Submission to the Office of the Australian Information Commissioner

Privacy (Children's Online Privacy) Code 2026

Exposure Draft Public Consultation

Submitted by:
Away from Keyboard Inc. (AFK)
Shop 4, 115 Anzac Avenue, Seymour VIC 3660
www.afk.org.au | 0427 203 595 | ABN: 44667764941

Contact:
[redacted], Founder and CEO
info@afk.org.au

Submission date: 5 June 2026

This submission is made in a public interest capacity and may be published. No personal information is included beyond the contact details above.

Executive Summary

Away from Keyboard Inc. (AFK) welcomes the release of the Exposure Draft of the Privacy (Children's Online Privacy) Code 2026 and commends the Office of the Australian Information Commissioner for the depth and rigour of the consultation process that has preceded it. The commitment to genuine engagement with children, young people, parents and carers alongside industry and civil society represents exactly the kind of multi-stakeholder process that good technology governance requires. The Code's core framework, particularly the privacy-by-default obligations, the consent architecture, the right to destruction, and the age-appropriate transparency requirements, represents a meaningful and overdue advance in privacy protections for Australian children.

This submission is offered in a spirit of constructive support. AFK has spent several years raising concerns about gaps in Australia's digital safety and child protection frameworks, through submissions to the Senate, correspondence with the Prime Minister and Federal Ministers, and engagement with United Nations processes including the Commission on the Status of Women, the Special Rapporteur on the Sale and Sexual Exploitation of Children, and the ITU/UN Joint Statement on Artificial Intelligence and the Rights of the Child. The issues we identify here are not new criticisms. They are longstanding concerns that we believe the Code, as currently drafted, has an opportunity to address before it is finalised and registered.

Our submission identifies twelve substantive gaps across four categories: structural and scope limitations; missing protections for specific forms of harm and vulnerable cohorts; accountability and enforcement weaknesses; and misalignment with Australia's existing international human rights commitments. We also flag a conceptual issue with the Code's foundational framing, specifically the use of 'online' rather than 'digital', which we consider the most significant structural gap in the current draft.

For each gap, we provide evidence drawn from the international human rights framework, domestic experience, and AFK's sustained advocacy, and we offer specific, actionable recommendations. We also reference Alt-TAB, AFK's pre-deployment AI ethics assessment tool, as an example of practical, accessible governance infrastructure that demonstrates what operationalised child rights protection looks like in an Australian context.

We submit these recommendations in the hope that they will strengthen a Code that Australia, and Australian children, genuinely need.

About Away from Keyboard Inc.

Away from Keyboard Inc. (AFK) is an Australian registered charity based in regional Victoria, working at the intersection of digital safety, ethical technology governance, child protection, and gender equality. Founded in 2023, AFK's work spans policy engagement, regulatory consultation, community education, and international advocacy.

AFK's engagement with the issues addressed by this Code is extensive and directly relevant. Our prior contributions include:

- Submissions to the Senate Environment and Communications References Committee on the Online Safety Codes, including detailed analysis of age assurance, TFGBV, and AI-generated harm;
- Correspondence to the Prime Minister of Australia requesting the establishment of a National Taskforce on Child Sexual Exploitation in response to the findings of the UN Special Rapporteur on the Sale and Sexual Exploitation of Children;
- Correspondence on to the Prime Minister regarding generative AI harms, non-consensual sexualised imagery, and the protection of women and girls online;

- Presentation at the United Nations Commission on the Status of Women (CSW70) on the Unsafe by Design risks of AI for the girl child;
- Engagement with the ITU/UN Joint Statement on Artificial Intelligence and the Rights of the Child (November 2025), and contribution to the Women Deliver 2026 Declaration consultation on technology-facilitated gender-based violence;
- Co-chairing of the IEEE Industry Connections Activity IC25-008-01 on AI and Family Violence (AIFV), a working group developing international standards at the intersection of artificial intelligence and domestic harm;
- Development of Alt-TAB, a pre-deployment AI ethics assessment tool that screens AI products simultaneously against 35 frameworks including child protection obligations, TFGBV standards, cybersecurity requirements, Indigenous data sovereignty principles, and jurisdiction-specific law.

AFK's Founder and CEO, Sarah Barnbrook, also holds roles as Company Secretary of the Australian Gender Equality Council, National Advocacy Lead for the Digital Safety Futures Project for Soroptimist International, and Human Rights and ICT Adviser to the National Council of Women Victoria. She is an accredited UN delegate, attending the Global Dialogue on AI Governance and an invited speaker at the WSIS forum and AI for Good Summit in Geneva (July 2026).

We bring to this submission both a sustained record of domestic and international advocacy and direct experience of the practical challenges of building accessible, human-rights-centred governance tools for an Australian context.

