

Privacy (Children's Online Privacy) Code 2026

Submission to the Office of the Australian
Information Commissioner

05 June 2026

www.humanrights.gov.au

ABN 47 996 232 602
GPO Box 5218, Sydney NSW 2001
General enquiries 1300 369 711
National Info Service 1300 656 419



**Australian
Human Rights
Commission**

Contents

Overview	4
Recommendations	4
1 Best interests of the child	5
Voices of children	5
Direct marketing	6
2 Age assurance	8
Growing reliance on age assurance	8
3 Privacy law reform	10
4 Scope	11
Likely to be accessed by children	11
5 Evolving capacity	12
Endnotes	13

About the Australian Human Rights Commission

Our vision is an Australian society where human rights are respected, promoted and protected and where every person is equal in dignity and rights.

The Commission's key functions include:

- Access to justice: We help people to resolve complaints of discrimination and human rights breaches through our investigation and conciliation services.
- Fairer laws, policies and practices: We review existing and proposed laws, policies and practices and provide expert advice on how they can better protect people's human rights. We help organisations to protect human rights in their work. We publish reports on human rights problems and how to fix them.
- Education and understanding: We promote understanding, acceptance and public discussion of human rights. We deliver workplace and community human rights education and training.
- Compliance: We are the regulator for positive duty laws requiring employers and others to address sexual harassment, sex discrimination and other unlawful conduct.

Australian Human Rights Commission www.humanrights.gov.au

ABN 47 996 232 602

GPO Box 5218 Sydney NSW 2001

For general enquiries, call us on 1300 369 711.

For complaints, call us on 1300 656 419.

For TTY, call 1800 620 241.

Overview

1. The *Privacy (Children's Online Privacy) Code 2026* (Code) is an important and necessary step in strengthening protections for children and young people in the digital environment. The Code appropriately centres the best interests of the child and introduces higher standards for how information about children is collected, used and disclosed. These are significant improvements that reflect guidance from the UN Office of the High Commissioner for Human Rights that the maximum protection of children's data be the default setting.¹
2. At the same time, the Code reflects a broader shift in Australia's digital regulatory approach, where many measures rely on age assurance to distinguish between children and adults online. This is contributing to a bifurcated model in which children and adults experience different digital environments. As reliance on these mechanisms grows, there is a risk that measures intended to protect children introduce new harms, including reduced access to information.
3. This submission supports the enactment of the Code as an important reform to Australia's privacy framework for children and young people.

Recommendations

Recommendations

1. The Office of the Australian Information Commissioner should enact the *Privacy (Children's Online Privacy) Code 2026*.

1 Best interests of the child

The Code's requirement that the best interests of the child be a primary consideration is a key strength, ensuring that the handling of children's personal information prioritises their rights and wellbeing in the digital environment.

4. Making the best interests of the child the primary principle when collecting, using and disclosing information is a key strength of the Code – as privacy measures must be developed in accordance with article 3 of the United Nations *Convention on the Rights of the Child* (CRC). Despite the CRC's importance in the Code, it is not as expressly set out as it could be. It is important that the visibility of the CRC be raised throughout the Code to ensure socialisation of the underpinning framework to the Code.
5. General Comment No. 14 (2013) on the Right of the Child to have their Best Interests taken as a Primary Consideration, issued by the United Nations Committee on the Rights of the Child, may be useful in any future consideration of the factors set out in the Exposure Statement. The Committee suggests drawing up a non-exhaustive and non-hierarchical list of elements that could be included by any decision-maker to determine the best interests of a child. These must be taken into consideration and balanced in light of each situation.²
6. Once identified, the best interests of the child may conflict with the interests of others, and this must be resolved on a case-by-case basis by carefully balancing the interests of all parties. However, decision-makers must bear in mind that 'the right of the child to have their best interests taken as a primary consideration means that the child's interests have high priority and not just one of several considerations'.³

Voices of children

7. Best interest considerations should not be based on assumptions about what is in the interests of children. Their views must be actively considered.⁴ In this regard, the Special Rapporteur on the Right to Privacy notes that an 'adult's interpretation of children's privacy needs can impede the healthy development of autonomy and independence and restrict children's privacy in the name of protection'.⁵ The Special Rapporteur elaborates:

