Law Council
OF AUSTRALIA

Office of the President

8 August 2025

Ms Elizabeth Tydd
Australian Information Commissioner
Office of the Australian Information Commissioner
GPO Box 5288
SYDNEY NSW 2001

By email: copc@oaic.gov.au

Dear Commissioner

Children's Online Privacy Code: Issues Paper

The Law Council is grateful for the opportunity to provide a submission to the Office of the Australian Information Commissioner (**OAIC**) in response to its Issues Paper on the Children's Online Privacy Code.

Please find our submission enclosed, informed by contributions from the Law Society of New South Wales, the Queensland Law Society, and the Business Law Section's Privacy Law Committee.

If the Law Council can be of any further assistance to the OAIC, please contact [redacted] in the first instance.

Yours sincerely

[redacted]

[redacted]

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

Law Council
OF AUSTRALIA

Children's Online Privacy Code: Issues Paper

Office of the Australian Information Commissioner

8 August 2025

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

Table of contents

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: 16 Australian State and Territory law societies and bar associations, and Law Firms Australia. The Law Council's Constituent Bodies are:

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

Through this representation, the Law Council acts on behalf of more than 107,000 Australian lawyers.

The Law Council is governed by a Board of 23 Directors: one from each of the Constituent Bodies, and six elected Executive members. 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 who normally serves a one-year term. The Board of Directors elects the Executive members.

The members of the Law Council Executive for 2025 are:

- Ms Juliana Warner, President
- Ms Tania Wolff, President-elect
- Ms Elizabeth Shearer, Treasurer
- Mr Lachlan Molesworth, Executive Member
- Mr Justin Stewart-Rattray, Executive Member
- Mr Ante Golem, Executive Member

The Chief Executive Officer of the Law Council is Dr James Popple. The Secretariat serves the Law Council nationally and is based in Canberra.

The Law Council's website is www.lawcouncil.au.

Acknowledgements

The Law Council acknowledges the contributions of the Law Society of New South Wales and Queensland Law Society in the preparation of this submission, in addition to the contributions of the Business Law Section's Privacy Law Committee.

Introduction

1. The Law Council of Australia appreciates the opportunity to respond to the Issues Paper published by the Office of the Australian Information Commissioner (**OAIC**) about the development of a Children's Online Privacy **Code**.

2. The Law Council supports the development and registration of the Code under the *Privacy Act 1988* (Cth) to strengthen privacy protections for children online, consistent with Proposal 16.5 of the Privacy Act Review Report.[1] We note that the Government subsequently agreed to this proposal.[2]

3. The *Privacy and Other Legislation Amendment Act 2024* (Cth) inserted section 26GC into the Privacy Act, providing that the Information Commissioner must develop and register an Australian Privacy Principles (**APP**) code about online privacy for children within 24 months of Royal Assent (by 10 December 2026).[3]

4. As outlined in the Issues Paper, the aim of the Code is not to prevent children from engaging online, but to ensure that their personal information is protected within that space.[4] Once registered, the Code will bind online services that are likely to be accessed by children,[5] including social media services, relevant electronic services, and designated internet services, as defined in the *Online Safety Act 2021* (Cth).[6] These categories comprise a wide range of online services, such as social media, messaging apps, websites, and cloud storage services.[7]

5. The Code will set out how one or more of the APPs will be applied, or is to be complied with, in relation to children's personal information.[8] The Code may also include additional requirements, if they are not contrary to, or inconsistent with, the APPs.[9]

6. As a first step when developing the Code, the OAIC should carefully consider the extent to which the Code should reflect and promote privacy rights alongside other rights, such as the best interests of the child. In addition, the Code should be drafted with the existing legislative landscape in mind, including the next tranche of reforms arising from the Privacy Act Review Report, Australia's obligations under international law, and the Australian Government's November 2024 commitment to legislate a digital duty of care.[10]

7. In developing the Code, there is also an opportunity to encourage harmonisation with relevant international regulatory approaches, enabling businesses to align with—and be supported in complying with—the increasing regulatory responses to these issues.

---

[1] Australian Government (Attorney-General's Department), *Privacy Act Review Report 2022* (February 2023) 157.
[2] Australian Government, *Government Response: Privacy Act Review Report* (September 2023) 13, 30.
[3] *Privacy Act 1988* (Cth) s 26GC(1), (10).
[4] Office of the Australian Information Commissioner ('OAIC'), *OAIC Children's Online Privacy Code Issues Paper* (June 2025) 3.
[5] *Privacy Act 1988* (Cth) s 26GC(5).
[6] *Online Safety Act 2021* (Cth) ss 13, 13A, 14.
[7] Office of the Australian Information Commissioner ('OAIC'), *OAIC Children's Online Privacy Code Issues Paper* (June 2025) 3.
[8] *Privacy Act 1988* (Cth) ss 26C(2)(a), 26GC(3).
[9] Ibid s 26C(3)(a).
[10] The Hon Michelle Rowland MP, *New Duty of Care obligations on platforms will keep Australians safer online* (Media Release, 14 November 2024).

