Law Council
OF AUSTRALIA

Privacy (Children's Online Privacy) Code 2026

Office of the Australian Information Commissioner

7 July 2026

Telephone +61 2 6246 3788
Email mail@lawcouncil.au
PO Box 5350, Braddon ACT 2612
Level 1, MODE3, 24 Lonsdale Street,
Braddon ACT 2612
Law Council of Australia Limited ABN 85 005 260 622
www.lawcouncil.au

Contents

Acknowledgements

The Law Council of Australia thanks:

- the Law Society of New South Wales;
- the Queensland Law Society;
- the Law Society of South Australia;
- the Law Institute of Victoria; and
- the Privacy Law Committee of its Business Law Section

for their contribution to the preparation of this submission.

Introduction

1. The Law Council of Australia welcomes the opportunity to provide feedback to the Office of the Australian Information Commissioner (**OAIC**) about the Exposure Draft of the *Privacy (Children's Online Privacy) Code 2026* (the **Code**) and Exposure Draft Explanatory Statement.

2. The *Privacy and Other Legislation Amendment Act 2024* (Cth) inserted section 26GC into the *Privacy Act 1988* (Cth), requiring the Information Commissioner to develop and register an Australian Privacy Principles (**APP**) code about online privacy for children within 24 months of Royal Assent, being by 10 December 2026. This is consistent with Proposal 16.5 of the Privacy Act Review Report.[1]

3. The Code is to be read as operating alongside an entity's existing obligations under the APPs, the Privacy Guidance on age assurance technologies and the Privacy Guidance on Part 4A (Social Media Minimum Age) of the *Online Safety Act 2021* (Cth).

4. The Code includes new rules that require organisations to ensure that they consider the best interests of children before collecting, using or disclosing their personal information. It is not intended that children's and young people's access to online spaces be restricted or limited as a result of the Code.

5. The Law Council strongly supports the intent of the Code and the positive steps being taken to advance online privacy protections for children consistent with Australia's obligations under Articles 3 and 16 of the Convention on the Rights of the Child.[2]

6. However, the Law Council maintains reservations about how the Code, in its current form and without further guidance, can be adequately implemented. We are particularly concerned about the extent to which the Code sufficiently clarifies obligations for the private entities that will be bound by it, and the potential for the Code to capture a wide range of industries or sectors that may already be subject to significant regulation. The regulatory burdens to be imposed by the Code should be proportionate to the risk they are seeking to mitigate; if this is not correctly calibrated, providers of some services may withdraw from the market and not provide services to young people.

7. Given the obligations the Code imposes, and the consequences of non-compliance (including inadvertent non-compliance), the Law Council's primary recommendation is that the necessary clarifications be made within the text of the Code itself. Supporting guidance and other materials have an important role in assisting entities to comply, but they should supplement, rather than substitute for, clear drafting of the operative obligations.

---

1 Australian Government Attorney-General's Department, *Privacy Act Review* (Report, 2022) 157.

2 *Convention on the Rights of the Child*, opened for signature 20 November 1989, 1577 UNTS 3 (entered into force 2 September 1990) ('CRC').

8. This submission builds on the Law Council's earlier submissions, in particular its submission of 8 August 2025 on the *Children's Online Privacy Code: Issues Paper*,[3] and its submission of October 2024 to the Senate Legal and Constitutional Affairs Legislation Committee on the Privacy and Other Legislation Amendment Bill 2024.[4]

9. The Law Council's comments are directed to strengthening the draft Code so that the entities bound by it can understand and implement their obligations in practice, while delivering meaningful protections for children.

Overarching Comments

Best interests of the child

10. Consistent with our previous submission, the Law Council supports the Code's incorporation of the best interests of the child.[5] However, we note the inherent tension in any protective regime and the risk, if not carefully calibrated, that the regime may undermine children's autonomy and their other rights under the Convention on the Rights of the Child.[6] To the extent possible, privacy protective measures should respect the evolving capacities of children, affording older children progressively greater autonomy.

11. The concept of "best interests of the child" is not defined in the text of the Code, and neither the Code nor the Explanatory Statement specify what weight is to be given to the child's own views when ascertaining what is in a child's best interests. The Explanatory Statement does provide a list of example factors an entity should consider when assessing the best interests of the child,[7] but it does not ascribe what weight should be given to each factor, or how these factors should be reconciled with the views of the child, and competing considerations such as safety and autonomy.

12. The consequence of the current framing is illustrated by subsection 11(1), for example, where an entity must not use or disclose a child's personal information unless the child consents *and* the use or disclosure is consistent with the child's best interests. This places the entity in judgment over the expressed wishes of a child old enough to consent under section 13. While we accept that consent alone may be an insufficient safeguard for many children,[8] a best-interests test applied without reference to the child's views risks operating as a vehicle for paternalism rather than protection.

