in order) were 3, 11, 7, 1, 5 and 6. They gave lower priority to rules 4, 13 and 14 as they found them less clear and doubted services would follow them.

Parents and carers also made some arguments which the Foundation does not support, but which we reproduce here in good faith to alert the OAIC of the range of views in the community. In particular:

- some parents worried that the Code would be hard for smaller companies to implement and could lead to commercial problems and poor consumer experiences for adults.
- some parents worried that they themselves might be held 'liable' under the Code eg. that they might be restricted from sharing pictures of their children on social media.
- some parents thought the Code should define children as under-16s to align with the social media age delay.
- some parents wanted to be able to monitor their children online without the children being informed.⁵³

Children want a Code to protect their privacy

We outline our engagements with primary students, secondary students and young adults in a separate report. In summary, most children and young people we consulted told us that they valued and worried about their privacy online, that they did not like the idea of online services using their data for purposes beyond the child's own activities or the services' main purpose, that they wanted meaningful, enforced rules to protect children's personal information, and that they supported most rules in the draft Code at least partly. Their comments included:

- *'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'.⁵⁴*

Children have rights to privacy protection

As an organisation committed to upholding children's rights, we look to the United Nations Convention on the Rights of the Child, Article 16, which states that children have a right to protection from arbitrary or unlawful interference with their privacy.⁵⁵

This right coexists with children's other rights, which include the rights to express their views freely on matters affecting them; to seek, receive and impart information; to exercise freedom of thought; to access high-quality materials which promote the child's wellbeing; to access education that develops the child's talents and abilities; to engage in play and cultural life; and to be protected from all forms of exploitation.⁵⁶

In addition, we look to General Comment 25 of the Convention ('On children's rights in relation to the digital environment'), which states that governments should ensure children's privacy is respected and protected by all organisations that process their data. Any interference with a child's privacy should be lawful, legitimate and proportionate and should uphold data minimisation and the best interests of the child. Governments should require privacy-by-design, prohibit commercial targeting and profiling of children, and prioritise children's best interests in relation to online advertising and marketing. Any consent from children and/or parents for processing of children's data should be informed and given freely. Privacy and data protection legislation and measures should not arbitrarily limit children's other rights.⁵⁷

General Comment 25 adds that children and their parents should be able to easily access stored data, correct inaccurate or outdated data, and delete data stored unnecessarily, subject to reasonable, lawful limitations. Data controllers should provide information on this subject in child-friendly language and accessible formats. When concerns arise, children must have access to reporting and complaint mechanisms which are free, safe, confidential, responsive, child-friendly, effective and accessible.⁵⁸

Many approaches outlined in the draft Code align well with this approach. We strongly support the draft Code's emphasis on the 'best interests of the child' principle, defined in line with Article 3 of the Convention.⁵⁹

Very vulnerable children need systems-level protection the most

Children who already face disadvantage – including children in out-of-home care and children with disability, mental ill health or caring responsibilities – are at elevated risk online. They are less likely than their peers to receive digital literacy education and appropriate supervision and more likely than their peers to encounter risks and harms online, including in relation to privacy and data. These risks include stalking, hacking, scams, fraud, unwanted contacts, over-spending, misuse of their personal images, and compulsive device use.⁶⁰

While these problems have complex causes, they are made worse by weak systemic protection for children's privacy and personal information. Robust regulation could benefit these children especially.

The Code should be backed by appropriate resources

A Code, however excellent, will have limited impact without adequate resources for implementation.

Industry compliance will likely prove challenging; the regulator must be adequately supported. As a crude example, the 2025 annual global revenues for Meta, Alphabet (Google), Microsoft, Apple and Roblox were, respectively,

US\$200.9 billion, \$402.8 billion, \$281.7 billion, \$416 billion, and \$4.9 billion. In contrast, the OAIC's 2024-25 revenue from Government was a little over \$38 million.⁶¹

The implementation of the UK's Children's Code offers lessons in resource allocation. The Children's Code has led to better privacy protections for children on many online services, and its 'wins' are credited in part to resourcing. The strategy for implementing the Code was prioritised internally, with substantial staffing and coordination, involving equivalent 22 FTE staff across 12 departments.⁶²

