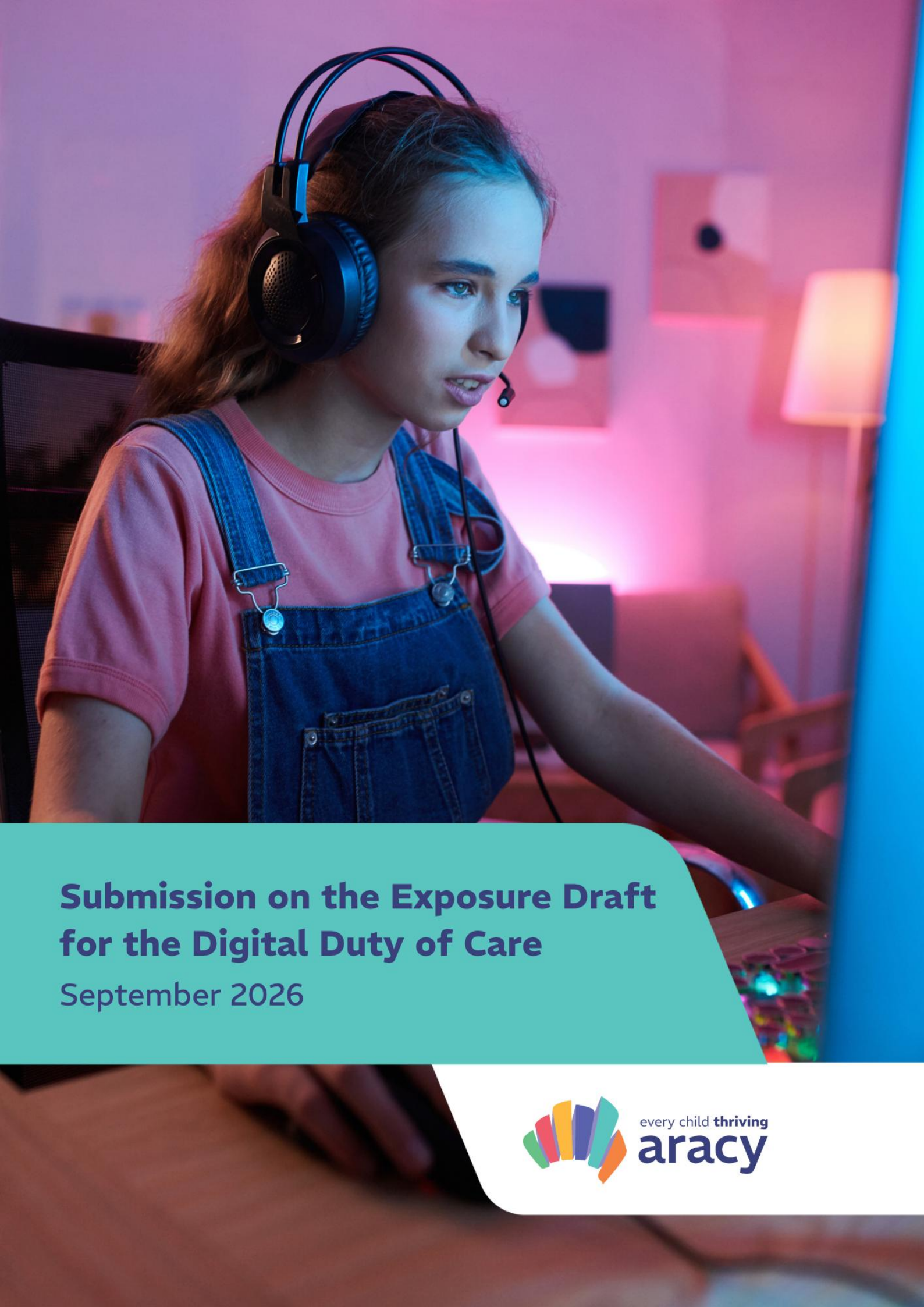




Submission on the Exposure Draft for the Digital Duty of Care

September 2026



22 September 2026

Online Safety Branch, Department of Infrastructure,
Transport, Regional Development, Communications, Sport and the Arts

Submission: exposure draft Online Safety Amendment (Digital Duty of Care) Bill 2026

ARACY – the Australian Research Alliance for Children and Youth welcomes the exposure draft. Every child and young person in Australia should be able to learn, connect and belong online. The spaces we build around our children shape how they grow. We strongly support a duty of care model. A toy maker cannot sell a product that harms a child. A food producer cannot sell one that makes a child sick. Online services should be held to the same standard.

