Submission to the Office of the Australian Information Commissioner

regarding the

Privacy (Children's Online Privacy) Code 2026

June 2026

Who we are

Digital Rights Watch is a charity founded in 2016 to promote and defend human rights as realised in the digital age. We stand for privacy, democracy, fairness, and freedom. Digital Rights Watch educates, campaigns, and advocates for a digital environment in which rights are respected, and connection and creativity can flourish. More information about our work is available on our website: www.digitalrightswatch.org.au

Acknowledgement of Country

Digital Rights Watch acknowledges the Traditional Owners of Country throughout Australia and their continuing connection to land and community. We acknowledge the Aboriginal and Torres Strait Islander peoples as the true custodians of this land that was never ceded and pay our respects to their cultures, and to elders past and present.

Contact

[redacted]

Contents

Privacy (Children's Online Privacy) Code 2026 **1**
Who we are 2
Acknowledgement of Country 2
Contact 2
Contents 3
General Position **4**
The Australian Privacy Principles and the privacy of children: our views and evidence **5**
Section 8: Ascertaining the age of end-users of an entity's service 5
Section 9: Entities may collect personal information about a child by default only if strictly necessary 6
Section 10: Collection of personal information about a child must be reasonably consistent with best interests of the child 7
Section 11: Use or disclosure of personal information about a child must be reasonably consistent with best interests of the child 8
Section 13: Consent given by child or person with parental responsibility 9
Section 14-19 Consent must be voluntary, informed, current, withdrawable, specific, unambiguous 10
Section 20: Assent of child under 15 years must be obtained in certain circumstances 11
Section 21: Consent must not be obtained by coercion etc. 12
Section 23-4: APP privacy policy requirements; Notification of the collection of personal information 13
Section 25: Review of privacy practices etc. 14
Section 26: Consent to cross-border disclosures 15
Section 27-28 Accessing personal information & request access to information about handling of personal information 16
Section 29 Opting out of direct marketing 17
Section 30 Dealing with requests for access to personal information about children 18
Section 31 Dealing with requests to correct personal information about children 19
Section 32 Request to destroy personal information about a child 20
Section 33 Notification of mechanisms that monitor or control service use or monitor geolocation 21
Sections 34-36 Application of this Code in relation to inquiries and complaints, Information about children's privacy rights, Child-friendly inquiry and complaints processes 22

General Position

Digital Rights Watch (DRW) welcomes the opportunity to provide feedback on the OAIC's *Exposure Draft* on the *Children's Online Privacy Code* (COPC).

The exposure draft of the COPC is an extremely welcome development, and DRW is broadly supportive of this initiative. The development of the COPC represents an important step forward for Australia's privacy landscape, which otherwise lags behind many comparable jurisdictions. With many Australians expressing concerns about the dangers and limitations of online environments, especially for young people, the draft COPC represents a rights-respecting approach to addressing a range of these concerns.

DRW supports the OAIC's objective of protecting children through strengthened privacy protections, rather than preventing children from engaging in the digital world. We see this approach as supportive of human rights such as freedom of expression and the best interest of the child. The Internet is a vital component of modern civil life and it is vital for the health of our democracy and of us as individuals that children are able to participate in the online world.

We do have some concerns about gaps in implementation and potential side-effects of some of the regulation, which is addressed in our submission.

We would like to note that the OAIC's approach to community consultation during the course of producing the COPC has been exemplary. We would like to thank the OAIC for engaging with us, and civil society more broadly, in the spirit of genuine dialogue and co-creation of the code. We have noticed the important efforts made by the OAIC in seeking input from children in particular, which we appreciate comes with various challenges, but will ultimately result in a better COPC. It has been a refreshing approach and one that we hope other governmental and regulatory agencies will use as a template for future consultations.

We refer the Commission to our previous submission on the Children's Online Privacy Code for general comments on children's privacy online.

The Australian Privacy Principles and the privacy of children: our views and evidence

Section 8: Ascertaining the age of end-users of an entity's service

DRW supports the framing that entities which treat all users with the same privacy protections as a child do not require age assurance. This incentivises entities who wish to avoid the cumbersome task of implementing age assurance to implement strong privacy protections, while allowing all Australians to benefit from enhanced privacy protections. As much as possible, DRW is of the view that this should be encouraged as the standard, default position for relevant services that are subject to the COPC.