That strategy's progress was attributed partly to resourcing of areas including research and analysis, theory of change, guidance for industry in targeted areas (eg. age assurance), testing and assessment tools for industry, public communications, and evaluation of impact, as well as 'upstream' interventions with industry (eg. engagement, advice, requests for information) and 'downstream' interventions (eg. audits, compliance monitoring, investigations, fines).⁶³

The Code should be rolled out through a phased, risk-based implementation approach. This should include an initial transition period supported by clear guidance, practical compliance tools and public communication, followed by targeted monitoring and enforcement focused first on high-reach and high-risk services. The OAIC should prioritise likely areas of confusion, including scope, age assurance, parental consent and the application of the best interests of the child principle. Over time, implementation should progress from education and upstream engagement to stronger audits, compliance action and penalties for persistent or serious breaches. The Code should also be reviewed after an initial implementation period to assess effectiveness, identify gaps and ensure it remains responsive to evolving technologies and risks.

Despite positive progress, no digital service operating in the UK has achieved full compliance. Australia must learn from the barriers experienced by the ICO and invest in initiatives to address key problems, including those relating to AI systems, recommender systems, and serious or persistent breaches of the Code.⁶⁴

'Personal information' should be defined expansively

We support the OAIC's framing of children's personal information as encompassing many things, including online activity and imagery as well as contact details and location. This speaks to the framing of personal information in the Privacy Act, which was always intentionally broad.⁶⁵

We trust that the definition underpinning the Code will be as expansive as it can be within the Act and framed in such a way that it is 'future-proofed' – recognising that digital technologies will continue to emerge and evolve in rapid, transformative ways.

Ultimately, in line with the recommendations of the Privacy Act review, personal information in the Code should include that obtained from any source and by any means, including inferred and generated data.⁶⁶

The Code should be communicated clearly to industry and the public

It is important that industry receives relevant, high-quality guidance about key topics. The UK experience indicates these topics will include how to assess and act upon risks in the handling of children's data and the best interests of the child.⁶⁷

Meanwhile, children themselves have a right to clear, age-appropriate, relevant, accessible information about how the Code can help them. Such communications should take into account the following issues:

- Many children and young people struggle to understand commercial data-handling.
- Children and young people are not used to getting real choices about what happens to their data.

- Children and young people have received mixed messages about the collection of their data: this can be portrayed as dangerous, normal, unavoidable, or protective.
- Many children and young people provide fake personal details online as a privacy measure.
- Children and young people experience the digital environment in its entirety, not as a series of discrete issues. Primary students, especially, may assume the Code will address many online threats eg. scams, stranger danger, scary content.

High-quality information for parents and carers is also important. At a consultation we commissioned recently, parents and carers workshopped ways the Code could be communicated effectively. Their ideas included:

- a concise, plain-language version which explains key terminology clearly for parents and carers.
- condensing the rules and presenting them in three groups: general rules (1, 2, 13, 14), personal information rules (3, 4, 9, 10, 11), and permission rules (5, 6, 7, 8).
- enlisting trusted actors to help communicate the Code, such as teachers and schools, government bodies and regulators, child safety organisations, and independent experts eg. psychologists.
- awareness-raising through emails, websites, social media campaigns, school communications, media ads, educational games and messaging for children, and information sessions in person and online.⁶⁸

These ideas echoed those we heard in our 2025 survey of 1,000 parents and carers.⁶⁹

One parent commented *'It has [to] be a collaborative approach by the authorities to bring everyone together with strong set of rules defined by experts on the child safety, academicians, parents/carers, kids, and the lastly the companies themselves. But it has to be backed by laws and regulations to enforce it. In addition, we need to create awareness in kids from a young age through social campaigns.'*⁷⁰

Finally, we believe it is likely the Code will be conflated and confused with the social media age delay. It is vital to communicate clearly to industry and the public that the purpose of any age assurance and/or parental consent mechanisms under the Code is not to prevent children from accessing services that are legal for them to use, but rather to ensure children's personal information is protected when they are using those services.