ARACY is a national not-for-profit working to improve the wellbeing of children and young people aged 0 to 25. We define holistic wellbeing through The Nest, Australia's most widely-used, evidence-based, wellbeing framework for children and young people. The Nest defines wellbeing across six interconnected domains: Valued, Loved and Safe; Material Basics; Healthy; Learning; Participating; and Positive Sense of Identity and Culture.

This submission draws on Australian and international evidence and amplifies the voices of children and young people who stand to benefit from a legislated Digital Duty of Care.

Funded by the Australian Government Department of Health, Disability and Ageing through the Health Peak and Advisory Bodies Program, ARACY's Young and Wise lived-experience research in 2026 consulted 53 young people across five priority communities: young people living in rural, regional and remote areas; young people who self-identified as LGBTIQ+, culturally and linguistically diverse, or neurodivergent; and Aboriginal and Torres Strait Islander young people. In addition, we ran a workshop with nine young people aged 13 to 18 on the Children's Online Privacy Code exposure draft.

Note on evidence: each recommendation below identifies the evidence that supports it. Lived-experience quotes that accompany each recommendation are illustrative. They confirm and humanise what the evidence shows. They are not the primary basis for regulatory change.

Summary of Recommendations

Recommendation 1: Children's Best Interests, Rights and Participation

1.1 Require decision-makers to seek and have regard to the views of children and young people.

Recommendation 2: Transparent and Testable Risk Management

2.1 Make risk assessments public, and make child impact a named component.

Recommendation 3: Future-Proofing for AI, Design Features and Emerging Risks

3.1 Keep the duty relevant to generative AI and services that do not exist yet.

3.2 Do not let design feature protections stop at 16 years.

Recommendation 4: Accessible, Effective and Trusted Safeguards

4.1 Make complaints age-appropriate, accessible and trusted.

4.2 Make plain language a standard, for the Commissioner and for services.

4.3 Do not repeal the industry codes until replacements are in force.

Recommendation 5: Implementation that Supports Children, Young People and Families

5.1 State how the duty and the Children's Online Privacy Code interact.

5.2 Review the effectiveness and impacts of the framework.

5.3 Fund parent and caregiver education so children do not carry it.



Framing: protect what works, not only what harms

A safe online environment should be more than one where nothing goes wrong. The draft defines a safe online environment almost entirely as the absence of harm. Young people consistently told us that digital spaces also deliver connection, identity, culture, learning, mental health support and civic participation. Under The Nest, this covers all six wellbeing domains required for children and young people to thrive.

A duty built only to stamp out harm will measure its own success incorrectly. We recommend the objects and explanatory materials recognise that children and young people have positive digital lives worth protecting and growing, consistent with General Comment 25 to the Convention on the Rights of the Child - which Australia has ratified. It treats the digital environment as carrying both benefits and risks for children, and it requires that children be consulted on laws that affect them. The digital duty of care should also support children's ability to access the trusted information, learning opportunities, communities of belonging and sources of support that contribute positively to their wellbeing. This includes ensuring children and young people can continue to reach information and resources of public and community value, including trusted health and mental health information and support services.

We also ask that the Bill be read across the whole life course. Children's digital lives now begin in the early years, before they have accounts of their own, through family sharing, connected toys, wearable technologies and educational technology. Protections pitched only at adolescents will miss younger children. The same design choices shape them, and they gain just as much when those choices are made well.

"...I couldn't talk to anybody in my real life about being queer. So of course I went to online spaces. And the same is also true for my friends who are part of like racial minorities...like finding community online is, it was like essential to me figuring out who I was." — **De-identified, LGBTIQ+ roundtable, Over 18**

Recommendations

Recommendation 1: Children's best interests, rights and participation

Embed children's best interests, rights and participation in the design, implementation and review of the Digital Duty of Care.

1.1 Require decision-makers to seek and have regard to the views of children and young people

We recommend the Bill require persons responsible for online services, the Commissioner and the Minister to treat the best interests of children as a primary consideration when exercising functions under the Digital Duty of Care. This should include consideration of children's rights to protection, privacy, development, participation, access to information, expression, identity, culture and connection.