To preserve the intention of the COPC, the default behaviour of entities must assume that users are children, unless proven otherwise. Without this, children will be assumed to be adults, and will continue to be exposed to harmful data practices.

DRW has the position that age assurance across platforms should be minimised, and used only where it is necessary and proportionate. The entrenching of age assurance into the Australian digital landscape raises serious concerns around data privacy.

Age assurance technologies currently approved by regulators have serious privacy shortcomings. The ability of this technology to meaningfully protect children's privacy is limited, given the concerns about reliability and in circumstances where the approved pathways for age assurance introduce new privacy harms.

Entities who wish to conduct age verification should ensure that their use of age assurance technology is limited and necessary, and generally align with a human rights approach. For example age assurance technology should be implemented only upon the creation of an account, as opposed to throughout the user's engagement with the platform.

Section 9: Entities may collect personal information about a child by default only if strictly necessary

DRW strongly supports default data collection only when *strictly necessary*. DRW supports the definition of 'strictly necessary' being information without which the delivery of the service would be impossible.

DRW also supports default settings for a child that are always privacy maximising. Any concessions made, such as for marketing, should always be opt-in. Furthermore, opting in must only be done with consent standards that are reflected elsewhere in the COPC, that is voluntary, informed, current, withdrawable, specific, unambiguous consent.

Section 10: Collection of personal information about a child must be reasonably consistent with best interests of the child

DRW supports that collection of a child's personal information must be consistent with the best interests of the child. DRW notes that the term "best interests of the child" is undefined within the COPC code. Given the subjective nature of this term, the Code would benefit from a clear definition, such as the one provided by Article 3 of The United Nations Convention on the rights of the Child offers the following definition,

> *"1. In all actions concerning children, whether undertaken by public or private social welfare institutions, courts of law, administrative authorities or legislative bodies, the best interests of the child shall be a primary consideration.*
>
> *2. States Parties undertake to ensure the child such protection and care as is necessary for his or her wellbeing, taking into account the rights and duties of his or her parents, legal guardians, or other individuals legally responsible for him or her, and, to this end, shall take all appropriate legislative and administrative measures.*
>
> *3. States Parties shall ensure that the institutions, services and facilities responsible for the care or protection of children shall conform with the standards established by competent authorities,*

particularly in the areas of safety, health, in the number and suitability of their staff, as well as competent supervision."[1]

DRW recommends extending the "best interests" principle to the entirety of the COPC, including to cover parental disclosure. Extending the "best interests" principle minimises the risk of loopholes being exploited in the COPC in a way that does not reflect the intention underlying its drafting.

When services consider whether the collection of a child's personal information is in the best interests of the child, DRW is of the view that such services should factor in the risks of a data breach, whereby the data is compromised and published. There should be an active obligation to consider the possibilities of such risks, even though the relevant entity might engage in its best efforts to prevent such an occurrence, given data breaches are a known and demonstrable problem in the Australian cybersecurity landscape. As the OAIC is well aware, 47% of Australians experienced a data breach in the period from 2022 to 2023 , and three quarters reported suffering harm as a result.[2] Since 2023 data breaches have consistently become more common in Australia.[3] Any risk analysis conducted by a relevant service must reflect this reality.

Section 11: Use or disclosure of personal information about a child must be reasonably consistent with best interests of the child

DRW addresses the issue of direct marketing further below in respect of section 29. For the purposes of this section, we note that DRW does not consider direct marketing to be consistent with the best interests of young children. Young children struggle to identify advertising, making them

---

[1] Convention on the Rights of the Child, opened for signature 20 November 1989, 1577 UNTS 3 (entered into force 2 September 1990) art 3, https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-rights-child.
[2] Office of the Australian Information Commissioner, Australian Community Attitudes to Privacy Survey 2023 (Report, 2023) 60–61 https://www.oaic.gov.au/__data/assets/pdf_file/0025/74482/OAIC-Australian-Community-Attitudes-to-Privacy-Survey-2023.pdf.
[3] Office of the Australian Information Commissioner, 'OAIC Stats Show Record Year for Data Breaches' (Web Page) https://www.oaic.gov.au/news/media-centre/oaic-stats-show-record-year-for-data-breaches.

particularly impressionable to the messaging.[4] Even when older children are able to identify advertising they lack the experience and cognitive ability to think critically about marketing messages.[5]

Furthermore, young children lack the financial independence required to understand and respond to targeted marketing in an informed way.