13. Furthermore, unlike judicial decision-making or decisions of government agencies, asking businesses to make a determination about what is in the best interests of a child raises a number of difficulties. We consider that it would be more appropriate

---

3 Law Council of Australia, *Children's Online Privacy Code: Issues Paper* (Submission, 8 August 2025).
4 Law Council of Australia, *Privacy and Other Legislation Amendment Bill 2024* (Submission, 22 October 2024).
5 See Law Council of Australia, *Children's Online Privacy Code: Issues Paper* (Submission, 8 August 2025) [10], [15].
6 Such as the rights to be heard, to access and impart information, and to a sphere of privacy of their own, free from excessive surveillance by others; see CRC Art 12, 13, 16 and 17.
7 Draft Explanatory Statement Exposure Draft Children's Online Privacy Code 9 ('Explanatory Statement').
8 See Law Council of Australia, *Children's Online Privacy Code: Issues Paper* (Submission, 8 August 2025) [66], [79]–[82].

for privacy compliance to be approached more akin to product safety, with clear guardrails, rather than leaving it to entities to decide what is in the best interests of their consumers and particularly children.

14. The importance of supporting organisations to undertake the best-interests assessment is illustrated by international commentary, which has highlighted a lack of guidance on how organisations can and should assess the full spectrum of child rights as new technologies emerge in the digital environment.[9] As part of its Children's Best Interests in a Digital World Project, UNICEF's working paper identifies that "while upholding the best interests of the child principle is increasingly found in policies and regulations in relation to the digital environment, there is little guidance on how to implement this in practice".[10]

15. We also note that, in April 2026, UNICEF published its 'Children's Best Interests in Digital Policy and Practice' report, which articulated the distinct responsibilities between Government and organisations in relation to the assessment of the best interests of a child with key recommendations including:

> *Governments should retain primary responsibility for assessing, determining and upholding the Principle through legislation, regulatory guidance, oversight and enforcement mechanisms. They should establish—or assign responsibility to existing—oversight or regulatory bodies to assess and determine children's best interests, offering a framework for how to do this …*
>
> *Technology companies should align their practices with applicable guidance and legal standards rather than defining the Principle unilaterally …*[11]

16. Accordingly, the Law Council recommends that the concept of "best interests of the child" is defined in the body of the Code, and that the OAIC consider whether framing the concept by reference to a set of minimum expectations of what factors should be considered may assist with compliance including taking into account the views and evolving capacities of a child. Additional supporting guidance should also be developed to articulate the matters relevant to a best-interests assessment to enable the "best-interests test" to be applied in business decision-making.

Education technologies and artificial intelligence

17. The Code is clearly directed to commercial entities collecting information in a business context. It may be necessary to tailor the Code to ensure that it appropriately engages with the operations of some organisations, such as schools, where particular and discrete issues may arise. We acknowledge this may be beyond the scope of the Code, and may require amendment to the Privacy Act itself.

18. We note that digital technologies are increasingly being used in the education sector and that artificial intelligence (**AI**) and data brokering within educational technology and other online service platforms presents heightened privacy risks and online

---

9 See e.g. Orissa Erwin-Rose, Hannah Darnton and Ife Ogunleye, BSR, *Global Guidance for Child Rights Impact Assessments in Relation to the Digital Environment* (Report, 2025) 4

10 UNICEF Office of Strategy and Evidence—Innocenti, 'The Evolving Digital Landscape and Best Interests of the Child', UNICEF (Web Page, 16 January 2026)

11 Bella Baghdasaryan and Steven Vosloo, UNICEF, *Children's Best Interests in Digital Policy and Practice*, (UNICEF Report, April 2026) 70.

harms for children. We recommend that the OAIC provide stronger guidance to support schools and families to navigate these technologies, to make better informed decisions and to support the provision of meaningful consent.

19. Further, the Code should require clear, age-appropriate disclosure where personal information about a child is used to train, fine-tune, personalise, profile, evaluate or otherwise materially inform the operation of an AI system, including a generative AI chatbot, particularly where that use may affect the child's rights, interests, choices, safety or online experience.

Personal information about a child

20. The Code's use of "personal information about a child" reflects the language in the definition of "personal information" at subsection 6(1) of the Privacy Act. However, we note there are ambiguities in relation to the definition of "personal information" including whether technical information such as metadata is "information about an individual".[12] This uncertainty is particularly relevant in the context of children's online services, where practices such as profiling and targeted advertising frequently involve technical and inferred information; to the extent that such information falls outside the definition, it falls outside the protections of the Code.

21. Proposals 4.1 and 4.2 of the 2022 Privacy Act Review recommended changing the word "about" in the definition of personal information to "relates to",[13] and the addition of a non-exhaustive list of information that may be considered personal information.[14] We note that the Australian Government agreed to these proposals in principle,[15] but that the amendments remain unlegislated. The Law Council acknowledges that this issue cannot be remedied within the Code itself, and we reiterate previous calls for a roadmap for the remaining tranches of privacy reform.[16]

Specific Feedback

Part 2: Entities and activities to which the Code applies

Breadth of activities captured

22. Under paragraph 26GC(5)(a) of the Privacy Act, an APP entity is bound by the Code where the entity is the provider of a social media service, relevant electronic service or designated internet service[17] (and is not a health service) and the service being provided by the entity is "likely to be accessed by children".

