# Submission on the Exposure Draft of the Children's Online Privacy Code 2026

This is a submission made by academics from a number of faculties across the University of Sydney including the Faculty of Arts and Social Sciences; Architecture, Design and Planning; and Medicine and Health

The University of Sydney
30 May 2026

# Table of Contents

# About the authors

[redacted]

Submission to the Office of the Australian Information Commissioner on the Exposure Draft of the Privacy (Children's Online Privacy) Code 2026 (the Children's Online Privacy Code)

[redacted]

# List of Recommendations

**Recommendation: Prohibit the sale or commercial transfer of children's personal information.**

**Recommendation: Strengthen accessibility requirements for children with disabilities (see specific amendment recommendations on page 9).**

**Recommendation: Adopt a tripartite strategy to support the operation of consent that includes public education and awareness, scenario-based impact assessments, and independent research and evaluation.**

**Recommendation: Embed privacy by design as a core requirement for the strong and effective implementation of the Code.**

**Recommendation: Impose stronger regulatory safeguards for age assurance systems and processes, including heavy penalties for retaining children's personal information and data breaches.**

**Recommendation: Require companies to respond promptly and at the point of need to requests about how personal information is handled.**

**Recommendation: Ensure definitions are fit for purpose and flexible to address the wide range of service types, configurations and rapid technological innovation, and remove the exception for health services.**

**Recommendation: Undertake privacy impact assessments conducted by independent bodies incorporating evidence-based research.**

**Recommendation: Support a national research ecosystem to monitor the impacts of the Code.**

# Introduction

We support the introduction of the Privacy (Children's Online Privacy) Code 2026. It represents a meaningful step towards protecting children's privacy online, including the best interests test, privacy-by-default requirements, the consent framework, transparency requirements, and the right to destruction of personal information. The Code falls short in some areas in relation to the sale or commercial transfer of children's personal information, accessibility requirements for children with disabilities, operation of consent practices, privacy by design, just-in-time requirements for handling personal information, privacy safeguards for age assurance systems, and definitions that are flexible and fit for purpose. To address these issues and strengthen the Code, we have made several recommendations for consideration.

# The data market for children's personal information

**Recommendation: Prohibit the sale or commercial transfer of children's personal information**

Children's personal data has significant commercial value. It can be used to build detailed behavioural profiles – tracking interests, habits, location, social connections and emotional states – which are then monetised through targeted advertising or in-app purchases and sold to data brokers, used for added revenue, or shared with third-party platforms.[1] Children are particularly vulnerable in this context because they are less able to understand what they are agreeing to, less aware of the long-term consequences, and more susceptible to manipulative design.[2]

The current Code addresses this risk indirectly through consent requirements, privacy-by-default settings, and the best interests test, but none of these amount to a hard prohibition on data being sold or transferred for commercial gain. An entity could, in theory, obtain technically valid consent (e.g. parental consent for an under-15) to share a child's data with third parties for commercial purposes, and then argue that arrangement is not inconsistent with the child's best interests.

Data monetisation is deeply embedded in the business models of many online platforms,[3] and the concern is that without an explicit prohibition, the Code's principles-based approach may not be strong enough to override those incentives in practice.

Given the significant commercial incentives to monetise children's data and the difficulty of enforcing principles-based protections against determined actors, we recommend that the Code includes an explicit prohibition on the sale or disclosure of children's personal information for commercial purposes.

Such a prohibition would strengthen the Code's protections, reduce compliance uncertainty, and send a clear signal that children's rights are prioritised over commercial interests in Australia.

---

[1] Eline L. Leijten, Simone van der Hof, Dissecting the commercial profiling of children: A proposed taxonomy and assessment of the GDPR, UCPD, DSA and AI Act in light of the precautionary principle, Computer Law & Security Review, Volume 57, 2025 https://doi.org/10.1016/j.clsr.2025.106143.