The draft requires the Minister to seek the Commissioner's advice before making key instruments. The process should also require consultation with children or young people. The guidelines under section 166B(1)(r), which govern protecting children from harmful design features, are not legislative instruments and are therefore not subject to parliamentary scrutiny. Nor does the Bill require consultation on their development.

Australia already has capable mechanisms, for example, eSafety Youth Council, Office for Youth, Australian Youth Affairs Coalition and other youth-centred organisations. The gap is not capacity; the gap is obligation.

We recommend the Bill require the Commissioner to seek and have regard to the views of children and young people before:

- formulating or amending guidelines under section 166B(1)(r)
- determining risk assessment requirements under section 26A(4)
- determining complaint and dispute process requirements under section 26F(3)
- making data access rules under section 205C
- giving advice to the Minister under section 27A, including on emerging categories of harm and services of concern
- advising the Minister under section 27B on the harm lists and the design feature list.

Children and young people should also participate in monitoring and reviewing the operation of the duty, including whether safeguards are effective, accessible and producing unintended consequences. Consultation should use developmentally appropriate methods and include younger children, who are often less likely to be heard in policy processes.

Consultation with children and young people should apply recognised co-design principles: young people involved from problem definition, not only validation; paid for their time; supported to participate across age, ability, language, culture and location; and told what changed because of them. The Commissioner should publish a short statement with each instrument setting out what young people said, what was adopted and what was not, and why.

Timing also matters. Schedules 2 and 3 commence 12 months after Royal Assent, and the Commissioner must build the guidelines, risk assessment requirements, complaint standards and data access rules inside that window. We ask the Department and the Commissioner to commit publicly to consulting children and young people across that period, sequenced to each instrument.

"...limiting the accesses to community that we have under the guidance of safety is really harmful and ridiculous because if they wanted to make it [social media] safe, they would actually consult us as opposed to making the decision and praying that it somehow gets better..." — Aspen, LGBTIQA+ roundtable, Under 18

Recommendation 2: Transparent and testable risk management

Require child-specific, transparent and testable risk management, including assessment of unequal and unintended impacts.

2.1 Make risk assessments public, and make child impact a named component

Section 26A requires a written risk assessment. However, there is no obligation to publish risk assessments undertaken, or how the organisation intends to address the risks identified. Further, there is no requirement to assess risk to children specifically and separately, or to assess how risk falls differently on different groups of children. The Commissioner may later require publication, but this is discretionary and deferred.

Our recent lived-experience evidence is that harm lands unevenly. This is consistent with national evidence from the eSafety Commissioner, which shows that some groups of children experience online hate at substantially higher rates. Among children aged 13 to 15, 41 per cent of sexually diverse children reported hate targeting their sexuality, 27 per cent of Aboriginal and Torres Strait Islander children reported hate targeting their identity, and 19 per cent of children with disability reported hate targeting their disability¹.

Young people described very different experiences, depending on where they live and who they are. Rural and regional young people, LGBTIQA+ young people, culturally and linguistically diverse young people, First Nations young people and neurodivergent young people each described distinct exposure and distinct reliance on online spaces. Young people also described experiences of racism, discrimination and identity-based hostility online. Therefore, assessments of risk and child rights impacts should explicitly consider how foreseeable harms may affect different groups of children and young people.

"My only friends were online, and I got completely cut off from them, at probably one of the worst times I could have been... And everyone else is just not being kicked off or affected. They've all got different communities, and they don't understand it because they're not in a rural community." — Ava, rural, regional and remote roundtable, Under 18

¹ eSafety Commissioner (2025). 'Digital use and risk: Online platform engagement among children aged 10 to 15'. Canberra: Australian Government.



As drafted, the Bill would make platforms responsible for a safe online environment but does not prescribe a child-specific assessment of how risks and proposed responses may affect children and young people.

Child impact assessments should consider the effects of both service design and proposed safety measures. This should include whether a measure may unnecessarily restrict children's access to connection, education, health information, cultural participation, peer support, creative expression or civic participation. Services should use the least restrictive effective response.

The Bill also does not require publication of how risks are identified, assessed or addressed. Meaningful transparency requires visibility of how risks are identified, assessed and addressed. An unpublished assessment cannot be tested by researchers, parents, teachers or young people.