23. Additional entities, or a class of entities, may be specified pursuant to paragraph 26GC(5)(b) of the Privacy Act, with section 5 of the Code specifying that

---

12 See *Privacy Commissioner* v *Telstra Corporation Limited* (2017) 249 FCR 24.
13 Australian Government Attorney-General's Department, *Privacy Act Review* (Report, 2022) 25–27.
14 Ibid 28–29.
15 Australian Government, *Government Response: Privacy Act Review Report* (September 2023) 5.
16 See Law Council of Australia, *Children's Online Privacy Code: Issues Paper* (Submission, 8 August 2025) 10 [34]; Law Council of Australia, Privacy and Other Legislation Amendment Bill 2024 (Submission, 22 October 2024) 17 [22].
17 Within the meaning of the *Online Safety Act 2021* (Cth).

the Code applies to a provider of a relevant service,[18] where the service is "primarily concerned with the activities" of children.[19] Note 1 to that section provides examples of these kinds of services as including applications that track early childhood development, family photo sharing applications, online school management systems that monitor student performance, and internet-connected baby monitors.[20]

24. Section 7 of the Code specifies the activities of an entity to which the Code applies, namely a social media service, relevant electronic service, or a designated internet service that is likely to be accessed by children or primarily concerned with the activities of children.[21]

25. The framing of the Code is such that it will apply to all APP entities providing services that are either "*likely* to be accessed by children" or "*primarily* concerned with the activities of children". This will capture a broad range of entities and their relevant activities with the view to maximising the protection of children's personal information.

26. We acknowledge the benefits of the intended breadth of application of the Code. However, we note potential negative consequences of broad application through additional regulatory burden for entities that are not high risk, and the possibility that entities may limit their services in the absence of greater clarity as to whether or not the Code applies.

27. Presently, there is insufficient guidance in the Code to support businesses and organisations to determine whether the Code applies to particular business activities. As noted in our previous submission,[22] while this may be easy to ascertain for some activities, it will be less clear for others, and the broad nature of the framing of the Code is also likely to capture entities that did not expect to come under the Code. Furthermore, these provisions have the effect that the Code may apply to some activities of an organisation and not to others, which may create complexity.

28. We further note there may be challenges in identification of the "provider" of services and queries have been raised as to whether the "provider" is who uses the platform to collect personal information or if it is who licences the platform for use by a third party.

29. We therefore recommend that, and consistent with our previous submission,[23] the Code should include a non-exhaustive list of factors relevant to determining whether a service is "likely to be accessed by children", drawing on the factors identified in the Explanatory Memorandum to the Privacy and Other Legislation Amendment Bill 2024,[24] together with equivalent guidance on the meaning of "primarily concerned with the activities of children". In this regard, the Code should incorporate some

---

[18] Being a social media service, relevant electronic service or designated internet service, and excluding health services.

[19] Noting section 6 of the Code specifies the entities that are not bound by the Code, which are currently carriage service providers within the meaning of the *Telecommunications Act 1997* (Cth).

[20] See Exposure Draft Privacy (Children's Online Privacy) Code (Cth) s 7 Note 1 ('Code').

[21] Ibid s 7.

[22] Law Council of Australia, *Children's Online Privacy Code: Issues Paper* (Submission, 8 August 2025) 13 [56].

[23] Ibid [56]–[57].

[24] Explanatory Memorandum, Privacy and Other Legislation Amendment Bill 2024 (Cth) [85].

threshold for when services are likely to be accessed by children, noting for the most part they will be broadly available to the public.

30. We further recommend that the commencement date of the Code be set to allow an adequate transition period following registration. In this regard, we note the transition period for the United Kingdom's Age Appropriate Design Code was twelve months. The Law Council has received feedback that twelve months would be insufficient time for implementation, particularly if further guidance still needs to be developed. There should be an extended period before commencement.

Application to small business

31. As observed earlier in this submission, many of the recommendations from the Privacy Act Review have not yet been progressed. These include the removal of the small business exemption (Proposal 6.1),[25] that the Government agreed in-principle.[26]

32. At present, a small business operator is generally not an APP entity (and therefore not bound generally by the Code) because the definition of "organisation" in section 6C of the Privacy Act excludes small business operators as defined in section 6D. We note, however, that section 6D contains exceptions under which a small business operator is nonetheless treated as an organisation, including where the operator trades in personal information. The OAIC may wish to consider whether, and on what basis, the Code may apply to small business operators that fall within an existing exception.