Direct marketing has adverse outcomes for children and is linked to family stress,[6] body image issues,[7] and childhood obesity.[8]

Accordingly, the use of disclosure of personal information about a child for the purposes of direct marketing should not be permitted for young children.

Section 13: Consent given by child or person with parental responsibility

DRW supports involving people with parental responsibility in the provision of the child's consent, and we think this approach to consent is

---

[4] Advertising Standards Authority and Committee of Advertising Practice, 'Recognising Ads: Children' (Web Page, 15 June 2022) https://www.asa.org.uk/advice-online/recognising-ads-children.html.

[5] Obesity Evidence Hub, 'Unhealthy Food Marketing and Children: Exposure and Impact' (Web Page, 23 April 2026) https://www.obesityevidencehub.org.au/collections/prevention/the-impact-of-food-marketing-on-children; Brian L Wilcox et al, Report of the APA Task Force on Advertising and Children (Report, American Psychological Association, 20 February 2004) 5 https://www.apa.org/pi/families/resources/advertising-children.pdf.

[6] L Bouakaz, 'The Impact of Digital Marketing on Parent-Child Relationships and Family Dynamics' (2025) 5(5) Journal of Posthumanism 379, 379–98 https://posthumanism.co.uk/jp/article/view/1347.

[7] A Slater et al, 'Just One Click: A Content Analysis of Advertisements on Teen Web Sites' (2012) 50(4) Journal of Adolescent Health 339, 339–45 https://research.sahmri.org.au/en/publications/just-one-click-a-content-analysis-of-advertisements-on-teen-web-s/; G Holland and M Tiggemann, 'A Systematic Review of the Impact of the Use of Social Networking Sites on Body Image and Disordered Eating Outcomes' (2016) 17 Body Image 100, 100–10 https://www.sciencedirect.com/science/article/abs/pii/S1740144516300912.

[8] Institute of Medicine of the National Academies, Food Marketing to Children and Youth: Threat or Opportunity? (National Academies Press, 2006) 2 https://books.google.com.au/books?hl=en&lr=&id=a_NyI4G3rHwC&oi=fnd&pg=PA1&ots=fGVoS0VUoE&sig=JV3JYeo0AeyjyUT4GuQAzSY2QaQ&redir_esc=y#v=onepage&q&f=false; S Linn, 'The Commercialization of Childhood and Children's Well-Being: What Is the Role of Health Care Providers?' (2010) 15(4) Paediatrics & Child Health 195, 195–7 https://pmc.ncbi.nlm.nih.gov/articles/PMC2866310/#b1-pch15195.

forward thinking and reflective of concepts such as autonomy and responsibility as relevant to both parties.

The COPC would be strengthened by the inclusion of explanatory notes that describe the levels of consent that a child of a certain age is able to provide, and the sorts of requests that an entity could make.

Further guidance relating to what constitutes “reasonable steps” to verify the person providing consent holds parental responsibility over the child will help prevent privacy invasive practices. Any data handed over in this process must be destroyed as soon as guardianship is confirmed, it should never be used to profile the user or used for marketing purposes.

Section 14-19: Consent must be voluntary, informed, current, withdrawable, specific, unambiguous

DRW very much supports the detailed definition of consent provided by the COPC, which we are pleased to see aligns with a human rights approach.

The COPR should specify that consent which is not voluntary, informed, current, withdrawable, specific, unambiguous is not consent. It is the responsibility of the entity to ensure that the consent obtained reaches these standards.

DRW is pleased to see an explicit prohibition on “dark patterns” for consent-gathering through manipulation or ambiguity. In particular, the exclusion of “consent” gained through the practice of denying use of a service if the customer does not accept marketing practices. DRW also commends the exclusion of bundled consent from being valid consent.