8. The Code will also play an important role in complementing the existing eSafety regime in Australia, including the social media age restrictions that will take effect from December 2025, pursuant to the *Online Safety Amendment (Social Media Minimum Age) Act 2024* (Cth).

9. Nonetheless, we are aware that there is a large cohort of institutions—including in the State and Territory public education and health sectors—that are unlikely to be covered by the Code because they do not fall within the definitions of 'APP entity' and 'Organisation' under the Privacy Act. This means that, unless these definitions are amended, the Code (and the Privacy Act) will not apply to these other institutions, even though many of them provide services to children. Greater attention, therefore, must be paid to what entities may, and may not, be covered by the Code.

10. Further, in developing the Code, obligations under the United Nations Convention on the Rights of the Child should be taken into account,[11] noting that Article 3 provides that:

> *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.*[12] [Emphasis added]

We suggest that the OAIC can more clearly reflect the best interests of the child as a primary consideration in drafting the Code. Further consultation by the OAIC on this point is needed, specifically on the incorporation of ratified international treaties in domestic laws.[13]

11. We understand that the OAIC intends to release a draft version of the Code for public consultation in early 2026.[14] We look forward to contributing further to this consultation process once the draft Code is published.

General comments

Consultation with children and young people

12. Children and young people should be given the opportunity to express their views in relation to matters that will affect them. We commend the OAIC for placing children and young people at the centre of the development of the Code,[15] and note that these previous consultations have identified a variety of privacy issues that children consider to be especially important, including:

- concerns about privacy and a call for stronger protections;
- transparency and age-appropriate communication;

---

[11] *Convention on the Rights of the Child*, opened for signature 20 November 1989, 1577 UNTS 3 (entered into force 2 September 1990) arts 3, 16.
[12] Ibid art 3.
[13] See *Minister for Immigration and Ethnic Affairs v Teoh* [1995] HCA 20; 183 CLR 273, which underscores that ratified treaties do not automatically become part of Australian law, but can influence administrative decision-making by creating legitimate expectations. This principle is subject to limitations and has been the focus of ongoing legal and governmental scrutiny.
[14] Office of the Australian Information Commissioner ('OAIC'), *OAIC Children's Online Privacy Code Issues Paper* (June 2025) 3-4.
[15] See Dr Kate Bower (OAIC), *Sunshine and double rainbows – building a better online environment for children and young people* (15 April 2025).

- informed consent and digital literacy;
- control over personal data and privacy;
- data minimisation, privacy settings, and geolocation data; and
- data security and protection from harm.[16]

13. The Law Council supports the OAIC's ongoing consultations with children and young people, as well as their parents and carers. In addition, we support Commonwealth funding for education and accessible resource initiatives to support children's awareness and decision-making when interacting with online services.

Best interests of the child

14. Determining the developmental capacities of different age cohorts—and the risks inherent in different age assurance methods—can be a complex undertaking.

15. The Law Council supports a principles-based approach that is as consistent as possible with existing Australian online safety legislation. We also support introducing an overarching 'best interests of the child' principle in the Code, noting the comments above. The OAIC should consider the best-interests principle in the design of the Code and its requirements, even when children are not the intended primary users of the online service. It is the Australian Government's obligation under international law to interpret and apply the 'dynamic' best interests standard when making regulations that affect children.[17]

16. For example, the Code could specify that the APPs, as they apply to children, should be implemented with children's vulnerability and greater need for protection in mind. This is not intended to be a new obligation, but an additional requirement that is consistent with the APPs, and will strengthen what is considered to be reasonable in the context of children's vulnerability. Imposing such a requirement is also consistent with paragraph 26C(3)(a) of the Privacy Act, which allows APP codes to 'impose additional requirements … so long as the additional requirements are not contrary to, or inconsistent with' the APPs.

17. In its General Comment on children's rights in relation to the digital environment, the UN Committee on the Rights of the Child calls on States Parties to ensure that Convention rights—including the right to be free from discrimination and to be protected from harm, as well as to have one's best interests prioritised and views respected—are upheld in the digital environment as they must be offline.[18] On the other hand, the Committee notes that children also have the right to impart and receive information freely in common with adults—but measures need to be put in place to allow them to exercise this right in safety. The Committee recommends that regulatory agencies engage closely with children and their representatives in developing the relevant policies.[19] They should also exercise oversight over the implementation of the relevant policies once they have been promulgated.[20]

---

[16] Office of the Australian Information Commissioner ('OAIC'), *OAIC Children's Online Privacy Code Issues Paper* (June 2025) 7-9.
[17] UNCRC, *General Comment 25*, UN Doc CRC/C/GC/25 (2 March 2021), [12]. See further *General Comment No 14 on the right of the child to have his or her bests interests taken as a primary consideration,* UN Doc CRC/C/GC/14 (29 May 2013).
[18] Ibid, [8]-[18].
[19] Ibid, [27].
[20] Ibid, [31].