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

Sarah Davies AM, CEO
sarah.davies@amf.org.au

Ariana Kurzeme, Director, Policy & Prevention
ariana.kurzeme@amf.org.au

Dr Jessie Mitchell, Manager, Advocacy
jessie.mitchell@amf.org.au

¹ Lewers Research for Alannah & Madeline Foundation, 'Upholding children's right to privacy online: final report,' 2025

² Lewers Research for Alannah & Madeline Foundation, 'Upholding children's right to privacy online: quantitative report,' 2025

- ³ For example: Lewers Research for Alannah & Madeline Foundation, 'The Draft Children's Online Privacy Code: Consultation with Parents and Carers of Primary Aged Children - qualitative research report,' prepared by Lisa Lewers, Moira Callard and Lauren Campbell, May 2026
- ⁴ Lewers Research for Alannah & Madeline Foundation, 'Upholding children's right to privacy online: quantitative report'
- ⁵ UK Information Commissioner's Office, 'Children's code strategy: interim impact review,' 2025, <https://ico.org.uk/media2/i2zmf3h5/childrens-code-strategy-interim-impact-review-november-2025.pdf>
- ⁶ Lewers Research for Alannah & Madeline Foundation, 'Upholding children's right to privacy online: final report'
- ⁷ eSmart (Alannah & Madeline Foundation), 'SKeSK: Lower Primary School Co-design results, External report,' 2024
- ⁸ Alannah & Madeline Foundation, 'Children's voices and the digital duty of care,' January 2025, <https://www.alannahandmadeline.org.au/what-we-do/advocacy/policy-submissions>
- ⁹ Lewers Research for Alannah & Madeline Foundation, 'Upholding children's right to privacy online: qualitative report,' 2025
- ¹⁰ Australian Competition & Consumer Commission, 'Digital platform services inquiry,' interim report 7, 2023, <https://www.accc.gov.au/about-us/publications/serial-publications/digital-platform-services-inquiry-2020-25-reports/digital-platform-services-inquiry-september-2023-interim-report>
- ¹¹ Early Childhood Australia, 'ECA Statement on young children and digital technologies,' 2025, <https://www.earlychildhoodaustralia.org.au/advocacy/statements/eca-statement-on-young-children-and-digital-technologies/>
- ¹² Onlinesafety.org.au, 'Consolidated Industry Codes of Practice for the Online Industry, Phase 1,' 2023, <https://onlinesafety.org.au/codes/>
- ¹³ Australian Government, 'Privacy Act Review: Report 2022,' 2023, p.157 <https://www.ag.gov.au/rights-and-protections/publications/privacy-act-review-report>; UK Information Commissioner's Office (ICO), 'Services covered by this code,' accessed 2026, <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/age-appropriate-design-a-code-of-practice-for-online-services/services-covered-by-this-code/#code1>
- ¹⁴ AusPlay, 'Data portal,' accessed 2026, <https://www.ausport.gov.au/clearinghouse/research/ausplay/results>; Digital Child, 'Baby apps - mapping the issues,' 2024, <https://digitalchild.org.au/research/publications/working-paper/baby-apps-mapping-the-issues/>
- ¹⁵ ABC News, 'Mental health apps are largely unregulated in Australia. Some experts fear vulnerable users could be harmed,' 2023, <https://www.abc.net.au/news/2023-06-02/mental-health-app-s-unregulated-cause-user-safety-concerns/102380956>; Edward Musole, The Conversation, 'Wearable devices can now harvest our brain data. Australia needs urgent privacy reforms,' 2024, <https://theconversation.com/wearable-devices-can-now-harvest-our-brain-data-australia-needs-urgent-privacy-reforms-229006>; Jeannie Marie Paterson and Swetha Meenal Ananthapadmanaban Centre for AI and Digital Ethics, University of Melbourne, 'Data privacy and consumer protection Practices of automated mental health, wellbeing and mindfulness mental health, wellbeing and Mindfulness apps report,' 2023, https://www.unimelb.edu.au/_data/assets/pdf_file/0008/4824404/Mental-Health-Apps-Report-updated-17-Dec.pdf; SBS News, 'Millions rely on fitness apps for motivation and guidance. They may do more harm than good,' 2025, <https://www.sbs.com.au/news/article/do-fitness-apps-cause-problematic-food-and-exercise-habits/ydtjhgu3>
- ¹⁶ American Psychological Association, 'Use of generative AI chatbots and wellness applications for mental health,' 2026, <https://www.apa.org/topics/artificial-intelligence-machine-learning/health-advisory-chatbots-wellness-apps>; U.S. PIRG Education Fund, 'The risks of AI companion chatbots as mental health support,' 2026, <https://pirg.org/edfund/resources/ai-chatbot-therapy/>; Sarah Wells, Stanford University Human-Centred Artificial Intelligence, 'Exploring the Dangers of AI in Mental Health Care,' 2025, <https://hai.stanford.edu/news/exploring-the-dangers-of-ai-in-mental-health-care>
- ¹⁷ Common Sense Media, 'Talk, trust and trade-offs: how and why teens use AI companions,' 2025, <https://www.common SenseMedia.org/research/talk-trust-and-trade-offs-how-and-why-teens-use-ai-companions>
- ¹⁸ Australian Prevention Partnership Centre, '#DigitalYouth pilot study: how children are targeted online,' 2025, <https://preventioncentre.org.au/resources/digitalyouth-pilot-study-how-children-are-targeted-online/>; Samuel Levine, 'Protecting kids from stealth advertising in digital media,' Bureau of Consumer Protection for the Federal Trade Commission, 2023,