[2] Gray, J.E., Carter, M., Egliston, B. (2024). Designing for Safety, Privacy and Inclusivity in Social VR. In: Governing Social Virtual Reality. Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-031-61831-4_5

[3] https://www.accc.gov.au/inquiries-and-consultations/finalised-inquiries/digital-platform-services-inquiry-2020-25/march-2021-interim-report

**An explicit prohibition is needed to disrupt the foundational data commercialisation mechanisms and ecosystems that currently drive the commercial exploitation of children's personal information online.**

We note that in the US the Federal Trade Commission (FTC) has treated the unauthorised sharing and monetisation of children's data with advertising networks and data brokers as an unfair or deceptive practice through its enforcement actions under the COPPA Rule.[4]

Recently, the FTC also strengthened its approach to the commercialisation of children's data through a 2025 update to the Children's Online Privacy Protection Rule (COPPA Rule). The updated Rule requires separate, active parental opt-in consent before operators may disclose children's data to third parties for targeted advertising and prohibits operators from conditioning children's access to services on providing that consent.

We submit that Australia should go further and adopt an explicit prohibition because consent-based frameworks – even well-designed ones – are susceptible to manipulation and erosion over time, particularly given the force of the commercial incentives at play.[5] Second, a clear prohibition is easier to enforce, easier for children and parents to understand, and sends an unambiguous signal that children's personal information is not a commercial commodity. The Australian Code, as currently drafted leaves room for commercial arrangements to be structured in ways that technically comply while still allowing for the sale of children's personal data to third parties. An explicit prohibition would close that gap.

# Accessibility for children with disabilities

**Recommendation: Strengthen accessibility requirements for children with disabilities (see specific amendment recommendations)**

The Code represents an opportunity to ensure stronger data privacy protections for all Australian children. However, as currently drafted, we are concerned the Code does not address the privacy rights and needs of children with disabilities, including children with print and cognitive disabilities.

Children with disabilities, including print disabilities affecting their ability to read standard print, are among the heaviest users of digital services and assistive technologies. They interact with online platforms through screen readers, braille displays, text-to-speech software, and other assistive tools. Their engagement with privacy-related information, consent mechanisms, and complaint processes is mediated entirely through these technologies. Yet the Code makes no reference to disability, accessible formats, or assistive technology anywhere in its provisions. As Goggin and Ellis[6] have argued, children with disabilities have been "an overlooked group in the debates on privacy and data management". Alper and Goggin[7] similarly demonstrate that digital rights frameworks routinely fail to account for the specific needs and experiences of children with disabilities.

This is a significant gap. The Code's transparency and consent requirements – which

[4] https://www.ftc.gov/news-events/news/press-releases/2025/01/ftc-finalizes-changes-childrens-privacy-rule-limiting-companies-ability-monetize-kids-data
[5] See e.g., Obar, J. A., & Oeldorf-Hirsch, A. (2018). The Clickwrap: A Political Economic Mechanism for Manufacturing Consent on Social Media. Social Media + Society, 4(3).
[6] Goggin, G., & Ellis, K. (2020). Privacy and Digital Data of Children with Disabilities: Scenes from Social Media Sharenting. *Media and Communication, 8*(4), 218–228. https://doi.org/10.17645/mac.v8i4.3350
[7] Alper, M., & Goggin, G. (2017). Digital technology and rights in the lives of children with disabilities. *New Media & Society*, 19(5), 726–740. https://doi.org/10.1177/1461444816686323.

depend on children being able to read, understand, and act on privacy-related information – are rendered ineffective for any child who cannot access that information in the format it is provided. A child-friendly privacy policy delivered as an untagged PDF, an image, or a video without captions may be perfectly "age appropriate" under the Code's definition while being entirely inaccessible to a child with a print disability. A consent mechanism that relies on drag-and-drop interaction, CAPTCHA, or poorly labelled form elements may technically comply with the Code's requirements while preventing a child using a screen reader from exercising their right to consent or withdraw consent.