18. In terms of business compliance, the Committee on the Rights of the Child notes that governments have a responsibility to protect children from infringements of their rights by businesses.[21] One way in which this can be done is to require businesses to carry out child rights impact assessments and due diligence, to assess how their policies and practices might affect children. Businesses should also be required to provide age-appropriate information for children using their services, including on any risks involved.[22] Finally, there should be enforcement mechanisms for non-compliant businesses, along with remedies for children whose rights are infringed by a business.[23]

Implementation and compliance

Practicality and workability

19. To the extent that the Code interacts with the pending social media age restriction reforms, we note that there are significant challenges with age verification—particularly regarding the need to ensure that any solution is technically workable and does not result in excessive data collection (especially with age estimation methods) or inaccurate or misleading data.

20. The June 2025 preliminary findings from Australia's Age Assurance Technology Trial indicate that effective age assurance is technically feasible, and can be implemented with appropriate privacy safeguards.[24] However, the trial also highlights concerns about some providers collecting and retaining more personal data than necessary, which raises privacy risks.[25]

21. As Australia awaits the final report of the Trial in late 2025, which will directly inform the implementation of the upcoming social media age restrictions, it is important that any age verification process remains technology-neutral and reasonably reliable. There should also be consistency in the acceptable use of technologies across different regulatory regimes to ensure clarity and fairness for users and service providers.

Compliance and enforcement

22. Breaches of the Code may result in enforcement, and potentially significant penalties under the eSafety and privacy regimes. However, barriers to enforcement may arise, such as jurisdictional challenges with overseas platforms, and the complexity of monitoring harmful content.

23. Ultimately, the Code must be supported by proactive compliance support. Ongoing education, industry engagement, and transparent enforcement by regulators will be critical to ensure that the Code is effective in protecting children online.

---

[21] Ibid, [37]. See also UNCRC, *General Comment 16 on State obligations regarding the impact of the business sector on children's rights*, UN Doc CRC/C/GC/16 (17 April 2013).
[22] Ibid, [38]-[39].
[23] Ibid, [43]-[49].
[24] Age Assurance Technology Trial, *Age Assurance Technology Trial publishes twelve preliminary findings ahead of full report* (News Release, 20 June 2025).
[25] Ibid.

Consultation questions

Scope of services covered by the Code

24. The scope of services addressed by the Code is a critical element in ensuring comprehensive protection for children online.

The UK approach

25. The United Kingdom's Age Appropriate Design Code (**UK Code**) establishes a broad framework that encompasses a wide range of online services that process personal data and are likely to be accessed by children.[26] This includes not only services specifically aimed at children, but also those that, while not primarily intended for children, are nonetheless *likely to be accessed* by them.[27]

26. The Explanatory Memorandum to the Privacy and Other Legislation Amendment Bill 2024 (Cth) makes clear that the Code is intended to align with the broad scope established by the UK Code.[28] Other jurisdictions have also adopted the UK approach, including Ireland[29] and California.[30] Using the UK Code as a starting point for the Code in Australia would, therefore, support international alignment and harmonisation, and would promote compliance for businesses operating across multiple jurisdictions.

27. However, the Law Council cautions that, given that the UK Code has been in place since 2021, the OAIC should conduct, and publish, an assessment of lessons learned from the UK. For instance, we have received feedback that whilst a high-level, conceptual approach to the UK Code may have been appropriate at that point in time, it would be beneficial if the Australian approach provided greater specificity so that businesses and legal practitioners have greater certainty, and can be appropriately supported to comply.

28. As the UK Code is relatively high-level, this may present difficulties for some entities seeking to operationalise its requirements in practice. There have also been significant shifts in public understanding and expectations regarding privacy since 2021—with recognition of the particular vulnerabilities of children online—highlighting the need for more detailed and practical requirements.

29. By way of illustration, the UK has recently legislated new requirements through its *Data (Use and Access) Act 2025*, including introducing an explicit requirement for online services that are likely to be accessed by children to consider children's needs when determining how their personal information is used.[31]

---

[26] This includes online products or services (including apps, programs, websites, games or community environments, and connected toys or devices with or without a screen): Information Commissioner's Office (UK), *Age Appropriate Design: A Code of Practice for Online Services* (2 September 2020), About this code.
[27] Information Commissioner's Office (UK), *Age Appropriate Design: A Code of Practice for Online Services* (2 September 2020), Services covered by this code.
[28] Explanatory Memorandum, Privacy and Other Legislation Amendment Bill 2024 [85], [96].
[29] Data Protection Commission (Ireland), *The Fundamentals for a Child-Oriented Approach to Child Processing* (December 2021).
[30] *California Age-Appropriate Design Code Act 2022*.
[31] See UK Government (Department for Science, Innovation and Technology), *Data (Use and Access) Act 2025: data protection and privacy changes* (27 June 2025).