Section 1: The 'Online' vs 'Digital' Framing Problem

The most significant structural gap in the Exposure Draft is one of foundational scope. The Code applies to entities providing social media services, relevant electronic services, and designated internet services, as defined under the Online Safety Act 2021. All three of these categories are predicated on internet connectivity. The Code's protections, therefore, apply only where a child is engaging with a service over the internet.

This framing does not reflect the reality of how children's personal information is now collected, processed, and acted upon. A substantial and growing volume of harm to children occurs through digital technologies that are not internet-dependent, or that operate in ways the Online Safety Act's categories do not capture:

- Local AI applications: Educational software, speech-to-text tools, tutoring applications, and assistive technology for neurodivergent children frequently collect, process, and store behavioural data locally, without internet connectivity at the point of data capture.
- Offline-capable platforms: Many gaming environments, particularly console-based games and downloaded mobile applications, collect detailed behavioural profiles during offline use and synchronise this data when connectivity is restored. The data collection and profiling occurs regardless of connectivity status.
- IoT and connected devices: Baby monitors, child GPS trackers, wearable devices, and smart toys collect location, biometric, audio, and video data about children. Many of these devices do not function as 'internet services' in the Online Safety Act sense, yet they generate and transmit highly sensitive personal information.
- Closed network environments: School management platforms, learning management systems, and institutional platforms for children may operate within closed networks and not meet the definition of a designated internet service, yet they hold substantial personal information about children and make automated decisions affecting them.
- Bluetooth and near-field technologies: Technologies that exchange data at close range without internet connectivity are entirely outside the Code's current scope, yet they interact with children's personal information.

Prior advocacy

AFK raised the limitation of 'online' framing in our 2025 Senate submission on the Online Safety Codes, noting that harm does not stop at the modem. The OHCHR's 'Getting Children's Safety Online Right' framework explicitly addresses the risk that narrowly scoped regulation pushes harm toward less monitored channels. The ITU/UN Joint Statement on AI and the Rights of the Child (November 2025) consistently refers to AI systems across their full lifecycle, not only internet-connected deployments.

The UK's Age Appropriate Design Code, which the OAIC has drawn on in developing this Code, has itself been critiqued internationally for the same limitation. Australia has an opportunity to lead by adopting a broader 'digital' framing that captures the full range of environments in which children's personal information is collected and processed, consistent with the Code's stated objective of protecting children within the digital world.

Recommendation 1

Replace the Code's foundational scope definition from 'online' to 'digital', and expand the definition of covered services to include AI applications, IoT devices, offline-capable platforms, and closed network environments that collect, process, or act upon children's personal information, regardless of internet connectivity at the point of data capture.

Section 2: Artificial Intelligence is Absent from the Code

The word 'artificial intelligence' does not appear in the Exposure Draft or the Code instrument. Large language models, generative AI systems, recommender algorithms, profiling systems, and AI-generated synthetic content are not named, not defined, and not specifically regulated. This is not a minor omission. It is a structural gap in a Code designed to protect children in 2026 and beyond.

AI systems are now among the primary mechanisms through which children's personal information is collected, processed, profiled, and acted upon at scale. Recommender systems shape what children see, hear, and believe. Generative AI creates content directed at or involving children, including non-consensual sexualised imagery and AI-generated child sexual abuse material. Emotional AI companions engage children in relationships designed to encourage attachment and disclosure. Automated profiling systems make decisions about children's education, behaviour, and access to services without meaningful human oversight.

The international human rights framework has moved well ahead of the Code's current drafting on this point. The ITU/UN Joint Statement on Artificial Intelligence and the Rights of the Child (November 2025), co-signed by ITU, UNICEF, UNESCO, OHCHR, ILO, IPU, UNICRI, and the UN Special Representatives for Children, states explicitly that 'most AI-supported tools and applications, along with their underlying models, techniques and systems, are not designed with children and their well-being in mind.' The Statement calls for child rights impact assessments as part of human rights due diligence, privacy-by-design and safety approaches embedded in AI systems, prohibition of AI-powered marketing and recommendation algorithms targeting children with harmful content, and specific in-design safeguards against unhealthy emotional attachment in AI systems that mimic human interaction.

The OHCHR's ten-step framework for children's safety online specifically identifies the need to mandate human rights due diligence by companies, including child rights impact assessments conducted before platforms introduce new AI tools and features. This obligation does not appear in the Code.