While children's dependency, hence vulnerability, can result in risks, risk does not equate to harm and navigating some risk is necessary for children to develop resilience and coping skills. Defining children by their vulnerability only, without consideration of their capacity or potential, is likely to result in overly protectionist agendas, potentially harmful to children's personality.⁶

8. Children from different cultural backgrounds may also experience and interpret digital risks and opportunities differently. The Code should give culturally sensitive guidance and support that reflects the diverse realities of children and the communities who support them to realise their rights.⁷ As noted by the UN Office of the High Commissioner for Human Rights:

Children have the right to be heard, including on how digital environments are designed, governed and regulated, and must have a say in shaping the digital world that shapes their lives.⁸

9. It is heartening to see commitment from the OAIC to ensure that the Code reflects the varied experiences and voices of children and young people. The extended timeline for feedback, launch of [Privacy for Kids](#), age-appropriate ways of engaging (e.g. provision of workbooks) for example demonstrate a genuine and best practice commitment to ensuring the voices of children and young people are heard.
10. The Commission commends OAIC's genuine engagement with children, which reflects a best practice approach that other regulators should be encouraged to replicate.

Direct marketing

11. In a digital economy, many businesses rely upon the collection and use of data to target advertising. While adults may have developed capacity to determine advertising from genuine information, younger children are more vulnerable as they do not as easily differentiate between advertising and reality.⁹ This necessitates the Code's proportionate approach which applies additional protections for children, while still allowing direct advertising for adults.
12. The Code does not prohibit direct marketing, with the Explanatory Statement noting that the best interest test 'does not mean that an entity cannot pursue its own commercial or other interests'. However, it is unlikely that direct marketing will satisfy the high bar set by the best interests test.¹⁰
13. Direct marketing is shaping the experiences of children online, and not always for the better.¹¹ As expressed by General Comment No. 25 on Children's Rights in relation to the Digital Environment, commercial activity and processing of personal information:

... may result in violations or abuses of children's rights, including through advertising design features that anticipate and guide a child's actions towards more extreme content, automated notifications that can interrupt sleep or the use of a child's personal information or location to target potentially harmful commercially driven content.¹²

14. This is especially important given the Special Rapporteur estimated that ‘the online advertising market for children could be worth 1.7 billion by 2021, with more than 72 million pieces of data collected for each child by online advertising companies before the child reaches the age of 13’.¹³
15. Additionally, the Special Rapporteur on the Right to Privacy has also highlighted their concern about such profiling, which can limit a child’s potential self-development – as ‘behavioural predictions and nudging techniques can predetermine options and choices’.¹⁴
16. General Comment No. 25 states that countries should make the best interests the primary consideration when regulating advertising and marketing.¹⁵ Although the Code is not intended to regulate direct marketing, by imposing additional obligations on advertisers to ensure the best interests of the child, the Code is complying with Australia’s obligations under the CRC.¹⁶ More recently, the UN Office of the High Commissioner for Human Rights has stated that the micro-targeting of children for marketing purposes should not be permitted.¹⁷
17. A related consideration is the impact of stricter data collection restrictions on recommender systems. While this may limit personalisation, it can reduce risks associated with profiling and the amplification of harmful content. It may also support a more neutral information environment for children. Any constraint on recommender systems should therefore be understood as an important safeguard, while ensuring services can still support access to age-appropriate content without intrusive data practices.
18. While some marketing will be impacted, for the purposes of protecting children and their development this is, in our view, a proportionate restriction.

2 Age assurance

The Code's reliance on age assurance raises concerns, as these mechanisms are increasingly central to digital regulation despite posing risks to privacy and other rights.

19. There are significant human rights concerns that need to be considered in the context of increasing reliance on age assurance processes. The technology is immature and often poses risks to privacy and other human rights.¹⁸ In particular, the growing use of government-issued identification and facial recognition technologies (FRT) are concerning, with the Commission having previously identified concerns about their use, particularly in the absence of mandatory human rights safeguards.¹⁹
20. 'Age inference' enables platforms to draw probabilistic conclusions about a user's likely age based on behavioural patterns, contextual data and metadata already held by the service.²⁰ While this method creates less friction, it relies on pervasive surveillance and profiling which includes accessing:
 - photos
 - tags
 - connections
 - engagement activity
 - linguistic analysis and/or
 - school-hour login patterns.
21. While the OAIC has released [privacy guidance on age assurance technologies](#) (in addition to entering into a Memorandum of Understanding with eSafety) there are still significant concerns.