Risk assessments should not be treated as a documentation exercise. Services should be required to identify the outcomes their safeguards are intended to achieve, test whether those safeguards are effective, identify unintended consequences and take further action where controls are not working. The Commissioner should be able to require independent assurance for high-risk services, systems and design features.

Transparency should work at two levels. Accredited researchers and public-interest organisations need detailed access to test what platforms claim. We welcome the Bill's framework for independent researcher access to platform data (section 205B) and the protections that let approved researchers and the Commissioner investigate services without revealing their identity (sections 205G to 205L). Researchers and civil society organisations play an important public-interest role in testing platform safety claims, building the evidence base for future reform, and translating complex evidence into information communities can use. Children, young people, parents and educators need something different again, for example, plain language, age-appropriate summaries of how a service is finding, assessing and reducing risk. Publishing in both forms is how everyone can learn what protections and tools they now have.

Recommendation 3: Future-proofing for AI, design features and emerging risks

Ensure the duty covers emerging technologies and the cumulative effects of commercial design systems.

3.1 Keep the duty relevant to generative AI and services that do not exist yet

We support the inclusion of services that let users generate material using artificial intelligence (AI) and share it. However, some of the AI services young people use most, including chatbots and companion applications, may not involve sharing material at all, and so risk falling outside the definition. Young people told us they increasingly turn to these tools for emotional and health support. The duty should reach conversational and generative AI services whether or not their output is shared.

"Recently, I've heard/seen many young people turning to AI and social media for emotional and health support, rather than going to a GP or accessing services such as KidsHelpline."

— Fatima, culturally and linguistically diverse roundtable, Under 18

"Yes its [AI chat companions] dangerous because they have your information and aren't really qualified to help make a huge impact or anything"

— Hania, culturally and linguistically diverse roundtable, Under 18, Meeting chat

For conversational and companion AI, risk assessments should consider generated information being presented as authoritative, repeated personalised interactions that may reinforce harmful patterns, the collection or inference of sensitive information, and failures to respond appropriately when a young user appears to need human support.

We recommend:

- the definition of online service capture conversational, companion and generative AI services, regardless of whether their output is shared.

3.2 Do not let design feature protections stop at 16 years

Section 25B(1)(c) switches off design features with negative behavioural impacts only for social media users under 16. Recommender feeds, endless scroll, feedback counts and disappearing content continue in full for everyone from their sixteenth birthday.

"The social media ban is not addressing addiction and those issues for older teenagers...we are just attempting to delay the issues to 16 not 13, rather than fixing them." — GZ, rural, regional and remote roundtable, Over 18

We recommend user empowerment tools under section 26(4) be required for all users, not only those aged less than 16 years. This is particularly important for older adolescents and young adults. Evidence indicates that capacities associated with impulse control, planning and risk evaluation continue to develop through adolescence and into early adulthood.² Exposure to recommender systems, algorithmic amplification and endless feeds does not stop at a young person's sixteenth birthday, even though child specific protections do.

User empowerment tools should also cover advertising, not only posts, since recommender features select both. The design feature list also omits the systems that decide what children see: content moderation, advertising approval and delivery. We support calls for a statutory review of that list, and for the safe online environment definition to address compulsion and overuse. We also ask that the explanatory materials set out the evidence basis for 16 years as the threshold.

Risk assessments should consider how data collection, profiling, recommendation, advertising, notifications, social feedback and purchasing features operate together. Services should assess their cumulative and foreseeable impacts on children and young people, rather than considering each feature in isolation.

² Tashjian, S.M. (2024), *Teen brains are wired to take risks, but that can be a good thing*, Pursuit, University of Melbourne, 19 September 2024, available at: <https://pursuit.unimelb.edu.au/articles/Teen-brains-are-wired-to-take-risks-but-that-can-be-a-good-thing>

Recommendation 4: Accessible, effective and trusted safeguards

Require accessible complaints, independent redress, plain-language information and continuity of existing protections.

4.1 Make complaints age-appropriate, accessible and trusted

Section 26F requires complaint and dispute processes "available equally to all Australians". Equal access is not the same as equitable access. A process designed for adults, offered 'equally' to a 13-year-old, is not a functioning safeguard. Young people also told us that when reporting is not anonymous, the fear of being identified can stop them from seeking help or raising concerns. While the example below relates to school-based wellbeing support, it reflects a broader concern that also applies to online reporting and complaints mechanisms.