Alt-TAB reference

AFK's pre-deployment AI ethics assessment tool, Alt-TAB, was developed precisely to address the gap between AI deployment velocity and governance readiness. Alt-TAB screens AI products simultaneously against 35 frameworks, including child protection obligations, TFGBV standards, cybersecurity requirements, and jurisdiction-specific law. Its existence demonstrates that AI-specific pre-deployment assessment is operationally feasible for Australian organisations of all sizes. The Code's Privacy Impact Assessment obligation in section 38 could be strengthened by incorporating AI-specific assessment criteria aligned with the child rights impact assessment methodology endorsed by the ITU/UN Joint Statement.

Section 28(2)(g) mentions automated decision-making once, in the context of access requests, noting that a child or parent may request information about 'whether there is any automated decision-making, including profiling, relating to the personal information.' This is welcome. It is not, however, a governance framework for AI systems processing children's data. It establishes a right to ask a question. It does not establish obligations on how AI systems affecting children must be designed, tested, or deployed.

Recommendation 2

Insert a dedicated Division addressing AI systems in the Code, including: a definition of AI systems and automated decision-making for the purposes of the Code; a prohibition on the

use of AI systems to generate, distribute, or facilitate access to sexualised content involving children; a requirement for AI-specific child rights impact assessments prior to deployment of AI systems likely to be accessed by or affecting children; mandatory disclosure of AI decision-making to children and parents in age-appropriate terms; and a prohibition on AI systems designed to encourage emotional attachment or dependency in children without explicit, informed parental consent.

Section 3: Technology-Facilitated Gender-Based Violence and Gendered Harms

The Code contains no reference to technology-facilitated gender-based violence (TFGBV), sextortion, image-based abuse, non-consensual sexualised imagery, or AI-generated child sexual abuse material. These are not peripheral risks. They are, according to the eSafety Commissioner's own BOSE Periodic Notices, among the fastest-growing categories of harm affecting Australian children.

The gendered dimension of digital harm to children is significant and documented. Girls experience sexual abuse, sextortion, and non-consensual image-based harm at disproportionate rates. The Australian Child Maltreatment Study found that 37.3 percent of girls had experienced child sexual abuse, and that girls were twice as likely as boys to have experienced sexual abuse. AI-generated child sexual abuse material has increased by 1,325 percent year-on-year according to eSafety Commissioner data. WeProtect Global Alliance has reported a 360 percent rise in self-generated sexual images of children aged seven to ten.

Boys are not protected from these dynamics either. Algorithmic amplification of misogynistic content, hypersexualised environments, and normalised coercive sexual narratives affect boys during formative developmental stages in ways that have documented long-term consequences for attitudes and behaviour.

The OHCHR's ten-step framework identifies TFGBV as a specific category of online harm requiring targeted regulatory response, not just coverage under general privacy principles. The ITU/UN Joint Statement specifically addresses AI-generated content that propagates hate speech, AI tools that create illegal images, and AI-based sextortion and extortion, calling for their explicit criminalisation, investigation, and sanction.

Prior advocacy

AFK has raised TFGBV as a child protection issue in multiple contexts: our 2025 Senate submission specifically identified deepfake detection, nudification, and sextortion as gaps in the Online Safety Code; our January 2026 correspondence to the Prime Minister addressed AI-generated non-consensual imagery, including estimates of approximately 2 million such images generated since 1 January 2026; and our CSW70 presentation, 'Unsafe by Design,' framed AI safety and TFGBV as a preventable harm issue at the UN level. These concerns remain unaddressed in the Code.

The Code's consent framework, privacy-by-default obligations, and best interests test are all valuable, but they do not create specific obligations relating to gendered forms of harm. A child's 'best interests' standard, applied without explicit reference to gendered harm patterns, may not reliably produce protections for the specific risks girls and gender-diverse children face.

Recommendation 3

Insert an explicit provision addressing technology-facilitated gender-based violence as a category of harm relevant to the Code's application. This should include: a prohibition on the collection or processing of children's personal information for purposes that facilitate or enable non-consensual sexualised imagery, sextortion, or grooming; a requirement that PIAs under section 38 explicitly assess gendered harm risks; a requirement that child-friendly complaints processes under section 36 include specific pathways for reporting TFGBV and image-based harm; and alignment with the eSafety Commissioner's existing BOSE obligations to create a coherent regulatory response.

Section 4: Neurodivergent and Disabled Children as a Distinct Cohort

The Code's 'best interests of the child' framework, as elaborated in the Explanatory Statement, identifies several factors relevant to assessing best interests, including the evolving capacities of children and differences in age, maturity, and developmental stage. The Explanatory Statement also notes that 'vulnerabilities of certain groups of children may need to be considered, such as children with disabilities.' This is important. However, it creates no binding obligation, and neurodivergent children are not named in the Code instrument itself.