30. The UK Information Commissioner is currently reviewing and updating existing guidance on the UK Code to reflect these new obligations, following the commencement of the Act on 19 June 2025.[32] This ongoing reform process highlights the importance of regulatory frameworks that are robust and guide effective compliance.

Question 1.1: Are there additional APP entities, or a class of entities, that should be covered by the Code?

31. Subsection 26GC(5) of the Privacy Act provides that, once registered, the Code will apply to APP entities if:

    (a) the entity is a provider of a social media service, relevant electronic service, or designated internet service (all within the meaning of the Online Safety Act); and

    (b) the service is likely to be accessed by children; and

    (c) the entity is not providing a health service.

    The OAIC may also specify in the Code additional entities, or a class of entities, to which the Code applies or does not apply.[33]

32. There should be clear and comprehensive guidance on which entities are intended to be captured. In particular, we suggest that the OAIC should consider the application of the Code to the entities outlined below.

Entities captured by subsequent tranches of reform to the Privacy Act

33. There are a range of proposals that were made in the Privacy Act Review Report, and that the Government agreed to (either in full, or in principle), that are yet to appear in the Government's legislative agenda. Such proposals include:

    (a) the eventual removal of the small business exemption (Proposal 6.1);[34]

    (b) the codification of current OAIC guidance that valid consent must be given with capacity (noting an entity may assume that an individual over the age of 15 has capacity, unless there is something to suggest otherwise) (Proposal 16.2);[35] and

    (c) the right to erasure (Proposal 18.3).[36]

34. The Law Council has repeatedly called on the Government to release a roadmap to outline its specific intentions for further tranches of reform arising out of the Privacy Act Review Report, including indicative timeframes.[37] Nonetheless, if the small business exemption is ultimately removed, then entities that currently sit outside the scope of the Privacy Act could become subject to the Code if they meet the relevant thresholds in section 26GC of the Privacy Act.

---

[32] Information Commissioner's Office (UK), *Our plans for new and updated guidance* (2025).
[33] *Privacy Act 1988* (Cth) s 26GC(5)(b).
[34] Australian Government, *Government Response: Privacy Act Review Report* (September 2023) 13, 30.
[35] Ibid 13, 29.
[36] Ibid 18, 31.
[37] See Law Council of Australia, *Privacy and Other Legislation Amendment Bill 2024* (Submission, 22 October 2024) 16-17.

35. Additionally, third parties that require, recommend, or approve the use of a service covered by the Code should be responsible for ensuring that the service complies with the Code before doing so.

Artificial intelligence (AI) chatbots

36. Concerns have been raised in the media about AI therapy chatbots accessed by children, which have provided morally objectionable and 'alarming' advice to users who are seeking therapy.[38]

37. The Code should explicitly include AI chatbot services, to avoid them being inadvertently excluded as a 'health service provider', which they are not, given that the chatbot behind the AI 'persona' is not a qualified human.

38. In addition, it is unclear whether AI chatbot services fall under 'relevant electronic service' per subparagraph 26GC(5)(a)(i) of the Privacy Act, as they do not facilitate communication between humans, as messaging applications typically do. Given the likelihood that personal information would be input by the user during an online interaction with an AI chatbot, the Law Council suggests the express inclusion of entities that provide this type of service.

Online purchases

39. The Code should consider whether any online purchase services are included, as it is currently unclear whether these would fall under the definition of a 'designated internet service'.

40. Careful consideration should be given to the benefits and drawbacks of such an approach. More benign examples are online shopping platforms that will inevitably require some personal information, such as a home address for delivery. More harmful examples are platforms that offer potentially illegal items for purchase, such as alcohol or weapons.

Geolocation or GPS services

41. Geolocation services, such as Google Maps and other navigation systems, may allow users to save their home address and other addresses in the system, for ease of navigation. It would be useful for clarity to be provided on whether these services would be captured by the Code.

Education providers

Schools and social media

42. We recognise that independent schools (and other private education providers) with an annual turnover of more than $3 million are already APP entities and, therefore, covered by the Privacy Act. However, public schools do not fall within the definitions of 'APP entity' and 'Organisation'. For public schools to be covered by the Code, consideration should be given to amending the definitions of 'APP entity' and

[38] See, e.g., Andrew Chow and Angela Haupt, 'A Psychiatrist Posed as a Teen with Therapy Chatbots. The Conversations Were Alarming', *Time* (Online, 12 June 2025); April McLennan, 'Young Australians using AI bots for therapy', *ABC News* (Online, 18 May 2025).

'Organisation' in the Privacy Act,[39] or creating complementary obligations under the applicable State and Territory-based regimes.

43. Schools often use internet services and communication apps on a child's behalf by posting a child's personal information on public online platforms. This includes posting photos of children, along with their names, classes, and achievements—or school newsletters—on social media.