The Code addresses this risk indirectly, if at all. Several provisions require information to be "clear, concise, transparent and easily accessible" (sections 23, 24 and 26), and some require it to be displayed in a "font size and type that is easy to read" (sections 11(6), 23(4), 26(3) and 29(4)). These formulations reflect a narrow, print-centric conception of readability. For a child using a screen reader, font size is irrelevant; what matters is semantic structure, proper heading hierarchy, meaningful link text, and compatibility with assistive technology. The Code's framing effectively equates "easy to read" with visual legibility, excluding children whose access depends on entirely different modalities.

Multiple provisions encourage entities to incorporate "non-text material" such as "diagrams, cartoons, graphics or video or audio content" to engage children effectively (sections 23(3)(c), 24(2)(d), 26(2)(d)). This is a welcome recognition that children engage with information in diverse ways. However, there is no requirement that such material include alt text, audio description, captions, or transcripts. Without these safeguards, entities could shift key privacy information into visual or multimedia formats that are inaccessible to children with print disabilities, while technically meeting the Code's requirements.

The Code's definition of "age appropriate" (section 4) is a developmental benchmark only. It does not encompass accessibility. A companion definition of "accessible" is needed, one that references the Web Content Accessibility Guidelines (WCAG) 2.2 at minimum AA conformance and requires that all information provided under the Code meet both the "age appropriate" and "accessible" standards.

This developmental framing also treats age as a proxy both for the information a child can engage with and for the capacity to give consent — a proxy that may work poorly for children with forms of cognitive disability. Section 4 sets the benchmark for "age appropriate" information at either the youngest child in the targeted age range or, by default, a 10–12 year-old. This treats chronological age as a stand-in for cognitive capacity — an assumption that does not hold for children with cognitive disability, who may need plain language, Easy Read, or other established accessibility formats regardless of age.

The same proxy problem runs through the Code's consent regime. For instance, section 13 sets 15 as the threshold for self-consent, and section 32(1)(c) acknowledges that a child of 15 or over may "lack capacity" to make a destruction request, but the Code provides no guidance on how capacity is to be assessed and no obligation on entities to support a child with cognitive disability to exercise their rights where they are able to do so. This is inconsistent with Article 12 of the Convention on the Rights of Persons with Disabilities, which establishes supported decision-making as a right, and with Article 7, which requires that disabled children's views be given due weight on an equal basis with other children. We recommend that the companion definition of "accessible" proposed above expressly includes cognitive accessibility.

Similar gaps exist across other parts of the Code. The requirements to ascertain age in section 8 do not acknowledge that common age assurance methods – facial estimation,

ID scanning, interactive challenges – may be inaccessible to children with print disabilities. The inquiry and complaint mechanisms required by Division 7 must be "clear, simple and easily accessible", but there is no requirement that they be operable by children using assistive technologies. The privacy impact assessment requirements in section 38 do not require entities to assess whether their privacy practices create accessibility barriers for children with disabilities. The privacy education and training requirements in section 40 do not include disability awareness or familiarity with assistive technologies.

Critically, the Code makes no reference to existing legal frameworks for disability rights. The *Disability Discrimination Act 1992*, the UN Convention on the Rights of Persons with Disabilities (particularly Articles 7, 9, and 21), and the UN Convention on the Rights of the Child (particularly Article 2 on non-discrimination, Article 16 on the right to privacy, and Article 23 on children with disabilities) all establish obligations that are directly relevant to how children's privacy protections are designed and delivered.