"...at schools, it's not done very anonymously... I've had friends who wanted to, but then chose not to because they're afraid of like the stigma that's around it."

— **Serena, culturally and linguistically diverse roundtable, Under 18**

A complaints mechanism cannot function as an effective safeguard if young people feel unsafe using it. Young people told us they may avoid reporting harm because they fear consequences for using a platform they were not permitted to access.

"If people are experiencing cyber bullying through social media or if they do encounter any issues online, then now they're no longer going to go ask for help because ... they're worried that it will be flipped on them and that they'll get in trouble and be punished as a result of it."

— **Serena, culturally and linguistically diverse roundtable, Under 18**

That low confidence is well founded. Reset.Tech Australia³ reported 395 posts promoting disordered eating, to Instagram, TikTok and X. The platforms only removed between 5 and 12 per cent of them. A complaints duty means little if reports go nowhere, which is why resolution times must be published.

The introduction of internal complaint and dispute resolution obligations is a welcome step. Where a complaint is not resolved within the prescribed period, users should have access to a free, accessible and independent escalation mechanism. Services should provide reasons for their decisions, preserve information needed for review and report systemic complaint trends to the Commissioner. The Commissioner should be empowered to investigate patterns of repeated or unresolved complaints.

³ Reset.Tech Australia (2023), *Not Just Algorithms: Recommendations for an Australian Digital Duty of Care*, Reset.Tech Australia, March 2023, available at: <https://au.reset.tech/uploads/Not-Just-Algorithms-web-230323-V1.0.pdf>

We recommend section 26F require complaint and dispute processes that are:

- age-appropriate, culturally safe, in plain language, and accessible to neurodivergent users, users with disability, and users whose first language is not English
- able to be used anonymously or pseudonymously, without a verified account
- subject to maximum response and resolution times set by the Commissioner, with median times published
- designed so that reporting harm does not expose a child to additional risk or deter them from seeking help because of concerns about account suspension, access restrictions or other consequences.

4.2 Make plain language a standard, for the Commissioner and for services

Transparency reports go to the Commissioner, but publication is discretionary. Again, there is no obligation requiring plain language or accessible formats, either in what the Commissioner publishes or in what services are required to publish under section 192M.

"Legal language only for legal - not HUMANS." — Online Privacy Code workshop participant, aged 13-18 years

"[on what would make privacy information usable] Make an easy read version for people with disabilities, neurodivergent people, or even everyday people who just want a quick way to read."

— Online Privacy Code workshop, Mentimeter response, participant aged 13-18 years

We recommend:

- a plain language and accessibility standard apply across the Commissioner's published outputs.
- We further recommend it apply to what services must publish. This mirrors ARACY's June 2026⁴ recommendations to the Office of the Australian Information Commissioner: layered, age-appropriate explanations, standardised formats and easy read summaries.

4.3 Do not repeal the industry codes until replacements are in force

Schedule 3 removes the online content scheme industry codes and standards. The duty and the Commissioner's guidelines are intended to replace them. For children and young people, this is a significant shift and an important opportunity to strengthen protections and accountability, building on lessons learned from previous approaches to online safety.⁵

⁴ ARACY (2026). *Submission on the Exposure Draft of the Children's Online Privacy Code*, Australian Research Alliance for Children and Youth (ARACY). <https://www.aracy.org.au/resources/submission-of-exposure-draft-of-the-childrens-online-privacy-code/>

⁵ Farthing, R. (2022), *How Outdated Approaches to Regulation Harm Children and Young People and Why Australia Urgently Needs to Pivot*, Reset Tech Australia and ChildFund Australia.

We recommend:

- Schedule 3 not commence until the replacement guidelines are in force
- The department publish a clear transition plan showing how child-specific protections under the current codes will operate under the new framework
- Any existing protection that is not clearly replicated or strengthened under the new framework should remain in force until an equivalent or stronger replacement commences.

Recommendation 5: Implementation that supports children, young people and families

Align safety and privacy requirements and support effective implementation, education and review.

5.1 State how the duty and the Children's Online Privacy Code interact

The definition of reasonably practicable at section 25H builds privacy in as a limit on safety action. Two regimes will soon govern the same services and the same children.