44. We understand that many parents may be signing school consent forms without fully understanding the privacy implications of the school's actions, or feeling that they have no choice but to do so. Consent for their child's photo to be taken is often combined with consent for the photos to be posted online, and refusal to consent generally means that child would be excluded from group photos.

45. In terms of any consent given to the social media platform, the school is effectively providing consent on behalf of the child. This is related to feedback provided earlier this year to OAIC by Reset.Tech Australia, where it was raised that consent provided by a school on behalf of the child should be critically analysed, and should not override the child's consent.[40]

46. Once the child's photo is posted on the school's social media platform, the child loses control over what other social media users do with their personal information, which may include harmful purposes, such as profiling, stalking, bullying, and intimidation.

47. The exposure of a child's personal information, including their photos, is also of concern where children or parents are affected by domestic and family violence: the child's photos might be used to ascertain their whereabouts, including the location of their school.

Education technologies and data brokers

48. The use and reliance on education technologies by Australian schools markedly increased during the COVID-19 pandemic, and remains a key component of the digital classroom.[41]

49. Despite the benefits of education technologies for schools and children, the collection, use, and disclosure of children's personal information through the use of these services has significant implications for children's privacy, particularly given their vulnerability to privacy risks and harm online.[42] The Code must sufficiently address these risks.

50. In particular, the increasing use of AI and data brokering within education technologies, and other online service platforms, presents additional risks for children. These risks include extensive profiling, targeted advertising, and the potential for commercial exploitation of children's personal data, which can have long-term impacts on their privacy and wellbeing.[43]

---

[39] Section 6 of the Privacy Act defines an *APP entity* to mean 'an agency or organisation', with *Organisation* defined by section 6C.
[40] Reset.Tech Australia, *Consultation with young people about the Children's Online Privacy Code and consent and agency* (Submission, March 2025) 5.
[41] Australian Institute for Teaching and School Leadership Limited, *Spotlight: Evaluating the evidence for educational technology: Part 2 – enabling learning* (March 2024).
[42] Luci Pangrazio and Anna Bunn, 'Assessing the privacy of digital products in Australian schools: Protecting the digital rights of children and young people', 6 *Computers and Education Open* (2024).
[43] Reset.Tech Australia, *The Children's Online Privacy Code and targeted advertising* (June 2025).

51. Internationally, the UK has taken steps towards the development of specific standards for educational technologies, AI, and automated decision-making under the *Data (Use and Access) Act 2025*, with the UK Government committing to develop codes of practice specifically for these technologies.[44]

52. The OAIC should consider adopting similar risk-based responses to address the potential harms that children may face when using these technologies. Guidance should also be provided to education service providers—particularly schools—when procuring and using third party educational technology tools.

When and how the Code should apply to APP entities

Health service provider exclusion

53. According to the Explanatory Memorandum to the Privacy and Other Legislation Amendment Bill 2024, the intention of the broad exclusion for health service providers is to ensure that the Code does not pose a barrier to providing essential health services to children.[45] Moreover, this approach is intended to align with the UK Code in preserving access to necessary health services for children.[46]

54. As stated in the Explanatory Memorandum, guidance from the OAIC clarifies that 'health service' providers include online health services, such as counselling, advice, and telehealth.[47] However, more general health, fitness, or wellbeing apps or services may be covered by the Code.[48]

55. The exclusion for health service providers should be clarified to ensure it is applied appropriately. A broad exclusion has the potential to allow a wide range of services to fall outside the Code's scope and protections, including some that may not be providing essential health services. The exclusion should be narrowly defined, and consistent with the legislative intention.

'Likely to be accessed' test

Question 2.1: What threshold should determine when a service is considered 'likely to be accessed by children'?

56. In some circumstances, the 'likely to be accessed by children' threshold under subparagraph 26GC(5)(a)(ii) of the Privacy Act will be easily ascertainable. However, given the nature of online service accessibility (especially for older children), the test will be less clear for some services. A list of non-exhaustive factors will likely be of benefit in these instances, as contemplated in the Explanatory Memorandum to the Privacy and Other Legislation Amendment Bill 2024:

> *In assessing whether a service is likely to be accessed by children, service providers should consider factors such as:*
>
> *(1) the nature and content of the service, and whether it has a particular appeal to children,*

[44] Information Commissioner's Office (UK), *The Data Use and Access Act 2025 – what does it mean for organisations?* (19 June 2025).
[45] Explanatory Memorandum, Privacy and Other Legislation Amendment Bill 2024 [85].
[46] Ibid.
[47] Ibid.
[48] Ibid.

(2) market research, current evidence on user behaviour, the user base of similar or existing services and service types, and

(3) the way in which the service is accessed, and whether any measures put in place are effective in preventing children from accessing the service.[49]

57. As set out in this Explanatory Memorandum, the Code should also emphasise proactive assessment by service providers, regardless of whether they are child-targeted.[50] If age cannot be reasonably determined, the Code's protections should be reasonably applied to all users.