**Specific amendments recommended**

We recommend the following amendments to the Code:

- insert a definition of "accessible" in section 4 that references WCAG 2.2 at minimum AA conformance, and require that all information provided under the Code meet both the "age appropriate" and "accessible" standards

- amend sections 23(3)(c), 24(2)(d), and 26(2)(d) to require that any non-text material provided under the Code be accompanied by text alternatives, captions, audio description, or transcripts as appropriate, consistent with WCAG 2.2

- replace or supplement references to "font size and type that is easy to read" with a broader formulation requiring that information be presented in a manner that is perceivable and operable for children using assistive technologies

- add requirements that consent and withdrawal mechanisms, age verification processes, and inquiry and complaint mechanisms be designed to be accessible to children with disabilities, including those using assistive technologies

- amend section 38(2) to require that privacy impact assessments specifically assess the accessibility of privacy practices for children with disabilities

- amend section 40(2) to require that privacy education and training address the accessibility needs of children with disabilities and familiarity with assistive technologies

- include a purpose clause or interpretive provision that explicitly acknowledges the rights of children with disabilities under the UN Convention on the Rights of Persons with Disabilities, the *DDA 1992*, and the UN Convention on the Rights of the Child.

**Without explicit accessibility requirements, the Code risks building a children's privacy framework that systematically excludes the very children who are most reliant on digital services and most vulnerable to privacy harms online.** Accessibility is not an afterthought or an enhancement – it is a precondition for the Code's protections to be meaningful for all children.

# Consent practices in everyday life

**Recommendation: Adopt a tripartite strategy to support the operation of consent that includes public education and awareness, scenario-based impact assessments, and independent research and evaluation.**

Given the complexity of how consent systems and processes operate in practice, and the lack of clarity around how consent requirements are translated from the Code into implementation, we recommend a tripartite strategy to support effective and accountable operation.

This strategy should include:

(1) Public education and awareness measures prior to commencement of the Code.

The range of everyday user knowledge of consent varies drastically based on experience, exposure to digital spaces, backgrounds, and education levels. The reality is that users are consenting to things they do not fully understand because of long wordy documents, purposefully confusing processes and priority given to frictionless sign-up design principles (see further description below). For example, privacy policies often exceed thousands of words and are written in legalistic language that even highly educated users struggle to interpret. Similarly, consent interfaces frequently bundle multiple permissions together (e.g., agreeing to data sharing as a condition of accessing a service). As such, **we recommend the design and deployment of educational materials, written in plain language and released in accessible formats, to explain the core principles of consent as per the Code.** Education materials should be aimed at a variety of audiences with varying skill levels, including educational institutions, child protection services and institutions that supervise children in custody. Materials could include but is not limited to standardised consent formats, independent auditing of consent interfaces, and restrictions on manipulative or deceptive design practices.

(2) Scenario-based impact assessments to test how consent models function across different contexts and user groups.

In addition to the educational materials for users, **we recommend conducting assessment of a range of scenarios that children and young people are presented with that require consent.** Signing up to a digital platform as part of an educational experience is significantly different to accepting the conditions of an AI assistant, which is again different to signing up to a commercial gaming platform. For example, students may feel compelled to consent to participate in core learning activities, while some gaming platforms (those designed for mainstream blockbuster and mobile games, rather than independent games) and social media platforms, often rely on persuasive or time-pressured design features that encourage rapid acceptance without meaningful engagement (and indeed, some gaming platforms require consent across many separate games). Children in a variety of circumstances, such as those living independently or involved in the child protection or criminal justice system, face unique barriers in seeking and obtaining consent. We encourage the government to undertake scenario-based impact assessments as a condition of compliance with the Code, to test how consent mechanisms operate in practice across diverse real-world contexts for children and young people.

(3) Independent research and evaluation of the impacts and effectiveness of consent models and processes over time (see also Independent Privacy Impact Assessments and A national, multidisciplinary research ecosystem).

**Independent research and longitudinal evaluation need to be undertaken to assess the impacts and effectiveness of consent models and associated processes over time.** Such evaluation should be mandated to ensure that consent mechanisms remain robust, meaningful, and responsive to evolving digital environments. These assessments should incorporate rigorous empirical user testing, including validated measures of user comprehension, voluntariness and behavioural outcomes. Relevant indicators may include, but are not limited to, default acceptance rates, the extent to which children engage with consent materials, and the accessibility and practical ease of exercising withdrawal or opt-out options.