33. To inform the potential application of the draft Code at a future date, it would be useful for the OAIC to ascertain relative information about the extent to which Australian small business operators collect, use and disclose children's personal information, proportionately to entities that would be bound by the Code. Such information would best inform the appropriateness of extending the Code to small business operators, and any impact assessments.

Tiered obligations according to risk

34. Feedback to the Law Council has suggested that consideration should be given to a tiered approach to obligations under the Code, noting that under the current framework, all services are treated equally regardless of potential risk factors. Noting the potentially broad scope of the Code, we query whether it is appropriate for all obligations to apply equally, or whether certain obligations can be tiered according to risk to online privacy for children.

---

[25] Australian Government Attorney-General's Department, *Privacy Act Review* (Report, 2022) 62.
[26] Australian Government, *Government Response: Privacy Act Review Report* (September 2023) 6.

Part 3, Division 1—General requirements

Section 8: Age ascertainment

35. Section 8 of the Code provides that, before an entity collects personal information, the entity must take steps, that are reasonable in the circumstances, to ascertain the age of the end-user including the collection of personal information necessary to ascertain the end-user's age.

36. The Law Council supports the inclusion of a risk-based age-ascertainment obligation, and welcomes subsection 8(5), which relieves an entity of that obligation where it elects to apply the Code's protections to all end-users regardless of age. This gives effect to our previous recommendation that, where age cannot reasonably be determined, the Code's protections should be capable of being applied to all users.[27]

37. The Law Council notes that, as currently drafted, subsection 8(1) requires entities to take reasonable steps to ascertain the age of *every* end-user, regardless of whether the end-user is likely to be an adult or a child. We query whether age ascertainment of every user is necessary, noting that that this tension stems from the Code's inherent principle of data collection minimisation, and the collection of personal information from children and adults, that would not have otherwise been collected, to ascertain age.[28]

38. We acknowledge subsections 8(3) and 8(4) may mitigate privacy risks by requiring an entity to only collect information to the extent that is necessary to comply with subsection 8(1), and sensitive information must be destroyed as soon as practicable after age has been ascertained (subject to only two exceptions). Nevertheless, there are concerns that, irrespective of this destruction requirement, there is risk that an entity may collect and retain personal information of an end-user indefinitely, whether due to ineffective internal operational policies or disregard (or ignorance) of requirements under the Code. Furthermore, those safeguards do not extend to non-sensitive personal information collected for the purposes of age ascertainment.

39. We therefore suggest that there be consideration as to whether section 8 should apply where activities are primarily concerned with the activities of children, where they are not likely to be accessed by children. We further recommend that section 8 reiterate where information must be collected for the purposes of ascertaining an end-user's age, that the entity collect the minimal personal information required for age assurance: for example, by reference to APP 3.2.

---

[27] Law Council of Australia, *Children's Online Privacy Code: Issues Paper* (Submission, 8 August 2025) 18 [84].

[28] Code (n 20) s 9. See also Explanatory Statement (n 7) 9.

Section 9: Only if strictly necessary

40. Subsection 9(1) of the Code states:

> *An entity must implement technical and organisational measures that ensure that, by default, the entity only collects, uses or discloses personal information about a child that is strictly necessary to provide the entity's service.*

41. As previously submitted, the Law Council broadly supports high privacy defaults for children and considers that it would be in the best interests of a child for the strictest privacy settings to be set as the default.[29] This shifts the onus for privacy protection to the entity providing the service, noting the challenges in determining whether a child is capable of providing meaningful consent. We therefore welcome the requirement under section 9 for privacy settings to be automatically set to "high privacy by default".[30]

42. However, we note that section 9 introduces a "strictly necessary" threshold that does not appear in existing privacy legislation. The Explanatory Statement notes that the 'strictly necessary' test establishes a narrower and more protective threshold than 'reasonably necessary'.[31] It explains that section 9 is directed to the default design of a service, and that it does not displace APP 3.1 and 3.2, under which an entity may still collect a child's personal information that is reasonably necessary for one of its functions or activities.[32] We observe that this test is a separate notion to the "best interests of the child" requirements for collection,[33] and use or disclosure,[34] of personal information about a child.

43. The relationship between the 'strictly necessary' and 'reasonably necessary' thresholds and the best-interests requirements are likely to be a source of uncertainty for entities seeking to comply with the Code. The Explanatory Statement provides some assistance, including the example of an online messaging service for which account creation is strictly necessary but personalised recommendations, targeted advertising and service improvements are not.[35] The Law Council recommends that such examples be expanded and incorporated into the Code or formal guidance, so that entities can determine with confidence how the "strictly necessary" default operates alongside the "reasonably necessary" standard and the best interests requirements.