This matters for several reasons. Neurodivergent children, including autistic children, children with ADHD, children with sensory processing differences, and children with intellectual or learning disabilities, interact with digital environments differently from neurotypical peers. They may be more susceptible to persuasive design features, more likely to form emotional attachments to AI companions, less likely to recognise grooming or manipulative consent interfaces, and more likely to benefit from genuinely age-appropriate and accessible privacy communications.

The UN Special Rapporteur on the Sale and Sexual Exploitation of Children, in her 2025 report on Australia, found that 'children with disabilities are more than twice as likely to experience physical or sexual abuse before the age of 15 than other children,' and specifically called for stronger protective measures for children with neurodevelopmental conditions. This finding is directly relevant to the Code's scope.

The Code's consent framework assumes a level of cognitive and communicative capacity that neurodivergent children may not share, particularly in relation to the 15-year age threshold for independent consent. A 15-year-old autistic child may have significantly different capacity to understand and evaluate consent notices than a neurotypical peer of the same age. The Code's binary treatment of age as the primary determinant of consent capacity does not account for this.

AFK's work includes direct advocacy on behalf of neurodivergent children. Sarah Barnbrook is a parent to three neurodivergent children and has direct experience of the ways in which digital platforms fail to account for neurodivergent needs and vulnerabilities. This is not abstract advocacy. It is grounded in the lived reality of Australian families navigating digital environments that are not designed with their children in mind.

Recommendation 4

Amend section 10 and the Explanatory Statement to create a binding obligation, not merely a listed factor, requiring entities to specifically assess the impact of their data handling practices on neurodivergent and disabled children as part of the best interests determination. Require that PIAs under section 38 include a specific assessment of disability and neurodivergence-related risks. Require that age-appropriate communications under sections 23, 24, and 27 be tested for accessibility with neurodivergent users, and that the consent framework under Division 2 acknowledge that cognitive capacity to consent may vary independently of age.

Section 5: First Nations Children and Indigenous Data Sovereignty

The Explanatory Statement identifies Aboriginal and Torres Strait Islander children as a group whose vulnerabilities 'may need to be considered' in the best interests assessment. This framing carries no binding force, and Indigenous data sovereignty, which is a distinct and established framework with its own principles and governance obligations, is not engaged with anywhere in the Code.

The UN Special Rapporteur's 2025 report on Australia documented in considerable detail the disproportionate exposure of First Nations children to sexual abuse, exploitation, and institutional harm. She found that Aboriginal and Torres Strait Islander children are 11.8 times as likely as non-Indigenous children to be in out-of-home care, that stigma and distrust of authorities severely limit disclosure and help-seeking, and that services remain inadequate and culturally unsafe for many First Nations families. She specifically called for the involvement, leadership, and participation of Indigenous communities in the design and implementation of solutions.

The CARE Principles for Indigenous Data Governance (Collective Benefit, Authority to Control, Responsibility, Ethics) and Australia's own Maiam nayri Wingara Indigenous Data Sovereignty framework establish clear expectations about how data relating to First Nations people should be collected, stored, accessed, and governed. These frameworks have not been incorporated into the Code.

This is a significant gap in an Australian context. Data about First Nations children is disproportionately collected, often through child protection, health, and education systems, and is frequently used in ways that communities have not consented to and cannot meaningfully oversee. The Code's general privacy protections apply to this data, but they do not create the culturally specific obligations that Indigenous data sovereignty frameworks require.

Prior advocacy

AFK's submissions and advocacy have consistently raised First Nations data sovereignty as a missing dimension of Australia's digital governance framework. The ITU/UN Joint Statement specifically calls for AI systems to be available in multiple languages and tailored to diverse cultural contexts, and for digital divides to be addressed to ensure equitable access for all children. These obligations have direct implications for First Nations communities.

Recommendation 5

Insert a provision in the Code requiring entities whose services are accessed by or primarily concern First Nations children to consult with relevant community representatives in the design of privacy practices, consent processes, and data handling systems. Require that PIAs under section 38 include an assessment of compliance with Indigenous data sovereignty principles, including the CARE Principles and Maiam nayri Wingara framework. Amend the best interests assessment factors in the Explanatory Statement to create a binding obligation to consider the specific vulnerabilities and rights of First Nations children, including the right to community-led data governance.

Section 6: Enforcement, Deterrence, and Proactive Compliance

The Code treats a breach as an interference with an individual's privacy under section 13 of the Privacy Act, and defers to the OAIC's existing investigation and penalty framework. This framework has historically been slow, resource-constrained, and oriented toward individual complaints rather than proactive systemic enforcement.