https://www.ftc.gov/system/files/ftc_gov/pdf/p214505kidsadvertisingstaffperspective092023.pdf ; Jenny Radesky, Yolanda (Linda) Reid Chassiakos, Nusheen Ameenuddin, Dipesh Navsaria, 'Digital Advertising to Children,' *Pediatrics*, vol 146, no 1, 2020, <https://publications.aap.org/pediatrics/article/146/1/e20201681/37013/Digital-Advertising-to-Children>; Jenny Radesky, 'The digital world is built on advertising. How do we help kids navigate it?', CNN, 2021, https://edition.cnn.com/2021/05/18/health/kids-digital-advertising-wellness/index.html?utm_source=chatgpt.com ; VicHealth, 'Under the radar: harmful industries' digital marketing to Australian children,' 2020, <https://www.vichealth.vic.gov.au/sites/default/files/Under-the-radar--Harmful-industries-digital-marketing-to-Australian-children.pdf>

¹⁹ Better Internet for Kids, 'Manipulative digital marketing practices targeted at children and youth online: rights and responsibilities under the existing EU legal framework,' 2024, https://better-internet-for-kids.europa.eu/sites/default/files/2024-08/AdWiseOnline_Research%20report_Manipulative%20Digital%20Marketing%20Practices%20targeted%20at%20children%20and%20youth%20online.pdf ; J. Harris, L. Reed, S. Maksi, S. Ananthan, G. Chenault, M. Story, M. Lott, 'Evidence-Based Recommendations to Mitigate Harms from Digital Food Marketing to Children Ages 2-17,' *Durham, NC: Healthy Eating Research*, 2024 <https://healthyeatingresearch.org>; Radesky et al, 'Digital Advertising to Children'; VicHealth, 'Under the radar'; Assoc. Prof. Normann Witzleb and Prof. Moira Paterson, Faculty of Law, Monash University, Jordan Wilson-Otto, Gabby Tolkin-Rosen and Melanie Marks, elevenM Consulting , for OAIC, 'Privacy risks and harms for children and other vulnerable groups in the online environment,' 2020, https://www.oaic.gov.au/_data/assets/pdf_file/0012/11136/Report-Privacy-risks-and-harms-for-children-and-other-vulnerable-groups-online.pdf

²⁰ The Australian, 'Facebook targets "insecure" young people,' 1 May 2017, <https://www.theaustralian.com.au/business/media/digital/facebook-targets-insecure-young-people-to-sell-ads/news-story/a89949ad016eee7d7a61c3c30c909fa6> ; Business and Human Rights Centre, 'Meta allegedly targeted ads at teens based on their emotional state,' 9 April 2025, <https://www.business-humanrights.org/en/latest-news/meta-allegedly-targeted-ads-at-teens-based-on-their-emotional-state/>; Frances Haugen, Statement to Subcommittee on Consumer Protection, Product Safety, and Data Security, 2021, <https://www.commerce.senate.gov/wp-content/uploads/media/doc/Frances%20Haugen%20Written%20Testimony.pdf>; Reset Australia, 'Profiling children for advertising: Facebook's monetisation of young people's personal data,' 2021, https://au.reset.tech/uploads/resettechaustralia_profiling-children-for-advertising-1.pdf

²¹ Reset Australia, 'Profiling children for advertising'; VicHealth, 'Under the radar'

²² Australian Prevention Partnership Centre, '#DigitalYouth pilot study'