44. Separately we observe that the Code variously uses the words "control", "enable", "consent" and "assent" to describe different actions that may be taken by a child or a person with parental responsibility, in relation to the handling of personal information about a child. The relationship between these terms is not clearly articulated, and this is likely to cause uncertainty for both children using a service and the entities concerned. As discussed below in relation to Division 2, we suggest further clarity from the OAIC would assist in understanding the various trigger points for when

---

29 Law Council of Australia, *Children's Online Privacy Code: Issues Paper* (Submission, 8 August 2025) 14 [59].
30 Explanatory Statement (n 7) 9.
31 Ibid 8.
32 Ibid 7–8.
33 Code (n 20) s 10.
34 Code (n 20) s 11.
35 Explanatory Statement (n 7) 8.

consent, assent or enabling of a control is required in relation to the collection, use or disclosure of a child's personal information.

Part 3, Division 2—Consent

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

45. We note that the Code has determined, for the purpose of section 13(1), that 15 years is the age threshold for a child to be able to give consent on their own behalf to the collection, use or disclosure of personal information about them. We acknowledge that the Explanatory Statement explains that the age of 15 "has been included to align with the OAIC's current guidance on children's presumed age of consent for the handling of their personal information", and was selected following "consideration of the research on child brain development and adolescent decision-making, as well as the types of decisions made under the Act and likely consequences of those decisions".[36]

46. However, we note that the guidance in Chapter B of the APP Guidelines, treats the age of 15 as a rebuttable presumption as to capacity to consent,[37] which is in contrast to the strict age requirements proposed under the Code. This means there is no ability under the Code to consider a child's individual capacity to consent and contributes to the tension between protecting a child's privacy and undermining their autonomy and other rights.

47. We also note that the age threshold is different across various legislative regimes and the Law Council has previously submitted that development of the Code represented an opportunity for alignment with the Online Safety Act in considering age thresholds and capacity to consent in relation to the age-restricted social media ban.[38] While we are not necessarily advocating for an increase in the age requirements to 16, from an implementation point of view, the varying age triggers across different legislative frameworks arguably create unnecessary complexity. To the extent possible, we recommend there should be consistency in relation to age thresholds or specific guidance on the interaction across regimes.

48. Subsection 13(3) provides that where, after a person with parental responsibility for the child provides consent, an entity must "provide an age appropriate notice to the child". Should this requirement progress, we suggest the OAIC provides further guidance on how the entity may deliver that notice to the child (e.g. how the entity might reasonably know the notice is being received by the child user and not the person with parental responsibility).

49. The Law Council welcomes the proposed carve out under subsection 13(4) for children seeking legal or health-related information. However, we recommend that these carve outs should not be restricted only to "legal or health related information or support *in connection with a person with parental responsibility for the child*" (emphasis added).[39] In our view, children should have the ability to seek information

---

36 Explanatory Statement (n 7) 12.
37 OAIC, *Australian Privacy Principles Guidelines* (Guidelines, combined May 2026) 12 [B.59]–[B.61].
38 Law Council of Australia, *Children's Online Privacy Code: Issues Paper* (Submission, 8 August 2025) 14 [69].
39 Code (n 20) s 4(a).

in relation to any legal issue, and this should not be constrained by requiring a connection to a person with parental responsibility.

50. From an access to justice perspective, there may be circumstances where a child may wish to understand their legal rights without the knowledge or involvement of their parents, and a legal service may need to collect the child's personal information to provide that advice. These children may access the website or online chat service of legal assistance providers (such as Youth Law Australia) for this purpose, and may need to provide personal information to access advice and assistance under these services.

Section 17: Withdrawal of consent

51. Subsection 17(1) states that "an individual who has given consent to the collection, use or disclosure of personal information about a child may, at any time, withdraw the consent". There may be circumstances in which a person with parental responsibility has provided consent for a child under 15 (pursuant to section 13), however the child themselves may wish to withdraw consent (while they remain under the age of 15 or at a later time).

52. However, in this situation the framing of the text as "individual who has given consent" appears to preclude the child from being able to subsequently withdraw consent. This is also difficult to reconcile with the obligations under paragraph 13(3)(e) for an entity to provide an age-appropriate notice to a child, where a person with parental responsibility has consented to the collection, use or disclosure of their personal information, as the notice must include information on the child's right to withdraw consent at any time. We recommend that the OAIC resolves this inconsistency.

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

53. Section 20 requires that, when a child under the age of 15 enables an entity to collect, use or disclose certain personal information,[40] the entity must seek the child's assent to that collection, use or disclosure, and the entity must contact a person with parental responsibility for the child for the purposes of obtaining their consent to that collection, use or disclosure.

54. The Explanatory Statement explains that, if the child does not assent and/or does not assent to a person with parental responsibility being contacted to provide consent, then the entity must not proceed with the collection of that information for that purpose.[41] However, as currently drafted, the text of the Code itself does not specify the consequence of the child's non-assent. We suggest that the Code explicitly prohibits the entity from performing the activities under paragraph 20(1)(b) where the child does not assent.