Ensuring that consent communications are written in understandable language is a vital part of sections 14-19. Clear consent communications will not just benefit children, but also their parents. While adults who speak English as a second language will especially benefit from clear privacy policies, everybody stands to gain from clearer communication around privacy.

Currently, it would take an Australian 14 hours a day to read all of the privacy policies he or she encountered in a single day.[9] Mandating that entities have understandable privacy policies will reduce the amount of time it takes to read a policy. DRW is hopeful this will remove a barrier to engagement with privacy policies.

Withdrawable consent is a vital tool for children's privacy. DRW recommends that consent be given a default expiry date after which it will have to be re-granted. Conceivably, this could be attached to age bands used to define what levels of consent are possible with or without parental consent.

In terms of consent specificity, this also needs to be bound to a future expiry date as perpetual consent is far from specific.

Section 20: Assent of child under 15 years must be obtained in certain circumstances

Requiring a child's assent before changing their privacy protections is a welcome and important safeguard. It recognises children are rights-holders with developing autonomy and have a personal stake in how their information is handled.

This approach is also practically valuable. Involving children in privacy decisions helps them build the skills they will need as adults, when they will be expected to make these choices independently.

Section 21: Consent must not be obtained by coercion etc.

DRW strongly supports that consent must not be obtained by coercion. We think it is appropriate especially in light of the recent findings by the Privacy Commission around renters' personal information being collected

[9] Brendan Kearns, 'Who Has 14 Hours to Read Privacy Policies?' CHOICE (Web Page, 22 July 2024) https://www.choice.com.au/data-protection-and-privacy/data-collection-and-use/who-has-your-data/articles/managing-your-privacy-report.

under pressure.[10] DRW is hopeful that the prohibition on coerced consent will protect consumers from tactics such as confirmation shaming.

The Code makes it clear that protections apply not only to personal information children create or provide about themselves, but also to information created, inferred or supplied by others about them.

This is particularly important in sectors such as rent-tech, where platforms have historically used manipulative design practices to pressure rental applicants into disclosing information about their children.[11] The Information Commissioner has already found that confirmation shaming can breach the Australian Privacy Principles.[12] It is appropriate that the COPC build on this position by providing stronger, child-specific protection against practices that pressure children or those with parental responsibility to disclose unnecessary information about a child.

Entities should only be permitted to withdraw, limit or refuse a service where the rejected data collection is strictly necessary for the service to function. The onus should lie with the entity to demonstrate this. A refusal to provide optional or excessive information about a child should not result in a penalty, degraded service, or exclusion from essential opportunities such as housing.

Section 23-24: APP privacy policy requirements; Notification of the collection of personal information

DRW approves strongly of the requirements to ensure that privacy policies are in clear, simple, and accessible language. Not only is this required to

---

[10] Office of the Australian Information Commissioner, 'RentTech Platforms Must Stop Unfair and Excessive Personal Information Collection, Says Privacy Commissioner' (Web Page, 22 April 2026) https://www.oaic.gov.au/news/media-centre/renttech-platforms-must-stop-unfair-and-excessive-personal-information-collection,-says-privacy-commissioner.

[11] Andy Kollmorgen and Kate Bower, 'RentTech Platforms Making Renting That Much Harder' CHOICE (Web Page, 18 April 2023) https://www.choice.com.au/data-protection-and-privacy/data-collection-and-use/how-your-data-is-used/articles/choice-renttech-report-release.

[12] Office of the Australian Information Commissioner, 'RentTech Platforms Must Stop Unfair and Excessive Personal Information Collection, Says Privacy Commissioner' (Web Page, 22 April 2026) https://www.oaic.gov.au/news/media-centre/renttech-platforms-must-stop-unfair-and-excessive-personal-information-collection,-says-privacy-commissioner.

communicate clearly with children, it will also help adults with lower levels of literacy to understand what an entity is doing with their data.

DRW strongly believes in the value of non-text material in communicating privacy practices. Evidence from multimedia learning and health-literacy research indicates that people understand and retain information better when plain language is paired with clear visual or audio support.[13] This is particularly relevant for children, who may benefit from age-appropriate icons, examples, diagrams, video or interactive explanations.