The challenge is not primarily one of penalty severity. It is one of enforcement architecture. The Code creates obligations but does not create mechanisms for proactive compliance monitoring, interim protective measures, or child-specific remedy pathways. The ITU/UN Joint Statement explicitly calls for 'child-friendly mechanisms for child users, their parents or other caregivers to report issues and taking responsibility for addressing such issues,' and for 'effective remedies and independent oversight, with legal consequences that serve as deterrents.'

The OHCHR framework states that all obligations 'must be supported by regular reporting mechanisms and subject to effective remedies and independent oversight.' The Code's PIA publication requirement under section 39 is a welcome transparency measure. It does not, however, create a mechanism for the OAIC to proactively identify and respond to systemic compliance failures before harm has occurred.

A specific concern is the timeframe for complaint resolution. Section 36(7) requires entities to take reasonable steps to deal with an inquiry or complaint within 30 days. For a child experiencing ongoing harm from a platform's data handling practices, 30 days is a significant period. There is no provision for interim relief, urgent escalation, or expedited response in circumstances of active harm.

Recommendation 6

Strengthen the Code's enforcement architecture by: requiring entities to publish annual compliance reports against the Code's obligations, not only PIA registers; creating a mechanism for the OAIC to conduct proactive audits of entities whose services are widely accessed by children; establishing an expedited complaint pathway for circumstances where a child is experiencing active harm; requiring entities to designate a children's privacy officer responsible for Code compliance; and introducing a mandatory notification obligation where an entity becomes aware of a breach likely to cause harm to a child, modelled on the Notifiable Data Breaches scheme.

Section 7: Child Rights Impact Assessments vs Privacy Impact Assessments

The Code requires Privacy Impact Assessments (PIAs) under section 38 before new services or activities likely to be accessed by children are made available. This is a meaningful obligation, and the content requirements in section 38(2) are substantive. However, a PIA is not the same as a Child Rights Impact Assessment (CRIA).

A PIA focuses on privacy risks. A CRIA is a broader tool that evaluates impacts across the full range of children's rights, including the right to be heard, the right to play and leisure, the right to education, freedom from exploitation, and the best interests principle. The ITU/UN Joint Statement specifically calls for 'child rights impact assessments as part of broader human rights due diligence by companies, conducted on a rolling basis ahead of platforms introducing new tools and features.' The UNICEF D-CRIA Toolbox provides an established methodology for conducting these assessments.

The Code's PIA requirements incorporate some CRIA-like elements, particularly the requirement to assess whether data handling is consistent with the best interests of the child. But the framing remains primarily privacy-focused, and the obligation does not require the

rolling, ongoing assessment cadence that the international framework contemplates. A PIA conducted before a service launches does not address the continuous evolution of that service, particularly as AI features are added or modified.

Alt-TAB reference

Alt-TAB's pre-deployment assessment methodology screens AI products against 35 frameworks simultaneously, including child protection obligations. This approach demonstrates that it is operationally feasible to integrate child rights assessment into pre-deployment processes without creating an unreasonable compliance burden. The methodology could inform the development of CRIA guidance by the OAIC.

Recommendation 7

Expand the PIA obligation in section 38 to incorporate Child Rights Impact Assessment requirements aligned with the UNICEF D-CRIA Toolbox methodology. Require that assessments are conducted on a rolling basis, not only prior to initial deployment, triggered by material changes to services, the introduction of new AI features, or evidence of emerging harm patterns. Require that CRIA findings are published in a child-accessible format, not only in the PIA register.

Section 8: Addictive Design Features

The Code addresses nudge techniques and manipulative consent practices under sections 14 and 21, prohibiting consent obtained through coercive or manipulative means. This is important and well-drafted. However, addictive design features, including infinite scroll, autoplay, persistent notifications, streak mechanics, and algorithmic amplification designed to maximise engagement time, are not addressed as a distinct category of harm to children.

The OHCHR's ten-step framework specifically identifies 'addressing addictive design (such as infinite scroll, autoplay, and persistent notifications)' as a core obligation for platform regulation. The ITU/UN Joint Statement calls for age restrictions on 'addictive design features' as a category warranting specific regulatory attention comparable to existing restrictions on pornography and gambling.

Addictive design harms children not primarily through privacy breaches but through the deliberate exploitation of developing neurological systems to extend engagement beyond healthy limits. The wellbeing impacts are documented and include sleep disruption, anxiety, depression, and reduced capacity for offline social connection. These harms are distinct from privacy harms but interact with them: addictive design increases time on platforms, which increases data collection, which enables more targeted profiling.

The Code's privacy-by-default obligation under section 9 partially addresses this by limiting default data collection to what is strictly necessary. However, this does not prohibit the use of addictive design features that do not involve data collection, and it does not create a positive obligation to audit and mitigate addictive design in services accessed by children.