---

[40] Specified at Code (n 20) s 20(1)(b) as sensitive information, use or disclosure of personal information for a purpose other than the purposed it was originally collected, or for the purpose of direct marketing.

[41] Explanatory Statement (n 7) 16

55. The Law Council notes that, unlike subsection 13(4), section 20 does not provide a carve out from notifying a person with parental responsibility when section 20 is triggered, when a child is seeking legal or health-related information. From a practical perspective this may be moot, and it may be implicit that a child under the age of 15 would not need to assent pursuant to subsection 20(2) where they have provided consent under subsection 13(4). However, this is not explicit on the face of section 20.

56. We further suggest that there is clarification about the interaction between section 8 and section 20 of the Code. Under section 8, an entity may collect personal information for the purposes of age ascertainment. The question arises as to whether paragraph 20(1)(b)(i) is triggered if an entity seeks sensitive information about a child under 15 for this purpose. While we consider that section 20 is unlikely to apply to sensitive information collected for the purposes of age ascertainment, and noting the requirement under subsection 8(4) to destroy sensitive personal information collected for this purpose, we recommend that this is clarified explicitly in the Code or Explanatory Statement.

Section 21: Consent by coercion

57. Section 21 of the Code provides that, in complying with APP 3.5, an entity does not collect personal information about a child through lawful and fair means if the entity seeks consent to the collection, use or disclosure of information in a way that coerces or manipulates the individual or substantially impedes the ability of the individual to decide whether to consent to the collection of the information.

58. The Explanatory Statement explains that this section is closely tied to voluntary consent and will preclude entities from seeking consent through design practices such as nudge techniques that are designed to compel an individual to consent to handling of more personal information than they would otherwise agree to.[42]

59. We understand that the Competition and Consumer Amendment (Unfair Trading Practices) Bill 2026 (**Unfair Trading Practices Bill**)[43] proposes to amend the Australian Consumer Law (**ACL**) including by introducing a general prohibition on conduct that unreasonably manipulates consumers or distorts the environment they make decisions in, causing detriment.[44]

60. While there will be many occasions in which only the Code would apply while the protections under the ACL (if amended) would not be triggered (or vice versa), the Law Council cautions that there is potential for overlap. This creates the potential for dual regulation and divergent tests. Accordingly, the OAIC may wish to consider and provide guidance on how section 21 is intended to operate, and interact with, the ACL should the Unfair Trading Practices Bill pass, in addition to the general sequencing concerns should tranche 2 of the privacy review reforms progress.

---

42 Explanatory Statement (n 7) 16.

43 Competition and Consumer Amendment (Unfair Trading Practices) Bill 2026 (**Unfair Trading Practices Bill**)

44 Ibid, Unfair Trading Practices Bill s 28B(1). See Unfair Trading Practices Bill s 28B(6) which sets out examples of such contraventions.

Part 3, Division 3—Transparency

Section 23: APP privacy policy requirements

61. Section 23 of the Code requires an entity whose service is likely to be accessed by children to have "a version of the entity's APP privacy policy that is directed specifically at children".

62. We note that the Explanatory Statement provides that an entity may choose to meet the obligation in section 23 by providing a separate child-friendly version of their main privacy policy or by producing a single privacy policy that is written in clear, simple and accessible language so it can be understood by both children and adults.[45] We suggest that guidance material is provided setting out an example of a privacy policy that has been "translated" for children, including example "icons, images, diagrams, animations or short videos"[46] to help set expectations for the relevant entities.

63. The Law Council has received feedback that entities may be reluctant to have multiple privacy policies for the different countries they operate in, preferring to have policies that, for example, satisfy both the APPs and the European Union's General Data Protection Regulation—and, potentially in light of section 23, policies that are appropriate for both adults and children. However, for entities such as these, there will need to be a period in which they reconcile their existing privacy policy with the requirements of the Code and this should be taken into account when considering an appropriate commencement date for the Code.

Section 24: Notification requirements

64. The Law Council welcomes the clarity requirements for notifications under section 24 of the Code, particularly the capacity to use non-text materials (where appropriate).[47] Developing this material for children requires significant consideration and stakeholder engagement to ensure the material is age-appropriate and capable of being understood. We commend the extensive consultation with children and young people, as well as their parents and carers, already undertaken by the OAIC, and strongly encourage ongoing consultation in the development of additional guidance materials.

65. However, we reiterate previously expressed concerns[48] that, irrespective of the format of a notification (and despite the obligations under paragraph 24(2)(c)), many children are still likely to have a limited understanding of the seriousness of the collection of their personal information. This emphasises the importance of the structural safeguards within the Code[49] to prioritise high privacy by default to reduce reliance on the comprehension and consent of children.

---

45 Explanatory Statement (n 7) 17.
46 Ibid.
47 Code (n 20) s 24(2)(d).
48 Law Council of Australia, *Children's Online Privacy Code: Issues Paper* (Submission, 8 August 2025) 17 [79]–[82].
49 See e.g. Code (n 20) ss 9-11.