# Privacy by Design

**Recommendation: Embed privacy by design as a core requirement for the strong and effective implementation of the Code.**

The Code includes some indirect recognition of design practices and interface features: in section 14(3) in the use of manipulative, deceptive or misleading practices to obtain voluntary consent; section 21(1) on coercive consent practices; and in section 29(3) concerning ways that children are discouraged or impeded from opting out of direct marketing. However, privacy by design extends far beyond these aspects – its practice must be embedded in the entire user experience. **The Code must explicitly address these interface design dimensions, not just data flows, by embedding privacy by design as a core requirement of relevant entities bound by the Code.**

Design encompasses how consent is sought, how information is communicated, and how interface design enables children to meaningfully understand and engage with data practices. This means designing age-appropriate, accessible, and inclusive interactions, accounting not only for developmental stages but also for diversity and disability, that help children grasp what their data represents and what they are agreeing to when consenting. Crucially, well-designed systems should introduce constructive friction at key decision points (such as sign-up or data sharing prompts) to create opportunities for reflection and informed choice, rather than enabling passive or manipulated consent. Privacy risks are often embedded in specific design features and techniques, including persuasive or manipulative interface elements that shape user behaviour.

Further, privacy impact assessments should systematically evaluate interface features and user journeys, including timing of consent, privacy defaults and visibility of terms, and consent pathways. Examples include impact assessment of grace periods for service access when a system identifies the user is a child, staged decision-making when users prompt account deletion, and assessing the impact of how time-sensitive terms of service clauses are advertised (e.g. 30-day arbitration opt-out window).

Finally, given that organisations will operationalise these requirements in varied ways, there must be robust oversight and scrutiny of how privacy by design is implemented in practice, ensuring alignment with ethical approaches and safeguarding against superficial or compliance-driven interpretations of the Code. Best practices in consent are available across research and health domains which can be replicated.

# Age assurance technologies and privacy risk

**Recommendation: Impose stronger regulatory safeguards for age assurance systems and processes, including heavy penalties for retaining children's personal information and data breaches.**

The Code requires that relevant companies take reasonable steps to ascertain the age of the end-user (section 8(1)). While there is an exemption for entities that apply the protections in the Code to all end-users (section 8(5)), age assurance technologies will likely become the main means to determine whether a child is under 15 years for the purpose of identifying the appropriate method of consent. This introduces new and significant privacy and data security risks for children. These risks are not hypothetical.

There have already been several widely reported incidents involving the exposure and misuse of children's personal information collected through age verification systems. One notable example was the late-2025 data breach involving a third-party age-verification vendor used by Discord, which exposed the names, email addresses, support messages, IP addresses, and government identification photos of approximately 68,000 users globally, with Australian children disproportionately affected.[8] In this case, selfies and identification documents uploaded by children for verification purposes were reportedly retained to support appeals and dispute resolution processes, illustrating how data collected for ostensibly limited purposes can quickly be repurposed and stored for extended periods.

These examples demonstrate that age assurance systems can create new concentrations of highly sensitive personal information, including biometric data, facial images, government identification documents, behavioural metadata and device information. Such datasets are particularly attractive targets for cyberattacks and identity theft and have the potential to be used for commercial purposes. Even with a provision to ensure that personal information collected to verify age is destroyed as soon as practicable (section 8(4)), data retention is a major concern and probability.

The Australian Government's Age Assurance Trial Final report[9], which examined the feasibility of introducing age assurance measures, found that providers frequently over-retained user data to satisfy regulatory, audit, enforcement, and dispute resolution requirements. This highlights a broader structural issue within age assurance ecosystems: even systems promoted as "privacy-preserving" may still require the ongoing storage of sensitive information to support accountability and compliance processes. In practice, this can undermine claims of data minimisation and create pressures toward expanded collection and retention practices over time.