Steps that captured APP entities should be required to take

58. To ensure robust privacy protections for children and young people in the digital environment, the Code should set out clear, enforceable requirements for APP entities. These requirements should be proportionate, risk-based, and responsive to where vulnerabilities are known, or emerge.

Privacy by design

59. At a broad level, the Law Council supports high privacy defaults for children. It is in the best interests of the child for the strictest privacy settings to be set as the default for services that are likely to be accessed by children. This would shift the onus for privacy protection to the entity providing the service, given that a child may not be capable of genuinely providing consent.

60. In her foreword to the UK Code, the UK Information Commissioner stated:

> *Settings must be "high privacy" by default (unless there's a compelling reason not to); only the minimum amount of personal data should be collected and retained; children's data should not usually be shared; geolocation services should be switched off by default. Nudge techniques should not be used to encourage children to provide unnecessary personal data, weaken or turn off their privacy settings*.[51]

61. The OAIC should consider adopting similar requirements in the Code as Standards 7, 10, and 12 of the UK Code regarding 'high privacy' by default, geolocation options to be switched off by default, and profiling to be switched off by default, taking account of the best interests of the child.[52]

62. Implementing default settings to protect privacy is consistent with Proposal 11.4 of the Privacy Act Review Report for online privacy settings to reflect a 'privacy by default' framework,[53] to which the Government agreed to, in principle.[54] Consistency should also be achieved between the Code and the *Online Safety (Basic Online Safety Expectations) Determination 2022* (Cth).

---

[49] Explanatory Memorandum, Privacy and Other Legislation Amendment Bill 2024 [85].
[50] Ibid.
[51] Information Commissioner's Office (UK), *Age Appropriate Design: A Code of Practice for Online Services* (2 September 2020), Information Commissioner's foreword.
[52] Information Commissioner's Office (UK), *Age Appropriate Design: A Code of Practice for Online Services* (2 September 2020), Code standards.
[53] Australian Government (Attorney-General's Department), *Privacy Act Review Report 2022* (February 2023) 8, 109.
[54] Australian Government, *Government Response: Privacy Act Review Report* (September 2023) 8, 26.

Consent

63. As acknowledged in the Issues Paper, children are particularly vulnerable to the misuse of their data, and may not fully understand the privacy implications of their online activity.[55]

64. Comparable jurisdictions have sought to protect children's online personal information by providing special protections for children's data, with variations in the age thresholds that trigger those protections. Dominant themes that arise are the vulnerability of children, and their capacity to consent to the collecting and processing of their data.

65. As Recital 38 of the European Union (**EU**) General Data Protection Regulation states, children's vulnerability means that they may be less aware of the risks and consequences of sharing their personal data online.[56] In addition, most member countries of the Organisation for Economic Cooperation and Development (**OECD**) give special protections to children's data, often on the basis of consent from the child or their parent.

66. The Law Council queries whether consent, when it comes to data collection, is a practicable and appropriate model, noting its limitations when it comes to children, especially vulnerable children. Furthermore, even a fully informed and mature adult may not be able to appreciate the full ramifications of consenting to their personal information being used or disclosed by an APP entity, especially potential future consequences. We do not yet have a settled view on this question, and we recommend that the OAIC conduct further consultations on the merits of a consent-based model, including how greater alignment with other law reform initiatives can be achieved.

67. The OECD recently reported that child-specific protections in privacy and data protection laws often add to a 'fragmented landscape', due to varied triggers for consent.[57] For example, some countries allow profiling for targeted advertising based on consent, while others permit advertising for 'a compelling reason' or if a 'best interests criterion' can be demonstrated.[58]

68. The United Kingdom's Age Appropriate Design Code (**UK Code**) specifies that children from ages 0–12 are incapable of providing consent to the processing of their personal data in the context of an online service offered directly to a child.[59] The lawful basis for processing the personal information of children under the age of 13 is parental consent.[60]

69. The Australian Government has introduced an obligation on age-restricted social media platforms to prevent children aged under 16 years from having accounts on their services by December 2025.[61] There is, therefore, opportunity for alignment with the *Online Safety Act 2021* (Cth) in considering age thresholds and capacity for consent. If parental consent is to be adopted in Australia, for example, for children

---

[55] Office of the Australian Information Commissioner ('OAIC'), *OAIC Children's Online Privacy Code Issues Paper* (June 2025) 6.
[56] European Union, 'Recital 38: Special Protection of Children's Personal Data', *General Data Protection Regulation* (27 April 2016).
[57] Organisation for Economic Cooperation and Development ('OECD'), *The legal and policy landscape of age assurance online for child safety and well-being* (June 2025) 37.
[58] Ibid.
[59] Information Commissioner's Office (UK), *Age Appropriate Design: A Code of Practice for Online Services* (2 September 2020), Annex B.
[60] Ibid.
[61] *Online Safety Amendment (Social Media Minimum Age) Act 2024* (Cth).

under 16 years old (to promote consistency with online safety laws), the OAIC should consider guidance on the mechanism for obtaining meaningful parental consent. For instance, the United States and Korea specific methods such as credit card authentication, email or text confirmation, or completing a consent form.[62]

70. At a minimum, it will be important for consent to be voluntary, current and specific, and informed. Clarity will be needed as to what valid consent will mean in the Code, and a relevant entity should be required to satisfy that consent has been validly obtained.