Recommendation 8

Insert a provision prohibiting entities from deploying design features in services accessed by children that are specifically intended to extend engagement time beyond the child's expressed intent, including infinite scroll without natural stopping points, autoplay without opt-in, persistent re-engagement notifications outside hours designated by the user, and streak mechanics that create anxiety about discontinuing use. Require that PIAs assess addictive design risks as a distinct category of harm to children's wellbeing.

Section 9: The 15-Year Consent Age Threshold in an AI Context

The Code sets 15 as the age at which a child may independently consent to the collection, use, or disclosure of their personal information. The Explanatory Statement traces this to OAIC guidance developed following the ALRC's 2008 report, which based the threshold on research into brain development and adolescent decision-making available at that time.

We do not argue that the threshold should simply be raised or lowered. We note, however, that the research underpinning the 15-year threshold was conducted before the widespread deployment of generative AI systems, AI emotional companions, and algorithmic profiling at the scale now operating. The decision-making context for a 15-year-old consenting to the handling of their personal information in 2008 was materially different from the context in 2026.

Specifically, the OHCHR framework warns against blanket age restrictions as potentially pushing children to riskier, less monitored platforms. At the same time, the ITU/UN Joint Statement calls for age assurance mechanisms that are consistent with data protection requirements and proportionate to the identified harms. The tension between these principles requires careful, evidence-based resolution, particularly in the context of AI systems designed to encourage emotional attachment and disclosure.

Our concern is not primarily with the threshold number but with the absence of any AI-specific analysis. A 15-year-old consenting to the use of their data by a recommender algorithm, an AI emotional companion, or a generative AI system is making a qualitatively different decision from consenting to the use of their name and email address for a newsletter. The Code treats these as equivalent.

Recommendation 9

Commission and publish updated research on adolescent decision-making capacity in relation to AI-specific consent scenarios, including emotional AI, recommender systems, and generative AI. Pending that research, insert guidance in the Explanatory Statement clarifying that the 15-year threshold should be applied with particular caution in AI contexts, and that entities should adopt heightened verification and transparency obligations where AI systems are involved. Consider whether AI-specific interactions warrant a higher or more stringent consent standard regardless of the general threshold.

Section 10: Cross-Border AI Providers and Offshore Accountability

The Code's cross-border disclosure provisions in section 26 require entities to inform children of the implications of disclosing their personal information to overseas recipients under APP 8. This addresses data transfers. It does not address the distinct challenge of AI systems developed, trained, and operated offshore that process Australian children's data as part of their normal operation.

Many of the AI systems most widely used by Australian children, including large language models, AI tutoring systems, AI companions, and generative AI tools, are developed and operated by companies based primarily in the United States or elsewhere outside Australia. These companies may not be subject to the Code even if their services are widely accessed by Australian children, depending on how the Privacy Act's extraterritorial reach applies.

The ITU/UN Joint Statement calls for states to 'protect against child rights violations in the context of AI within their territory and/or jurisdiction by third parties, including business enterprises,' and to 'set out clearly the expectation that all business enterprises domiciled in their territory and/or jurisdiction respect children's rights.' The Code does not address how these obligations apply to offshore AI providers.

This is not a gap unique to this Code. It reflects a broader challenge in digital governance. However, the Code's silence on offshore AI providers means that some of the highest-risk services Australian children use may fall entirely outside its reach.

Recommendation 10

Clarify in the Explanatory Statement how the Code applies to offshore providers of AI services accessed by Australian children, including guidance on the extraterritorial application of the Privacy Act. Issue guidance on the obligations of Australian entities that procure or embed offshore AI services in their platforms. Consider, in the Code's review cycle, whether additional provisions are required to address offshore AI providers, including mechanisms for the OAIC to work with international counterparts.

Section 11: AI Literacy and Child-Facing Remedy Pathways

The Code's transparency provisions in Division 3 create meaningful obligations for entities to communicate in age-appropriate terms. Section 35 requires entities to provide children with clear information about their privacy rights. These are valuable provisions.

However, neither the Code nor the Explanatory Statement addresses AI literacy as a distinct form of digital literacy that children need to meaningfully exercise their privacy rights in AI contexts. A child's right to know whether automated decision-making is affecting them, established in section 28(2)(g), is only meaningful if the child has sufficient understanding of what automated decision-making is and how it affects them. The Code does not create any obligation on entities to support that understanding.

The ITU/UN Joint Statement calls for AI literacy to be integrated into school curricula, for non-formal educational programs to be developed for children, and for parents and caregivers to have access to guidance to help them understand AI risks and opportunities. The UNICRI AI Literacy Guide for Parents identifies specific knowledge gaps that are directly relevant to children's ability to exercise privacy rights in AI environments.