Importantly, the introduction of age assurance requirements may normalise the routine collection of identity and biometric data from children as a precondition for accessing online services. This risks shifting digital participation toward increasingly invasive forms of identification and surveillance, contrary to long-established privacy principles of proportionality and data minimisation. It also creates the possibility that children may be required to disclose more personal information in order to access low-risk or everyday digital services than would otherwise be necessary.

For these reasons, **the Code should have stronger safeguards around data minimisation, monitoring, independent auditing, transparency, and accountability of age assurance systems and processes.** In particular, the Code should prohibit the secondary use of age assurance or any other data collected for commercial purposes as per recommendation one. The regulator of the Code needs to be sufficiently authorised and resourced to enforce heavy penalties for non-compliance.

[8] https://ia.acs.org.au/article/2025/discord-breach-hits-68-000-australians.html
[9] https://www.infrastructure.gov.au/department/media/publications/age-assurance-technology-trial-final-report

# Just-in-time provision of personal information

**Recommendation: Require companies to respond promptly and at the point of need to requests about how personal information is handled.**

The Code introduces important transparency requirements in how companies deal with children's personal information (section 28), including a right for children to request information about the handling of their personal information. One concern is the operation of this feature, particularly in terms of timeliness of response. In the Code, companies are given up to 30 days to respond and in certain circumstances, up to 60 days. **Timeliness is not just a technical or administrative matter but fundamental to the effective operation of the service and its accessibility for children and young people.** Delays of up to 30, and in some cases, 60 days to receive an answer from a company substantially undermine the practical value of this right. For children, whose digital practices, social relationships and online environments can change rapidly, delayed access to information may mean that the information is no longer relevant, actionable, or meaningful by the time it is received. This is particularly significant where children are attempting to understand how their personal information is being used, contest harmful profiling or recommendations, address experiences of online harm, or make informed decisions about continuing to use a service.

Timeliness is also critical because children and adolescents are still developing the digital literacies and capacities required to navigate complex privacy and data systems. Long waiting periods create additional barriers to engagement, reduce trust in complaint and transparency mechanisms, and may discourage children from exercising their rights altogether. Delayed responses can also exacerbate harms where personal information is being actively used to shape content feeds, recommendations, advertising, or interactions in real time. In these contexts, access to information months after a request has little practical utility, particularly where the data practices in question may already have influenced a child's behaviour, wellbeing, or opportunities.

The Office of the Australian Information Commissioner (OAIC) recognises punctuality as a key component of meaningful transparency. In its guidance on age assurance technologies, the OAIC identifies as a core consideration the need to "Be transparent, at the moment it matters", recommending the use of APP 5 just-in-time notices to explain what information is collected, why it is collected, who it is shared with, how long it is retained, and the choices available to individuals, including review processes. This emphasis on contextual and timely disclosure reflects the reality that transparency is only effective when information is provided at a point where users, including children, are able to understand and act upon it.

**Accordingly, the just-in-time provision of personal information held about a child should be treated as a standard expectation and explicitly incorporated into the Code.**

# Definition matters

**Recommendation: Ensure definitions are fit for purpose and flexible to address the wide range of service types, configurations and rapid technological innovation, and remove the exception for health services.**

The definitions of entities captured under the Code (section 4), while broadly aligned with those contained in the *Online Safety Act (2021)*, are not sufficiently fit for purpose. In

practice they require more specificity and flexibility to allow for the diverse range of social media services and services that incorporate social media-like functionalities. Rather than rely entirely on broad category labels such as "social media", the Code would benefit from including services that offer bundled features and designs that rely on the collection of personal information for their use such as "infinite scrolling", "algorithmic content curation", "recommendation systems" and "autoplay". This feature-based approach provides a more adaptable framework and reflects the reasoning adopted in landmark litigation against Meta and Google in Los Angeles, where core platform features were treated as design choices associated with foreseeable harms.[10]

We support the expansion of binding entities to include those services "that are not directly accessed by children but are nonetheless primarily concerned with children's activities and that such services may present comparable privacy risks" (section 5). However, we are concerned about the carve out for entities that are providing health services. It is important to recognise that a growing number of health, wellbeing, and social support/companionship services, including period tracking apps, meditation apps, and social chatbots that increasingly rely on generative AI, are marketed to, and widely used by, children and teenagers, even where this is not made explicit. Exempting health services from the scope of the Code therefore creates a potential loophole, allowing providers of these services to avoid the obligations and accountability measures established under the Code.