²³ 5Rights Foundation, 'Pathways: How digital design puts children at risk,' 2021, <https://5rightsfoundation.com/resource/pathways-how-digital-design-puts-children-at-risk/> Also: Center for Countering Digital Hate, 'Deadly by design: TikTok pushes harmful content promoting eating disorders and self-harm into users' feeds,' 2022, <https://counterhate.com/research/deadly-by-design/>; Centre for Countering Digital Hate, 'YouTube's UK Anorexia Algorithm,' 2024, <https://counterhate.com/research/youtube-anorexia-algorithm-uk/>

²⁴ 5Rights Foundation, 'Pathways: How digital design puts children at risk'

²⁵ Children and Screens: Institute of Digital Media and Child Development, 'A call for platform transparency: putting parents back in charge of firearm safety,' 2025, <https://www.sandyhookpromise.org/news/press-releases/social-media-loopholes-are-exposing-minors-to-dangerous-gun-marketing/>

²⁶ Amnesty International, 'Driven into the darkness: how TikTok encourages self-harm and suicidal ideation,' 2023, <https://5rightsfoundation.com/resource/driven-into-the-darkness-by-amnesty-international/> . Also 5Rights Foundation, 'Disrupted childhood: the cost of persuasive design,' 2024, <https://5rightsfoundation.com/resource/updated-report-disrupted-childhood-the-cost-of-persuasive-design/>

²⁷ 5Rights Foundation, 'Pathways: How digital design puts children at risk'; 5Rights Foundation, 'Disrupted childhood: the cost of persuasive design'; 60 Minutes, 'Facebook whistleblower reveals social media companies' tactics to lure children,' 2026, <https://www.youtube.com/watch?v=rVmtKTth2ek> ; ABC, 'Meta ordered to pay \$538m in US trial over child exploitation, user safety claims,' 25 March 2026, <https://www.abc.net.au/news/2026-03-25/meta-ordered-to-pay-375m-in-us-trial-child-exploitation-claims/106495616> ; Consumer Policy Research Centre (CPRC), 'Playing the player: unfair digital gaming practices and their impact on Australians,' 2025, <https://cprc.org.au/report/playing-the-player/>; Federal Trade Commission, 'FTC Staff Report Finds Large Social

Media and Video Streaming Companies Have Engaged in Vast Surveillance of Users with Lax Privacy Controls and Inadequate Safeguards for Kids and Teens,' 2024, <https://www.ftc.gov/news-events/news/press-releases/2024/09/ftc-staff-report-finds-large-social-media-video-streaming-companies-have-engaged-vast-surveillance> ; NPR, 'Jury finds Meta and Google negligent in social media harms trial,' 25 March 2026, <https://www.npr.org/2026/03/25/nx-s1-5746125/meta-youtube-social-media-trial-verdict>

²⁸ United Nations (UN) Convention on the Rights of the Child, 'General Comment 25: on children's rights in relation to the digital environment,' 2021 <https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-25-2021-childrens-rights-relation> ; UN Convention on the Rights of the Child, 'General Comment No 16 (2013) on State obligations regarding the impact of the business sector on children's rights,' 2013, https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/Download.aspx?symbolno=CRC%2FC%2FGC%2F16&Lang=en

²⁹ UK ICO, 'Children's code evaluation,' 2023, <https://ico.org.uk/media2/migrated/4025494/childrens-code-evaluation-report.pdf>

³⁰ FTC Bureau of Consumer Protection, 'Bringing dark patterns to light,' 2022, https://www.ftc.gov/system/files/ftc_gov/pdf/P214800%20Dark%20Patterns%20Report%209.14.2022%20-%20FINAL.pdf

³¹ Chandni Gupta, Winston Churchill Memorial Trust, 'Made to manipulate: the impact of deceptive online design practices on wellbeing and strategies to mitigate harm,' 2023, <https://www.churchilltrust.com.au/fellow/chandni-gupta-vic-2023/>; Marie Potel-Saville and Mathilde Da Rocha, 'From Dark Patterns to Fair Patterns? Usable Taxonomy to Contribute Solving the Issue with Countermeasures,' *Annual Privacy Forum*, 2023, https://www.researchgate.net/publication/371314839_From_Dark_Patterns_to_Fair_Patterns_Usable_Taxonomy_to_Contribute_Solving_the_Issue_with_Countermeasures