Growing reliance on age assurance

22. A broader concern arising from the Code is the extent to which digital regulation in Australia is becoming dependent on age assurance. An increasing number of regulatory measures aimed at improving safety and protecting human rights rely on the ability to distinguish between children and adults online. This includes the social media ban, SES Codes and potentially the proposed Digital Duty of Care.
23. This trend is contributing to a bifurcated model of digital regulation, where one set of rules applies to young people and another applies to adults. This approach is not inherently problematic. Different standards for children and adults have long been recognised, including through content classification systems (e.g. film classifications). A bifurcated model can also avoid the application of restrictive child-settings to adults, that would otherwise limit lawful access to information.

24. The shift toward a dual digital experience also affects how young people encounter information and form views. Earlier regulatory models, such as film classification, operated in a context where content could be clearly categorised and limited. In contrast, the online environment is continuous and embedded in everyday life.
25. A further concern is the limitation of current age assurance technologies, which have repeatedly had problems with accuracy for women and people from racialised groups.²¹ There is also growing evidence that the age assurance being implemented are not effective, being bypassed by many under-16s.²² Reliance on these systems is therefore problematic, as they can be bypassed in practice, creating a risk that regulatory measures appear effective while failing to restrict access.
26. In this context, a segmented online experience risks producing a narrow or mediated representation of the world for younger users. While restricting access to harmful content is appropriate, overly rigid or opaque filtering limits the opportunity for gradual exposure and critical engagement. This is particularly relevant in relation to civic and political information, where exposure to different perspectives supports informed participation and the development of independent views.
27. The increasing reliance on age assurance within regulatory design warrants scrutiny. While there are few workable alternatives to enable a bifurcated model, the growing dependence on age assurance as the mechanism for doing so raises significant concerns. The primary concern is the use of age assurance as the gateway to a bifurcated system. A secondary concern is the longer-term effect of such a system, particularly the extent to which it may restrict access to information or undermine the autonomy of children as they mature.

3 Privacy law reform

Privacy law reform is necessary to support and reinforce the Code, ensuring that broader gaps in the current framework do not undermine protections for children's personal information.

28. Children's right to privacy raises specific issues due to:
 - the vulnerability of children
 - the role and responsibilities of parents in raising their children
 - children's evolving capacities and development impacting on consent mechanisms.
29. While this Code represents a significant improvement to Australia's privacy landscape, it is only part of the necessary reforms to the *Privacy Act 1988* (Cth) which the Australian Government has committed to.²³ The Act in its current form is no longer fit-for-purpose, with the previous Attorney-General stating that it 'has not kept pace with the changes in the digital world'.²⁴
30. The Code's reliance on age assurance should be supported by the introduction of the full suite of proposed privacy reforms, which are urgently required to address the increasing threat to privacy in the modern world. The Australian Government must prioritise tranche two of reforms – including the introduction of a 'fair and reasonable test' that would operate as a 'shield' against excessive data collection for all people – including children and young people.²⁵

4 Scope

The Code's scope should remain broad to ensure that children are protected wherever they are likely to engage online, including on services they may access even where use is formally restricted.

31. The Commission had previously recommended that the Code adopt a broad definition of services that are likely to be accessed by children.²⁶ This is particularly important where children may have access to social media, despite age-restricted social media platforms being required to take reasonable steps to prevent Australians under the age of 16 from creating or keeping an account.
32. Ensuring that the scope is set broadly and that it automatically applies to social media platforms is important. Early research is showing that 27% of 14–15-year-olds continue to have social media.²⁷ This is supported by eSafety's first compliance update which showed that 7 out of 10 parents reported that their child still had an account on Facebook, Instagram, Snapchat and TikTok.²⁸
33. Regardless of who is legally allowed to hold an account on social media, the Code must ensure that even those who retain an account on social media platforms have privacy protections.