For this reason, **it is important that definitions must be sufficiently fit for purpose and adaptable to account for the diverse range of service types and configurations and the pace of technological change. Moreover, because of the increasingly blurred boundaries surrounding personalised health and wellbeing services, we recommend removing the exception for health services.** The Code should clarify how obligations apply to educational technologies (EdTech) in schools and other educational settings, and ambient, shared-device (multi-user) environments, where children's voice-activated interactions and other service use behaviours may be passively captured alongside those of adult account holders and other household members (e.g., voice assistant services such as Alexa), often without clear user boundaries or meaningful opportunities for consent.

# Independent privacy impact assessments

**Recommendation: Undertake privacy impact assessments conducted by independent bodies incorporating evidence-based research**

While impact assessments are generally noted as a useful mechanism for driving and assessing how privacy is designed, deployed and operationalised, the process of the assessment is often opaque. Key concerns are present within the ways in which assessments are undertaken, who does the assessing, the determination and assigning of the assessment criteria, and the measurements that are or are not in place to determine whether the privacy arrangements are suitable for users, especially younger users. Further to these concerns, privacy assessment is undertaken by the same commercial providers who manage and facilitate the platforms on which highly sensitive data activities take place, removing a large proportion of objectivity for those assessments. Privacy impact assessments should be independent and systematically evaluate interface features and user journeys as well as how privacy by design is implemented in practice.

[10] https://www.scientificamerican.com/article/what-the-meta-and-google-verdict-means-for-social-media-design/

**We urge the Government to support the formation of an independent privacy assessment body that draws on evidence-based research data for best practice for user privacy across digital environments**. We suggest these kinds of independent privacy reviews should take place periodically on digital media environments to ensure the technology providers operating in this space do indeed have user privacy not only as a core value, but as a legitimate practice that serves the people it engages.

We also urge the Government to provide a more standardised structure for privacy impact assessments, building on existing OAIC guidance, that includes accessibility as a core criterion, to account for the needs of a diverse population of internet users. The Code requires that a privacy impact assessment be conducted when a new service or activity is introduced or when there are changes to the handling personal information (section 38), however we recommend specific reference to a requirement that all entities conduct privacy impact assessments prior to the commencement of the Code and the inclusion of a mechanism for periodic (e.g., annual) reassessment to ensure that privacy protections remain effective, consistent, and responsive to evolving technologies, privacy practices, changes in service design, and patterns of use.

# A national, multidisciplinary research ecosystem

**Recommendation: Support a national, multidisciplinary research ecosystem for monitoring the impacts of the Code**

Given the complexity of the Code in its interpretation and application, and the potential for uneven and unintended impacts across populations, **we recommend that the Government support the development of a coordinated, national research ecosystem to generate independent evidence on the impacts of the Code over time**. Rather than relying on a single institution or group, this could be enabled through targeted funding mechanisms (e.g., ARC schemes or commissioned programs) that engage multiple public universities and cross-sector partners. Such an approach should explicitly support multidisciplinary research, spanning areas such as health, communication sciences, law, design, technology, and employ diverse methodological approaches, including those that centre the lived experiences of children, young people, and their support networks. This is critical to identifying unintended consequences, understanding differential impacts across populations, and ensuring that the implementation of the Code remains aligned with human rights and children's rights, without disproportionately disadvantaging certain groups.