³² CPRC, 'Playing the player; European Data Protection Board, 'Guidelines 03/2022 on deceptive design patterns in social media platform interfaces: how to recognise and avoid them,' 2023, https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-032022-deceptive-design-patterns-social-media_en; Gupta, 'Made to manipulate'; Office of the Privacy Commissioner of Canada Sweep Report 2024: Deceptive Design Patterns, 2024, https://www.priv.gc.ca/en/about-the-opc/what-we-do/international-collaboration/international-privacy-networks/international-privacy-sweep/2024_sweep/opc-sweep-report-2024/ ; UK ICO, 'Age appropriate design: a code of practice for online services,' <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/age-appropriate-design-a-code-of-practice-for-online-services/13-nudge-techniques/>

³³ Office of the Privacy Commissioner of Canada Sweep Report 2024: Deceptive Design Patterns, 2024, https://www.priv.gc.ca/en/about-the-opc/what-we-do/international-collaboration/international-privacy-networks/international-privacy-sweep/2024_sweep/opc-sweep-report-2024/

³⁴ CPRC, 'Playing the player'

³⁵ CPRC, 'The cost of managing your privacy,' 2024, https://cprc.org.au/wp-content/uploads/2024/07/CPRC_Cost-of-Privacy-Report_Final.pdf

³⁶ Karishma Brahmabhatt and Steve Wood, 'Are you afraid of the dark? Protecting children from the harm of dark patterns,' *Data & Privacy Protection*, vol 24, issue 5, 2024, <https://edge.sitecorecloud.io/allenoverlylp1-aoshearmanwe0db-production-ecf3/media/project/aoshearman/pdf-downloads/are-you-afraid-of-the-dark-protecting-children-from-the-harms-of-dark-patters.pdf>

³⁷ Office of the Privacy Commissioner of Canada Sweep Report 2024: Deceptive Design Patterns

³⁸ CPRC, 'The cost of managing your privacy'. See also: CPRC, 'Consumer understanding - and misunderstanding - of data broking, data privacy, and what it means for them'; OAIC, 'Australian Community Attitudes to Privacy Survey,' 2023, https://www.oaic.gov.au/_data/assets/pdf_file/0025/74482/OAIC-Australian-Community-Attitudes-to-Privacy-Survey-2023.pdf ; Reset Australia, 'Did we really consent to this? Terms & Conditions and young people's data,' 2021, <https://au.reset.tech/news/did-we-really-consent-to-this-terms-and-conditions-young-people-s-data/>

³⁹ Lewers Research for Alannah & Madeline Foundation, 'Upholding children's right to privacy online: quantitative report,' 2025

⁴⁰ Justine Humphry, Olga Boichak, Jonathon Hutchinson, 'Emerging Online Safety Issues: Co-creating social media with young people - Research Report,' 2023, <https://ses.library.usyd.edu.au/handle/2123/31689>; OAIC, 'Australian

Community Attitudes to Privacy Survey'; Reset Australia, ' "Keep it to a limit": The rules young people want protecting their data,' 2021, https://au.reset.tech/uploads/resettechaustralia_policymemo_pollingreport_final-oct.pdf

⁴¹ Alannah & Madeline Foundation, Cardinia Shire Year 6 Leadership Day report 2025; Alannah & Madeline Foundation, 'Children's voices and the digital duty of care'; eSmart, 'Safe Kids are eSmart Kids: Lower primary school co-design results - external report'; Lewers Research for Alannah & Madeline Foundation, 'Upholding children's right to privacy online - qualitative report'

⁴² eSafety, 'Mind the gap: parental awareness of children's exposure to risks online,' 2022, <https://www.esafety.gov.au/research/mind-the-gap>

⁴³ eSafety, 'The online experiences of children in Australia,' 2025, <https://www.esafety.gov.au/research/the-online-experiences-of-children-in-australia>

⁴⁴ eSafety, 'Levelling up to stay safe: young people's experiences navigating the joys and risks of online gaming,' 2024, <https://www.esafety.gov.au/sites/default/files/2024-02/Leveling%20up%20to%20stay%20safe%20-%20gaming%20report.pdf?v=1776901420868>

⁴⁵ Common Sense Media, 'How girls really feel about social media,' 2024, <https://www.common sense media.org/research/teens-and-mental-health-how-girls-really-feel-about-social-media>

⁴⁶ Australian Child Maltreatment Study, 'Children's online sexual victimization in Australia,' 2025, <https://www.acms.au/resources/childrens-online-sexual-victimization-in-australia%2F>