Likely to be accessed by children

34. In determining whether children are likely to access an online service, organisations will need clarity on how this threshold is assessed. The Code is currently unclear on this issue. Further guidance would be useful to support consistent and workable application.
35. Rather than relying on a fixed numerical threshold, guidance could adopt a multi-factor, risk-based approach, consistent with the [UK Information Commissioner's Office](#).
36. This approach focuses on whether it is reasonably foreseeable that children will access a service, based on available evidence. Relevant factors may include:
 - the nature and content of the service and its appeal to children
 - how the service is designed and marketed
 - patterns of user behaviour and
 - whether children form a material or identifiable user group.
37. While this approach introduces some flexibility, it is supported by structured factors and evidence – avoiding the rigidity of a strict demographic threshold. Clear guidance on the application of these factors would be important to ensure that the standard remains predictable and enforceable in practice.

5 Evolving capacity

Age-appropriate standards may be more workable to implement in practice, even though they do not fully reflect differences in children's maturity and decision-making capacity.

38. Throughout the Code 'age appropriate' is used as a threshold (e.g. provision of information, notifications, consent etc). While from an implementation perspective it makes sense to set the bar at age appropriate-levels, the principle of the evolving capacity of children should also be considered. As noted by the Special Rapporteur 'children vary enormously in their physical, intellectual, social and emotional capacity'.²⁹
39. The Special Rapporteur cautioned that the 'notion of age-appropriateness sits uneasily with the principle of evolving capacity' and recommended that State parties 'adopt age-appropriate standards as a regulatory instrument only with the greatest of caution when no better means exist'.³⁰
40. Any measures that respond to children must also recognise their differing levels of decision-making ability, based on their maturity and development. A one-size fits all approach for children may not be the most fulsome way to protect their rights.³¹
41. However, overly broad language within the Code may create greater risks than relying on an age-based standard. While recognising the conceptual strengths of 'evolving capacity', it may be challenging to operationalise in a consistent and workable way for business. In this context, age-appropriate standards provide a more practical and implementable approach, even if they do not fully capture the nuance of children's varying capacities. To use evolving capacity as a standard may create a risk of increased data collection by services to determine children's capacity, which is inconsistent with the Code's privacy objectives.
42. Age-appropriate standards operate as a necessary and proportionate measure, provided they are:
 - based on the most up-to-date research on children's evolving capacities and development and
 - complemented by mechanisms that allow children to exercise agency, such as accessible complaint and feedback processes.
43. This should include a staged approach, where features and safeguards evolve over time to reflect children's increasing capacity. For example, affording greater autonomy and control to older adolescents compared to younger children.
44. General Comment No. 25 provides guidance that 'the design of age-appropriate measures should be informed by the best and most up-to-date research available, from a range of disciplines'.³²