We recommend:

- the Bill and explanatory materials clearly state how the Digital Duty of Care and the Children's Online Privacy Code interact, so that a service cannot rely on one regime to avoid obligations under the other
- safety measures, including age assurance, should be necessary, proportionate, privacy-preserving and accessible
- services be required to assess risks of misclassification, exclusion and disproportionate impacts on children who lack identity documents or rely on anonymous or pseudonymous access
- compliance with the Digital Duty of Care should not justify the unnecessary collection, inference, use or retention of children's personal information.

5.2 Review the effectiveness and impacts of the framework

The statutory review should commence within three years of the duty taking effect. It should examine the framework's effectiveness, enforcement, unintended consequences and unequal impacts, including whether key definitions and design feature lists remain fit for purpose. The review should include on independent evidence, complaints data and direct consultation with children and young people. Its report and the Government's response should be published.

5.3 Fund parent and caregiver education so children do not carry it

The Bill places the duty on services and the powers with the Commissioner. Parents and caregivers do not appear. Parents want to help, and most are already concerned. In a recent national survey, more than one in two Australian parents (56%, n= 3,745) rated their child's social media use a moderate or large problem. This was their second highest concern, behind their child's anxiety.⁶

⁶ ARACY & Parenting Research Centre. (2026). When kids answer back: Parenting Today through young eyes. Melbourne.

Young people we consulted in 2026 ranked "rapidly changing technology, including AI and social media" last, by a wide margin, among 8 options of what they want parents to focus on. Parents and children are focused on different things. Closing that gap is a job for adults. Young people told us that support from parents and caregivers includes adults taking responsibility for educating themselves, rather than relying on children and young people to explain the challenges they face. The participant quoted below later reflected on relying on online spaces for information, community and support when those needs were not being met offline.

"...parents and caregivers being able to educate themselves about what they need to do in order to support their queer child and not leaving it on the shoulders of that child to be able to teach them about everything..."

— Beau, LGBTQIA+ roundtable, Under 18

We recommend that commencement be accompanied by public communication and funded education for parents and caregivers, including information about the new protections and how to support children and young people to use them.

Adults and children can learn this together, with adults properly supported to lead.

Regulation and education play complementary roles. The Digital Duty of Care can reduce foreseeable risks, while digital literacy and critical thinking help young people understand, assess and respond to the information, interactions and technologies they encounter online.

Young people told us their school education on digital safety was often absent, late or out of date. They also told us what good teaching looks like.

"...even if schools tried to make a resource for that [digital safety], it wasn't really applicable because social media changes so quickly and they were taught by like millennials who didn't understand the culture."

— Jay, neurodivergent roundtable, Over 18

One roundtable participant reflected on an elective class available at their school that was relevant and effective at teaching children the skills they needed to navigate the internet safely. However, only 10 students accessed the course.

We recommend:

- the Department work with the Department of Education and state and territory education authorities on sequenced, curriculum-embedded digital literacy and critical thinking
- the Commissioner's education function at section 166B(1)(f) be exercised in partnership with the education portfolio, and reported on.



Conclusion

This Bill can do something no previous online safety measure has done. It shifts the onus of responsibility towards the services that design and operate digital environments, creating an opportunity to better protect children and young people while supporting their participation, development and wellbeing.

To realise its full potential, implementation matters. Risk assessments should be meaningful and transparent, complaints systems must be usable and trusted, and the framework should continue to be informed by the perspectives and lived experiences of children and young people as it evolves over time.

As technologies, services and online behaviours continue to evolve, so too should the framework. Ongoing engagement with children, young people, parents, caregivers and communities will be important to ensure the Duty of Care remains effective, responsive and grounded in lived experience. Young people have told us that safety measures designed without them have not worked. They also want platforms held to account. Those priorities are complementary, and together they provide a strong foundation for the next phase of online safety reform.

ARACY would welcome the opportunity to discuss this submission, and to put young people in front of the Department for policymakers to hear directly from the children and young people who stand to gain most from the successful passage and implementation of this important legislation.

Australian Research Alliance for Children and Youth

Enquiries Contact: Adam Valvasori, Lead, Advocacy adam.valvasori@aracy.org.au

www.aracy.org.au