Section 29: Opting out of direct marketing

66. The Law Council has previously asserted that the default position should be that children's personal information should not be used or disclosed for targeted marketing purposes, subject to specific exceptions where it would be in the child's best interests.[50]

67. We recommend that section 29 be strengthened to require that direct marketing communications to children be off by default. Any opt-in should be specific, informed, time-limited, age-appropriate and available only where the proposed use or disclosure is consistent with the child's best interests. Separate consideration should be given to equivalent default-off protections for non-essential cookies and behavioural advertising technologies.

Part 3, Division 4—Access to, and correction of, personal information about children

Sections 30 and 31: Requests for access to, or correction of, personal information

68. Sections 30 and 31 of the Code specify the timeframes in which an entity (that is an organisation) must respond if a child requests access to personal information, or makes a request to correct personal information.

69. The Law Council notes that, in contrast to section 20, the Code and Explanatory Statement are silent as to whether, and in what circumstances, a person with parental responsibility should be notified of, or involved in, an access or correction request of a person under the age of 15. As with our feedback on section 13(4) and section 20, if a person with parental responsibility is to be notified of a request by a child under the age of 15, consideration should be given to appropriate carve outs.

Part 3, Division 5—Destruction of personal information about children

Section 32: Request to destroy personal information about a child

70. Section 32 of the Children's Online Privacy Code provides that entities must destroy specified personal information about a child upon request by the child or a person with parental responsibility for the child, subject to specific exceptions. This contrasts with APP 11.2, which requires an entity to take "such steps as are reasonable in the circumstances to destroy information or to ensure that the information is de-identified" where the entity considers it no longer needs the information.

71. As noted in the Explanatory Statement,[51] section 32 exceeds the current requirements under APP 11.2 as it would impose a strict obligation for the erasure of data (subject to specific exemptions in section 32(3)), irrespective of the reasonableness of the steps necessary to destroy the data,[52] with de-identification

---

[50] Law Council of Australia, *Children's Online Privacy Code: Issues Paper* (Submission, 8 August 2025) 22 [112].

[51] Explanatory Statement (above n 7) 21.

[52] Noting the Code does not provide guidance on what is technically required for the purposes of "destruction".

insufficient to satisfy this new requirement.[53] We understand from a practical perspective the current framing of section 32 is likely to be challenging for entities, as true deletion can be difficult to achieve in some instances (such as across backups or shared systems).

72. We note the Government has agreed in principle to proposals 18.3 and 18.6 of the Privacy Act Review Report,[54] which proposed introducing a right to erasure for all individuals, subject to exceptions,[55] including where compliance would be technically impossible or unreasonable.[56] While the Report noted that such exceptions would need to be carefully drafted to prevent exploitation by organisations seeking to avoid their obligations,[57] in its current form, section 32 has the potential to impose obligations on entities that may be unduly burdensome, or practically impossible to implement. Entities may contravene the section despite undertaking genuine reasonable steps to erase data, where it does not result in the actual destruction of all data.

73. We further note that, in 2025, the Productivity Commission queried the underlying assumptions of the Privacy Act Review Report proposals in relation to a right to erasure, raising concerns in particular about the practicalities and costs of implementation.[58] We note that this analysis was directed at a general right to erasure for all individuals in relation to all personal information, rather than the narrower question of whether individuals should retain the right to request destruction of personal information collected about them during their childhood.

74. The Law Council suggests that section 32 be amended to include a technical reasonableness test: such as where it would be technically impossible, or require disproportionate effort, to destroy the data, or that consideration be given to defining within the Code what is meant by and required for the purposes of "destruction". We also recommend that there be more explicit consideration and guidance about destruction requests made by a child to platforms where the parent is the account holder, as such requests are likely to result in unintended consequences.

75. While mindful of imposing excessive additional burdens on entities, we observe that section 32 is silent about an entity's obligations where personal information of a child has been shared with a third party. We note proposal 18.3 of the Privacy Act Review Report indicated that where an APP entity had collected information from, or disclosed information to, a third party, the right to erasure should require the entity to inform the individual about the third party and notify the third party of the erasure request (unless it was impossible or involved disproportionate effort).[59] The Law

---

53 Explanatory Statement (above n 7) 21, which notes increasing challenges of deidentification of personal information, particularly risks of re-identification.

54 Australian Government, *Government Response – Privacy Act Review Report* (September 2023) 31.

55 Australian Government Attorney-General's Department, *Privacy Act Review* (Report, 2022) 176, Proposal 18.3.

56 Ibid 182, Proposal 18.6, including further exceptions for competing public interests and relationships with a legal character.

57 Ibid.

58 Australian Government Productivity Commission, *Harnessing Data and Digital Technology* (Report 2025) 178–180.

59 Australian Government Attorney-General's Department, *Privacy Act Review* (Report, 2022) 176. Proposal 18.3(b).

Council therefore recommends that Section 32 be extended to include these obligations.