71. There may also be a need for additional consent requirements in certain circumstances, such as the imposition of a strict consent requirement for all uses and disclosures that may now, or in the foreseeable future, involve direct marketing or biased decision-making.

72. We note that consent to the collection of personal information is commonly obtained in conjunction with—or is embedded in—agreements, terms of use, product licences, or other contracts for goods and services. The ability of children to enter into those kinds of agreements is a matter for State and Territory laws and is beyond the scope of the Code and the Privacy Act.

Erasure rights

73. Processes for requesting the deletion of personal data must be simple, age-appropriate, and responsive to the needs of children. Entities should ensure that children and their guardians can easily understand and navigate these processes, including by providing clear guidance and support throughout.

Age range-specific guidance

74. UNICEF's *Online privacy checklist for parents* recommends implementing age-appropriate privacy settings and controls, recognising the importance of adapting protections to suit different age groups and abilities.[63] There is a significant difference in digital literacy between a young person aged 12 to 15, and a child under the age of five. Additionally, the Code should consider the needs of children living with disabilities or specific vulnerabilities that entities should be conscious of.

75. We suggest a risk-based approach with specific requirements to address high-risk areas, such as direct marketing—particularly online targeted advertising—to children.

76. Regardless, the purpose of such age-appropriate settings and controls should be to empower the user. There remains a risk that online businesses may see these requirements as minimum thresholds that, once met, will enable them to exploit children's data.

[62] Organisation for Economic Cooperation and Development ('OECD'), *The legal and policy landscape of age assurance online for child safety and well-being* (June 2025) 36-37.
[63] UNICEF, *Online privacy checklist for parents* (2025).

APP 1—Open and transparent management of personal information

Question 4.1: What communication methods should APP entities use to ensure privacy policies are meaningfully understood by children of different ages, abilities and backgrounds?

77. Privacy policies and collection notices for adult users already tend to be lengthy and technical. Privacy policies directed at children should be clear, concise, and understandable. We refer the OAIC to the child-friendly privacy policies of Lego[64] and Paramount[65] as useful examples in this regard.

78. Further, to improve the effectiveness of notification, standardised graphics or videos, such as infographics or animations, should be required by the Code where consent of a child is likely to be sought, along with standardised templates, layouts, and terminology. Such an approach would facilitate consistency and harmonisation of communicating privacy policies to children, and would be aligned with Proposals 10.1, 10.3 and 16.3 of the Privacy Act Review Report.[66]

79. Nonetheless, and as indicated earlier in this submission, the Law Council holds reservations that children will, in practice, be capable of giving meaningful consent to the use of their personal information in many situations, especially in the online context. The use of icons, cartoons, or other child-friendly layouts cannot change this fact. We question the merits of the consent-based model as a means of regulating privacy rights in the digital environment.

80. Such an approach fails to reflect that consent is likely to arise where a large corporation is seeking to harvest data. Even if some form of acknowledgement or consent is sought in a clear and understandable way, it is difficult to see how the power imbalance between the entity and child user could be overcome.

81. Further, the significance of the personal information being sought cannot be overstated, as what an older child may agree to share could remain online permanently, even after they become an adult.

82. Online services should not be permitted to shift the burden of determining whether the service is 'privacy safe' to children through a privacy police and collection notice. The service provider should nonetheless be required to ensure that the service meets the requirements of the Code and the APPs more generally.

Question 4.2: How should APP entities ensure APP 1 obligations are met when their services are used by both adults and children, particularly when children are not the intended primary users?

83. The Code should provide specific guidance on how the APPs should be applied in the children's online safety context, similar to the level of specificity provided by the current APP Guidelines.[67]

[64] Lego, *Our Privacy Policy* (8 February 2024).
[65] Paramount, *Let's Talk About Privacy!* (2025).
[66] Australian Government (Attorney-General's Department), *Privacy Act Review Report 2022* (February 2023) 97, 100, 151.
[67] OAIC, *Australian Privacy Principles guidelines* (December 2022).

Question 4.3: What should be considered under the 'reasonable steps' test when implementing internal practices, procedures and systems for managing children's personal information?

84. As a general principle, the Law Council supports consistency in implementation. There should not be a requirement for two sets of practices for handling the information of adult and child users.