Section 25: Review of privacy practices etc.

Entities should be required to provide records of reviews and changes made when privacy policies are updated. Entities should be prohibited from alerting users to unspecified changes and directing them towards the new privacy policy. Changes between newer and older versions can be difficult to identify, particularly in longer texts, however bolding or italicising the changes can assist people in identifying the differences.[14] Users should be able to easily track the changes made in updated versions of the privacy policy.

Change recording is already regarded as good privacy governance in the UK.[15]

The reviews of privacy practices conducted by entities should be provided to the OAIC by default. The OAIC should keep a register of privacy practices of APP covered entities, and provide access to the public of these policies on request.

---

[13] N Mbanda et al, 'A Scoping Review of the Use of Visual Aids in Health Education Materials for Persons with Low-Literacy Levels' (2021) 104(5) Patient Education and Counseling 998, 998–1017 https://www.sciencedirect.com/science/article/abs/pii/S0738399120306583; R E Mayer, 'The Past, Present, and Future of the Cognitive Theory of Multimedia Learning' (2024) 36 Educational Psychology Review 8 https://link.springer.com/article/10.1007/s10648-023-09842-1.

[14] C Emmott, A J Sanford and L I Morrow, 'Capturing the Attention of Readers? Stylistic and Psychological Perspectives on the Use and Effect of Text Fragmentation in Narratives' (2006) 35(1) Journal of Literary Semantics 1, 1–30 https://eprints.gla.ac.uk/5968/.

[15] Information Commissioner's Office, 'Records of Processing and Lawful Basis' (Web Page) https://ico.org.uk/for-organisations/advice-and-services/audits/data-protection-audit-framework/toolkits/accountability/records-of-processing-and-lawful-basis/.

Section 26: Consent to cross-border disclosures

Children should not be able to consent to entities using offshore processing to reduce their privacy protections.

Entities using offshore processing must adhere to protections of the COPC, regardless of user consent or alternative regulations in the offshore location. If the privacy regime of the offshore processing location is incompatible with the COPC, for example, if states have unfettered access to the data, alternative locations for processing should be sought.

If entities are unable to provide their service without offshore processing, they should anonymise children's data before sending it to the offshore provider eg: by replacing identifiable data points with UUIDs that are only connected to the user within Australia and under coverage of domestic privacy laws.

DRW notes the research by Vanessa Teague in reidentifying de-identified data. Her work illustrates the importance of entities understanding what is required to achieve genuine anonymisation.[16] DRW suggests that the OAIC publish guidance on how all data, particularly children's, can be safely anonymised.

[16] Priya Dev and Vanessa Teague, '"Anonymous" Voting Software Used by Some of Australia's Biggest Companies Is Flawed, New Investigation Reveals' The Conversation (online, 3 December 2024) https://theconversation.com/anonymous-voting-software-used-by-some-of-australias-biggest-companies-is-flawed-new-investigation-reveals-244181; Vanessa Teague, 'Australia Doesn't Have Online Voting for Federal Elections and We Should Keep It That Way' The Conversation (online) https://theconversation.com/australia-doesnt-have-online-voting-for-federal-elections-and-we-should-keep-it-that-way-180865; Chris Culnane, Benjamin I P Rubinstein and Vanessa Teague, 'Two Data Points Enough to Spot You in Open Transport Records' Pursuit (online, 15 August 2019) https://pursuit.unimelb.edu.au/articles/two-data-points-enough-to-spot-you-in-open-transport-records; Josh Taylor, 'Melbourne Professor Quits after Health Department Pressures Her over Data Breach' The Guardian (online, 7 March 2020) https://www.theguardian.com/australia-news/2020/mar/08/melbourne-professor-quits-after-health-department-pressures-her-over-data-breach.

Section 27-28: Accessing personal information & request access to information about handling of personal information

The right to access one's own personal information should be accessible to children. DRW therefore supports that entities who provide children with access to their own data should do so in a way that is understandable to the child.

We do note that access to children's data can be weaponised, particularly in family violence contexts.