⁴⁷ eSafety, 'Children and technology-facilitated abuse in domestic and family violence situations, 2020, <https://www.esafety.gov.au/sites/default/files/2020-12/Children%20and%20technology-facilitated%20abuse%20-%20Summary%20report.pdf?v=1739442988743>

⁴⁸ Lewers Research for Alannah & Madeline Foundation, 'Upholding children's right to privacy online: final report'

⁴⁹ Lewers Research for Alannah & Madeline Foundation, 'The Draft Children's Online Privacy Code: Consultation with Parents and Carers of Primary Aged Children - qualitative research report,' prepared by Lisa Lewers, Moira Callard and Lauren Campbell, May 2026

⁵⁰ Lewers Research for Alannah & Madeline Foundation, 'Upholding children's right to privacy online: quantitative report'

⁵¹ Lewers Research for Alannah & Madeline Foundation, 'The Draft Children's Online Privacy Code: Consultation with Parents and Carers of Primary Aged Children - qualitative research report,' prepared by Lisa Lewers, Moira Callard and Lauren Campbell, May 2026

⁵² Lewers Research for Alannah & Madeline Foundation, 'The Draft Children's Online Privacy Code: Consultation with Parents and Carers of Primary Aged Children - qualitative research report,' prepared by Lisa Lewers, Moira Callard and Lauren Campbell, May 2026

⁵³ Lewers Research for Alannah & Madeline Foundation, 'The Draft Children's Online Privacy Code: Consultation with Parents and Carers of Primary Aged Children - qualitative research report,' prepared by Lisa Lewers, Moira Callard and Lauren Campbell, May 2026

⁵⁴ Alannah & Madeline Foundation, 'Youth Engagement Program workshop on the Children's Online Privacy Code', 2026

⁵⁵ U.N. Convention on the Rights of the Child, 1989, <https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-rights-child>

⁵⁶ U.N. Convention on the Rights of the Child

⁵⁷ U.N. Convention on the Rights of the Child, 'General comment No. 25'

⁵⁸ U.N. Convention on the Rights of the Child, 'General comment No. 25'

⁵⁹ Australian Government, Office of the Australian Information Commissioner, 'Exposure draft explanatory statement: Privacy (Children's Online Privacy) Code 2026,' 2026

https://www.oaic.gov.au/_data/assets/pdf_file/0019/262630/Draft-Explanatory-Statement-Exposure-Draft-Childrens-Online-Privacy-Code.pdf

⁶⁰ Adrienne Katz & Dr Aiman El Asam, with Internet Matters, 'Refuge and Risk: life online for vulnerable young people,' 2021, <https://www.thecybersurvey.co.uk/>. See also: Children's Commissioner (England), ' "I've seen horrible things": children's experiences of the online world,' Oct 2024,

<https://www.childrenscommissioner.gov.uk/resource/ive-seen-horrible-things-childrens-experiences-of-the-online-world/>; Lisa De Bortoli, Catherine Underwood, Tim Friedman, Eveline Gebhardt, 'PISA 2022: Reporting

Australia's Results,' vol.2, <https://www.acer.org/au/pisa/>; eSafety, 'A new playground: the digital lives of young people

with disability,' 2023, <https://www.esafety.gov.au/sites/default/files/2023-11/A-new-playground-report.pdf?v=1754282019692>; eSafety, 'Cool, beautiful, strange and scary: The online experiences of Aboriginal and Torres Strait Islander child and their parents and caregivers,' 2023, <https://www.esafety.gov.au/research/online-experiences-aboriginal-torres-strait-islander-children-parents-caregivers>; Sameer Hinduja, 'The Role of Parents in Preventing Bullying and Cyberbullying,' 2022, <https://cyberbullying.org/parenting-preventing-bullying-cyberbullying>; Internet Matters, 'The new face of digital abuse: children's experiences of nude deepfakes,' 2024, <https://www.internetmatters.org/hub/research/children-experiences-nude-deepfakes-research/>; Internet Matters, 'Me, myself and AI: understanding and safeguarding children's use of AI chatbots,' 2025, <https://www.internetmatters.org/hub/research/me-myself-and-ai-chatbot-research/>; Justin W Patchin, 'Vicarious Supervision: Preventing Problematic Behaviors Online through Positive Parent-Child Relationships,' Cyberbullying Research Centre, 2022, <https://cyberbullying.org/vicarious-supervision-preventing-cyberbullying>; Pilar Rioseco, Suzanne Vassallo, 'Growing Up in Australia Snapshot Series – Issue 5,' 2021, <https://aifs.gov.au/growing-australia/research/research-snapshots/adolescents-online>; Heather Wolbers, Timothy Cubitt, Sarah Napier, Michael Cahill, Mariesa Nicholas, Melanie Burton, Katherine Giunta, 'Sexual extortion of Australian adolescents: Results from a national survey,' 2025, <https://www.aic.gov.au/publications/tandi/tandi712>; Youth Endowment Fund, 'Children, violence and vulnerability 2020', <https://youthendowmentfund.org.uk/reports/children-violence-and-vulnerability-2024/social-media/>