Endnotes

- ¹ UN Office of the High Commissioner for Human Rights, *Getting Children's Safety Online Right* (Guidance document, 29 May 2026) 1.
- ² Committee on the Rights of the Child, *General Comment No.14 on the Rights of the Child to have his or her Best Interests taken as a Primary Consideration* (29 May 2013, UN Doc CRC/C/GC/14) 12 [50].
- ³ Committee on the Rights of the Child, *General Comment No.14 on the Rights of the Child to have his or her Best Interests taken as a Primary Consideration* (29 May 2013, UN Doc CRC/C/GC/14) 10 [39].
- ⁴ Committee on the Rights of the Child, *General Comment No. 25 on Children's Rights in relation to the Digital Environment* (02 March 2021, UN Doc CRC/C/GC/25) 16-18.
- ⁵ Joseph Cannataci, *Artificial Intelligence and Privacy, and Children's Privacy* (Report of the Special Rapporteur on the Right to Privacy, 2021, UN Doc A/HRC/46/37) 12 [80].
- ⁶ Joseph Cannataci, *Artificial Intelligence and Privacy, and Children's Privacy* (Report of the Special Rapporteur on the Right to Privacy, 2021, UN Doc A/HRC/46/37) 19 [118].
- ⁷ Convention on the Rights of the Child, *General Comment 4* 12.
- ⁸ UN Office of the High Commissioner for Human Rights, *Getting Children's Safety Online Right* (Guidance document, 29 May 2026) 2.
- ⁹ Joseph Cannataci, *Artificial Intelligence and Privacy, and Children's Privacy* (Report of the Special Rapporteur on the Right to Privacy, 2021, UN Doc A/HRC/46/37) 14 [91].
- ¹⁰ *Privacy (Children's Online Privacy) Code 2026*, ss 11-12.
- ¹¹ Committee on the Rights of the Child, *General Comment No. 25 on Children's Rights in relation to the Digital Environment* (02 March 2021, UN Doc CRC/C/GC/25) 7 [40].
- ¹² Committee on the Rights of the Child, *General Comment No. 25 on Children's Rights in relation to the Digital Environment* (02 March 2021, UN Doc CRC/C/GC/25) 7 [40].
- ¹³ Joseph Cannataci, *Artificial Intelligence and Privacy, and Children's Privacy* (Report of the Special Rapporteur on the Right to Privacy, 2021, UN Doc A/HRC/46/37) 14 [90].
- ¹⁴ Joseph Cannataci, *Artificial Intelligence and Privacy, and Children's Privacy* (Report of the Special Rapporteur on the Right to Privacy, 2021, UN Doc A/HRC/46/37) 14 [92].
- ¹⁵ Committee on the Rights of the Child, *General Comment No. 25 on Children's Rights in relation to the Digital Environment* (02 March 2021, UN Doc CRC/C/GC/25) 7 [41].
- ¹⁶ *Convention on the Rights of the Child*, art 3.
- ¹⁷ UN Office of the High Commissioner for Human Rights, *Getting Children's Safety Online Right* (Guidance document, 29 May 2026) 1.
- ¹⁸ See generally Age Check Certification Scheme, *Age Assurance Technology Trial - Final Report* (Report, 2025); Australian Human Rights Commission, Submission to the *Senate Inquiry into the Internet Search Engine Services Online Safety Code (SES Code) and the Social Media Ban* (Submission, 10 October 2025) 9-15.
- ¹⁹ Australian Human Rights Commission, Submission to the *Senate Inquiry into the Internet Search Engine Services Online Safety Code (SES Code) and the Social Media Ban* (Submission, 10 October 2025) 9-15.
- ²⁰ eSafety, *Social Media Minimum Age Regulatory Guidance* (Regulatory Guidance, September 2025) 12-14.
- ²¹ Lorraine Finlay & Patrick Hooton, 'Fast Law, Fragile Rights: The Human Rights Consequences of Australia's Rapid Social Media Reforms' (2025) 13(1) *Griffith Journal of Law & Human Dignity* 1, 20-21.
- ²² See generally eSafety, *Social Media Minimum Age: Compliance update* (Report, March 2026); Leonardo Bursztyn, et al., *Why Bans Fail: Tipping Points and Australia's Social Media Ban* (Research brief, University of Chicago, 21 May 2026).
- ²³ See generally, Attorney-General's Department, *Government Response Privacy Act Review Report* (Report, 2023).
- ²⁴ The Hon Mark Dreyfus KC MP, Landmark Privacy Act Review report released (Media Release, 16 February 2023).

8.

²⁵ Attorney-General's Department, *Government Response Privacy Act Review Report* (Report, 2023) 8, proposals 12.1-12.3.

²⁶ Australian Human Rights Commission, Submission to the *Office of the Australian on the Children's Online Privacy Code* (Submission, 30 July 2025) 6-7 [10]-[15].

²⁷ Leonardo Bursztyn, et al., *Why Bans Fail: Tipping Points and Australia's Social Media Ban* (Working Paper No 2026-57, April 2026) 1.

²⁸ eSafety, *Social Media Minimum Age* (Compliance update, March 2026) 13.

²⁹ Joseph Cannataci, Report of the Special Rapporteur on the Right to Privacy, *Artificial Intelligence and Privacy, and Children's Privacy* (Human Rights Council, UN Doc A/HRC/46/37, 2021) 96.

³⁰ Joseph Cannataci, Report of the Special Rapporteur on the Right to Privacy, *Artificial Intelligence and Privacy, and Children's Privacy* (Human Rights Council, UN Doc A/HRC/46/37, 2021) 115, 127.

³¹ Australian Human Rights Commission, Submission to the Attorney-General's Department, *Exposure draft of the Privacy Legislation Amendment (Enhancing Online Privacy and Other Measures) Bill 2021 (Cth)* (1 December 2021) our sub 23 [110]

³² Committee on the Rights of the Child, General Comment No. 25 on Children's Rights in relation to the Digital Environment (02 March 2021, UN Doc CRC/C/GC/25) [19].