Care should be taken to ensure sections 27 and 28 are not misused by hostile actors for the purpose of harassing another person. As these sections currently stand, a parent may utilise their parental right to the child's data to learn the address of an ex-partner with custody. We note that 27% of family violence cases involve the technology enabled abuse of children.[17]

The introduction of exemptions similar to those outlined in section 32(3) would mitigate the risk of access to children's data being weaponised.

Section 29: Opting out of direct marketing

Direct marketing is unlikely to be in the best interests of children and should not be directed to them as a default.

If the Code permits direct marketing to children in limited circumstances, it should require clear, informed, opt-in consent. Consent should not be bundled with other permissions or obtained through default settings, pre-ticked boxes, dark patterns, or pressure to accept.

Any opt-in consent should also be time limited. Children's understanding, preferences and capacity develop over time, and consent given at one age should not be treated as ongoing permission to receive direct marketing

[17] eSafety Commissioner, 'Children and Technology-Facilitated Abuse in Domestic and Family Violence Situations' (Web Page) https://www.esafety.gov.au/research/children-and-technology-facilitated-abuse-in-domestic-and-family-violence-situations.

indefinitely. Entities should be required to seek renewed consent at regular intervals, using age-appropriate language and design.

Section 32: Request to destroy personal information about a child

The right to request the deletion of one's personal data is important, so DRW supports the right to delete for children.

The Code should consider a default deletion requirement for children's data when a child turns 16, unless the young person gives clear, informed consent for that data to be transferred into an adult account.

The Code should also require entities to delete children's personal information by default once it is no longer necessary to provide the service. This obligation should apply throughout the life of the account, not only at account closure or transition to adulthood. Nor should the obligation only arise in response to a request from the child or a person with parental responsibility. For example, if a child's home address is collected at sign-up to send physical items, that information should be deleted once the items have been delivered and the address is no longer required.

This approach would ensure that children are not followed into adulthood by unnecessary data collected when they had limited capacity to understand or control its future use.

Section 33: Notification of mechanisms that monitor or control service use or monitor geolocation

Children should be notified when their geolocation is being tracked or shared. The COPC would benefit from further clarification regarding which tools might infer user location eg; IP address, or proximity to other location-aware devices. The COPC should make clear that inferred location information is subject to the same user protections as directly collected location.

Geolocation-sharing with other user accounts should require regular consent validation. A "set and forget" approach is not appropriate as

children's preferences may change as they age, and importantly, their circumstances may also change. Geolocation sharing can pose serious risks to safety, particularly in family violence contexts, for example, as a parent could provide a device to a child with a geolocation-sharing in order to harass the parent with custody.

Entities should be required to consider if fuzzy location-sharing is sufficient for the purposes of their service, rather than precise location-sharing, and prioritise the most privacy protecting alternative.

Sections 34-36: Application of this Code in relation to inquiries and complaints, Information about children's privacy rights, Child-friendly inquiry and complaints processes

DRW is supportive of sections 34, 35 and 36. DRW's view is that for the purposes of transparency and scrutiny, entities should hold reporting obligations regarding complaints and the timeliness of the resolution. Users filing complaints should be made aware that basic, non-identifiable information regarding their complaint may be made available to the OAIC for reporting purposes. Reporting should never identify the individual who filed the complaint.

When entities make changes to their collection notices, updated collection notices which specifically highlight the changes made should be provided to users.

Sections 37-40: Privacy impact assessments; privacy education and training

DRW supports Privacy Impact Assessments (PIAs) being mandatory when entities provide a new or changed service that is likely to hold data relating to children.

The COPC would benefit from further clarification regarding section 39(2). In particular, DRW's view is that the COPC should indicate whether the

register is to be publicly accessible, and if so whether the language is required to be understandable to children. Regardless of the publishing of the PIA register online, entities should be required to file PIAs with the OAIC by default.

DRW is supportive of mandatory staff training for all staff who have "regular or frequent access to children's personal information" regarding the safe and responsible handling of this data. Staff training should include education on tech-facilitated-family-violence and prompt employees to consider how the service they provide could be weaponised in family and gender-based violence contexts. The COPC should extend to provide avenues for staff to report non-compliance with the COPC without fear of repercussions from the entity.