⁶¹ Apple, 'Apple reports fourth quarter results,' 30 Oct 2025, <https://www.apple.com/newsroom/2025/10/apple-reports-fourth-quarter-results/>; Forbes, 'Alphabet Beats Earnings Expectations As Annual Revenue Tops \$400 Billion For First Time,' 4 Feb 2026, <https://www.forbes.com/sites/tylerroush/2026/02/04/alphabet-beats-earnings-expectations-as-annual-revenue-tops-400-billion-for-first-time/>; Meta, 'Meta Reports Fourth Quarter and Full Year 2025 Results,' <https://investor.atmeta.com/investor-news/press-release-details/2026/Meta-Reports-Fourth-Quarter-and-Full-Year-2025-Results/default.aspx>; Microsoft, 'Annual Report 2025,' <https://www.microsoft.com/investor/reports/ar25/index.html>; OAIC, 'Annual report 2024-25,' vol. 1, 2025, <https://www.oaic.gov.au/about-the-OAIC/our-corporate-information/oaic-annual-reports/annual-report-2024-25>; Roblox, 'Q4 2025 Report: Shareholder letter,' <https://ir.roblox.com/financials/quarterly-results/default.aspx>

⁶² UK ICO, 'Children's code strategy: interim impact review,' 2025, <https://ico.org.uk/media2/i2zmh3h5/childrens-code-strategy-interim-impact-review-november-2025.pdf>

⁶³ UK ICO, 'Children's code strategy: interim impact review'; UK ICO, 'Protecting children's privacy online: Our Children's code strategy,' <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/protecting-childrens-privacy-online-our-childrens-code-strategy/>

⁶⁴ 5Rights Foundation, 'The Age Appropriate Design Code can protect children from AI harms – if properly enforced,' Jan 2026, <https://5rightsfoundation.com/the-age-appropriate-design-code-can-protect-children-from-ai-harms-if-properly-enforced/>; 5Rights Foundation, 'UK's Age Appropriate Design Code: 4 years of global impact,' Sep 2025 <https://5rightsfoundation.com/uks-age-appropriate-design-code-four-years-of-global-impact-before-key-review/>; 5Rights Foundation, 'UK Information Commissioner issues first financial penalty under the Children's Code,' Feb 2026, <https://5rightsfoundation.com/uk-information-commissioner-issues-first-financial-penalty-under-the-childrens-code/>; UK ICO, 'Children's code strategy: interim impact review'

⁶⁵ Australian Government, 'Privacy Act Review: Report 2022,' p.23

⁶⁶ Australian Government, 'Privacy Act Review: Report 2022,' pp.5, 23-30

⁶⁷ UK ICO, 'Children's code evaluation', 2023, <https://ico.org.uk/media2/migrated/4025494/childrens-code-evaluation-report.pdf>

⁶⁸ Lewers Research for Alannah & Madeline Foundation, 'The Draft Children's Online Privacy Code: Consultation with Parents and Carers of Primary Aged Children - qualitative research report,' prepared by Lisa Lewers, Moira Callard and Lauren Campbell, May 2026

⁶⁹ Lewers Research for Alannah & Madeline Foundation, 'Upholding children's right to privacy online: quantitative report'

⁷⁰ Lewers Research for Alannah & Madeline Foundation, 'The Draft Children's Online Privacy Code: Consultation with Parents and Carers of Primary Aged Children - qualitative research report,' prepared by Lisa Lewers, Moira Callard and Lauren Campbell, May 2026