76. We further note that the right to request the destruction of data, as currently drafted, would only be available to individuals who are children at the time of the request. This means that individuals whose data was collected when they were a child, but subsequently turn 18 without having made a request, will no longer have the opportunity to request the erasure of their data, when the same policy rationale for enabling children to request the erasure of their data continues to exist despite that child turning 18.

77. Personal information collected about a child online may persist indefinitely and continue to be used or disclosed by entities long after the child reaches adulthood. An individual's ability to make an informed and autonomous decision about their childhood data footprint is likely to be enhanced upon reaching adulthood, when they more fully appreciate the risks and long-term implications of data collection.

78. Accordingly, the Law Council recommends that consideration be given to extending the right to request destruction to any individual, regardless of their current age, in relation to personal information that was collected about them while they were a child and is still held by an entity.[60]

79. Finally, we note that, unlike the other age thresholds in the Code, subsection 32(1) includes the additional category of a child who is over the age of 15, "but lacks capacity to make the request".[61] While recognising the protective intent of this provision, it is inconsistent with the approach to age and capacity throughout the rest of the Code. It further raises questions in relation to implementation as to the definition of capacity, who is responsible for assessing capacity and the evidence required for such purposes, which is also likely to be contrary to the data minimisation principles.

Part 3, Division 8—Privacy impact assessments and privacy education and training

Section 39: Privacy impact assessments

80. The Law Council welcomes the privacy impact assessment requirements under section 38 of the Code for new or significantly changed services. However, we note that section 39 only refers to an entity maintaining a register of the privacy impact assessments it undertakes, which may extend beyond those undertaken for the purposes of the Code. While the Law Council welcomes transparency, there is a risk of scope creep beyond the remit of the Code. Therefore, we recommend that section 39(1) is clarified with an insertion such as "An entity must maintain a register of the privacy impact assessments that it conducts *[under section 38 of this Code]*".

---

[60] See also Law Council of Australia, *Children's Online Privacy Code: Issues Paper* (Submission, 8 August 2025) 24 [124].

[61] Code (n 20) s 32(1)(c).

Typographical errors

81. We note the following typographical errors in the draft Code:

(a) in section 4, the *Note* refers to "(b) personal information" and "(c) sensitive information", this should be referenced as "(d) personal information" and "(e) sensitive information";

(b) the word "reasonably" appears in the headings section 10 and 11 in the Explanatory Statement,[62] but does not appear in the text of the Code itself;

(c) in subsection 11(6), the numbering for subparagraph 11(6)(ii) should be 11(6)(b);

(d) in subsection 15(4), the reference to subparagraph 3(b) should be a reference to paragraph 3(c);

(e) in subsection 18(2), both subparagraphs are labelled subparagraph 18(2)(a);

(f) in subsection 20(4), both subparagraphs are labelled subparagraph 20(4)(a);

(g) in subsection 20(6), the reference to subparagraph 5(b)(ii) should be a reference to subparagraph 5(b)(iii); and

(h) in subsection 29(4), the numbering for subparagraph 29(4)(ii) should be 29(4)(b).

[62] Explanatory Statement (n 7) 9–10.

About the Law Council of Australia

The Law Council of Australia represents the legal profession at the national level; speaks on behalf of its constituent bodies on federal, national, and international issues; promotes and defends the rule of law; and promotes the administration of justice, access to justice, and general improvement of the law.

The Law Council advises governments, courts, and federal agencies on ways in which the law and the justice system can be improved for the benefit of the community. The Law Council also represents the Australian legal profession overseas, and maintains close relationships with legal professional bodies throughout the world. The Law Council was established in 1933, and represents its constituent bodies:

- the Australian Capital Territory Bar Association;
- the Law Society of the Australian Capital Territory;
- the New South Wales Bar Association;
- the Law Society of New South Wales;
- the Northern Territory Bar Association;
- the Law Society Northern Territory;
- the Bar Association of Queensland;
- the Queensland Law Society
- the South Australian Bar Association;
- the Law Society of South Australia;
- the Tasmanian Bar;
- the Law Society of Tasmania;
- the Victorian Bar Incorporated;
- the Law Institute of Victoria;
- the Western Australian Bar Association;
- the Law Society of Western Australia; and
- Law Firms Australia.

Through these bodies, the Law Council represents more than 110,000 Australian lawyers.

The Law Council is governed by a board of 23 Directors: one from each of the constituent bodies, and six Executive members elected by Directors. The Directors meet quarterly to set objectives, policy, and priorities for the Law Council. Between Directors' meetings, responsibility for the policies and governance of the Law Council is exercised by the Executive members, led by the President. In 2026, the Law Council Executive comprises:

The Chief Executive Officer of the Law Council is 

The Law Council's Secretariat is based in Canberra. Its website is www.lawcouncil.au.