The Code's education and training obligation in section 40 applies to entity staff. There is no corresponding obligation to support children's own understanding of AI systems and their rights in relation to them.

Recommendation 11

Require entities whose services use AI systems to provide children and parents with accessible, age-appropriate explanations of how AI affects them specifically, not only general privacy information. Require that the child-friendly inquiry and complaints process under section 36 includes specific information about how to raise concerns about automated decision-making. Encourage the OAIC to develop and publish guidance on AI literacy for children and parents as a companion resource to the Code.

Section 12: Alignment with Australia's International Human Rights Commitments

Australia has ratified the Convention on the Rights of the Child and the majority of the international human rights instruments relevant to child protection. The Code sits within this framework and draws on it through the best interests principle and the right to be heard. However, several specific international commitments that are directly relevant to the Code's subject matter are not reflected in its provisions.

The ITU/UN Joint Statement on Artificial Intelligence and the Rights of the Child (November 2025) represents the most current and comprehensive statement of the international human rights framework as it applies to AI and children. AFK has engaged with this framework through our IEEE AIFV work and our participation in UN processes. The Statement's recommendations on child rights-based AI governance, data protection, child safety, and non-discrimination are largely absent from the Code.

The UN Special Rapporteur's 2025 report on Australia identified specific systemic gaps in Australia's child protection framework, including the absence of harmonised legislation, inadequate data collection and sharing mechanisms, and insufficient protections for First Nations, disabled, and migrant children. Several of the Special Rapporteur's recommendations are directly relevant to the Code's design and have not been addressed.

The Women, Peace and Security agenda, which Australia has committed to implementing, increasingly encompasses technology-facilitated harm as a core component of contemporary conflict and security dynamics. The Code's silence on gendered harm patterns represents a gap in Australia's coherent implementation of its WPS commitments in the digital domain.

Recommendation 12

The OAIC should publish a statement of how the Code aligns with Australia's obligations under the Convention on the Rights of the Child, the ITU/UN Joint Statement on AI and the Rights of the Child, and the recommendations of the UN Special Rapporteur on the Sale and Sexual Exploitation of Children. Where gaps exist, the statement should identify how they will be addressed in the Code's review cycle or through complementary regulatory action.

Additional Supportive Measures

In addition to the twelve substantive gaps identified above, AFK wishes to draw the OAIC's attention to two further matters that, while not requiring specific Code provisions, would significantly strengthen the Code's practical impact.

Regional and remote children

AFK is based in regional Victoria and has direct experience of how digital harm affects children in communities where access to specialist support, digital literacy resources, and justice pathways is more limited than in metropolitan areas. The Code's provisions for child-friendly complaints processes and age-appropriate transparency are welcome, but their practical implementation will require targeted support for entities whose services reach regional and remote communities. We encourage the OAIC to consider regional accessibility as a specific implementation priority.

Review and evolution mechanism

AI systems and digital platforms evolve rapidly, and governance frameworks risk becoming obsolete within a short period of finalisation. The Code should include a mandatory review mechanism with a cycle of no more than three years, requiring the OAIC to assess whether the Code's provisions remain adequate in light of developments in AI capabilities, emerging

harm patterns, and international best practice. The review should include consultation with children and young people as a mandatory component.

Summary of Recommendations

AFK makes the following twelve recommendations, each addressed in detail in the relevant section above:

1. Replace the Code's foundational scope definition from 'online' to 'digital', expanding coverage to include AI applications, IoT devices, offline-capable platforms, and closed network environments that collect, process, or act upon children's personal information.
2. Insert a dedicated Division addressing AI systems, including definitions, prohibition on AI-generated sexualised content involving children, AI-specific child rights impact assessments, mandatory disclosure of AI decision-making, and prohibitions on AI emotional dependency design.
3. Insert an explicit provision addressing technology-facilitated gender-based violence, including specific obligations in PIAs, complaints processes, and alignment with the eSafety Commissioner's BOSE framework.
4. Create a binding obligation requiring entities to specifically assess the impact of data handling on neurodivergent and disabled children, and require that age-appropriate communications be tested for accessibility with neurodivergent users.
5. Insert a provision requiring consultation with First Nations communities in the design of privacy practices for services accessed by Indigenous children, and require that PIAs assess compliance with Indigenous data sovereignty principles.
6. Strengthen enforcement architecture through annual compliance reporting, proactive audit mechanisms, expedited complaint pathways for active harm situations, mandatory children's privacy officer designation, and mandatory breach notification.
7. Expand PIA obligations to incorporate Child Rights Impact Assessment requirements aligned with the UNICEF D-CRIA Toolbox, conducted on a rolling basis and published in child-accessible formats.
8. Insert a provision prohibiting addictive design features in services accessed by children, including infinite scroll without stopping points, autoplay without opt-in, persistent re-engagement notifications, and anxiety-inducing streak mechanics.
9. Commission updated research on adolescent decision-making capacity in AI-specific consent contexts, and insert guidance clarifying heightened obligations where AI systems are involved.
10. Clarify how the Code applies to offshore AI providers, issue guidance on procurement of offshore AI services, and initiate international engagement with counterpart regulators.
11. Require entities using AI systems to provide accessible AI literacy information to children and parents, and develop OAIC guidance on AI literacy as a companion resource to the Code.
12. Publish a statement of alignment between the Code and Australia's obligations under the Convention on the Rights of the Child, the ITU/UN Joint Statement on AI and the Rights of the Child, and the UN Special Rapporteur's recommendations on Australia.

Conclusion

The Privacy (Children's Online Privacy) Code 2026 is a significant and genuinely needed advance in Australian privacy law. AFK supports it unreservedly as a foundation. The concerns raised in this submission are not arguments against the Code. They are arguments for making it as strong and as durable as it needs to be.

Children's digital lives are changing faster than regulatory frameworks are designed to accommodate. The AI systems, platforms, and devices that will shape Australian children's experiences in 2030 are being designed and deployed right now, without the protections this Code is intended to create. Every provision that is missing from the final Code is a gap that industry will operate within, and that children will pay the price for.

The international human rights community has moved with unusual speed and coherence on these issues. The ITU/UN Joint Statement on AI and the Rights of the Child represents the most consolidated and current expression of what is required. Australia has the opportunity, through this Code, to demonstrate that it takes these obligations seriously not merely as aspirations but as operational requirements with teeth.

AFK stands ready to contribute further to the finalisation and implementation of the Code, including through our Alt-TAB assessment methodology, our IEEE AIFV working group, and our ongoing engagement with international human rights processes. We thank the OAIC for the opportunity to contribute to this consultation and for the genuine commitment to child-centred governance that the consultation process has demonstrated.

[redacted]
Founder and CEO, Away from Keyboard Inc.
Co-Chair, IEEE Industry Connections Activity IC25-008-01 (AI and Family Violence)
Human Rights and ICT Adviser, National Council of Women Victoria
5 June 2026

References

The following sources are cited in or inform this submission, listed alphabetically:

- Australian Child Maltreatment Study (Haslam et al., 2023). Queensland University of Technology.
- Australian eSafety Commissioner (2025). Basic Online Safety Expectations (BOSE) Periodic Notice: CSEA and Sexual Extortion.
- Away from Keyboard Inc. (2025). Logged Out, Left Out: Closing the Gaps in Online Safety Codes. Submission to the Senate Environment and Communications References Committee.
- Away from Keyboard Inc. and Women 4 STEM (2025). Gender Equality in the Digital Age: Technology-Facilitated Harm as a National and Economic Security Risk. Submission to parliamentary inquiry.
- Away from Keyboard Inc. (2025). Letter to the Prime Minister of Australia regarding the UN Special Rapporteur's findings on child sexual exploitation. 9 July 2025.
- CARE Principles for Indigenous Data Governance (2020). Global Indigenous Data Alliance.
- Maiam nayri Wingara Indigenous Data Sovereignty Collective (2018). Indigenous Data Sovereignty Principles for Australia.

- National Council of Women Victoria and Away from Keyboard Inc. (2026). Letter to the Prime Minister of Australia regarding government use of X and generative AI harms. 13 January 2026.
- Office of the Australian Information Commissioner (2026). Children's Online Privacy Code: Exposure Draft and Explanatory Statement.
- Office of the United Nations High Commissioner for Human Rights (2024). Getting Children's Safety Online Right: Ten Key Steps.
- UN Committee on the Rights of the Child (2021). General Comment No. 25 on Children's Rights in Relation to the Digital Environment.
- UN Human Rights Council (2025). Report of the Special Rapporteur on the Sale, Sexual Exploitation and Sexual Abuse of Children: Visit to Australia (A/HRC/58/52/Add.1).
- UNICEF (2021). Policy Guidance on AI for Children.
- UNICEF (2025). Assessing Child Rights Impacts in Relation to the Digital Environment: Implementing the D-CRIA Toolbox.
- UNICRI, ITU, UNICEF et al. (November 2025). Joint Statement on Artificial Intelligence and the Rights of the Child.
- UN Women (2024). Normative Advances on Technology-Facilitated Violence Against Women and Girls.
- WeProtect Global Alliance (2023). Global Threat Assessment.