85. If certain APP entities have children accessing their service as well as adults, the vulnerability of children should be prioritised in the 'reasonable steps'. If this results in stricter internal practices, procedures, and systems, these should cover both children's and adults' personal information.

86. As soon as there is the likelihood that children may access the service, the best interests of children should be the primary consideration that balances other interests, and should apply to practices, procedures, and systems that handle the personal information of all users, regardless of their age.

87. The Code should provide specific guidance on openness and transparency. For example, in the context of schools, the 'reasonable steps' should include consideration as to whether social media is an appropriate forum to post regular updates about students, and how internal procedures could be improved to minimise what information is given to a public online platform.

Question 4.4: What steps should APP entities take to ensure children, and their parents, can easily make privacy-related inquiries or complaints, and how should APP entities respond in a child appropriate way?

88. The current APP standard should not change, but the entity's communication should be tailored to an audience that includes children, so as to readily enable them to make privacy-related inquiries or complaints.

APP 2—Anonymity and pseudonymity

Question 5.4: Do you have any specific views on how APP 2 should be applied or complied with in relation to the privacy of children?

89. The Law Council's general position is that data minimisation should be prioritised. APP entities will, therefore, need to consider whether the information is necessary. For example, whether it is necessary to collect details about a child's residential address for a messaging service.

90. Whether a child can be easily identified also depends on the number of service users, and what other information is collected from the child. For example, if the child user is categorised into a school group or sports group in an online forum, the likelihood of anonymity would be smaller.

APP 3—Collection of solicited personal information

Question 6.1: What criteria should define what is 'reasonably necessary' for an APP entity's functions or activities when collecting children's personal information, and how can APP entities ensure they adhere to this?

91. If the service can be delivered with less information, the APP entity should collect less information. We recommend consistency with the UK Code that only the minimum amount of personal data should be collected and retained.[68]

92. Moreover, APP entities should not be permitted to use nudge techniques to encourage children to provide unnecessary personal data, weaken, or turn off their privacy settings.

93. More broadly, further consideration should be given to the role of APP 3 and the potential for the Code to incorporate child-specific elements relevant to the necessity requirements, noting that:

    - an agency may only solicit and collect personal information that is reasonably necessary for, or directly related to, one or more of its functions or activities (APP 3.1); and
    - an organisation may only solicit and collect information that is reasonably necessary for one or more of its functions or activities (APP 3.2).

Question 6.2: What does 'lawful' and 'fair' mean in the context of children's personal information? How should these terms be applied specifically for children, given their evolving developmental and digital engagement stages?

94. Collection of children's personal information may be lawful, but not fair. In this respect, we caution against direct parity with the UK and EU approaches, given that there is no direct correlation between the UK and EU notion of 'lawful basis for processing' and the requirement under APP 3 that personal information must only be collected by 'lawful and fair means'. Noting this, the Code may have a useful role to play in assisting to determine what is 'fair means' in the context of services to children, especially social-media related matters.

95. Further, as the Australian Government agreed to a 'fair and reasonable test' in its Response to the Privacy Act Review Report,[69] this may form part of a subsequent tranche of privacy law reforms. We reiterate our call for the Government to release a roadmap to outline its specific intentions for further tranches of reform.

Question 6.3: Are there cases in which the collection of children's personal information would not be considered fair in any circumstances?

96. The collection of children's personal information may not be fair if providing personal information is the only way to gain initial or continued access to a certain age-appropriate service. However, careful consideration should be given to access and funding considerations for such services.

97. Further, it may be unfair if there are incentives or 'discriminating benefits' for users who provide their personal information for use. That is, handing over data in order to access perks, such as greater functionality or custom graphical interfaces. Many

[68] Information Commissioner's Office (UK), *Age Appropriate Design: A Code of Practice for Online Services* (2 September 2020), Data minimisation.
[69] Australian Government, *Government Response: Privacy Act Review Report* (September 2023) 27.

games and free to use programs have adopted this model to harvest data from users under 18 years old, and these status perks can be highly persuasive.

Question 6.4: How can APP entities obtain genuine consent from children, or their parents or guardians, for the collection of sensitive information?

98. As stated above, the Law Council questions the merits of a consent-based model for the collection—and subsequent use and disclosure of—children's personal information. When the onus or responsibility is shifted to the child, they can feel coerced and believe there is no choice but to provide the information.

99. With specific reference to this question, we query why an online service that is not providing a health service would require sensitive information at all. Sensitive information (as defined in section 6 of the Privacy Act), such as ethnicity or criminal records, would not be 'reasonably necessary' for a service accessed by a child.

APP 4—Dealing with unsolicited personal information

Question 7.1: What processes should APP entities implement to identify and appropriately handle unsolicited personal information related to children?

100. Currently, if an APP entity receives personal information that it did not solicit, it must (within a reasonable period after receiving the information) determine whether it could have collected the information under APP 3. If not, the APP entity must destroy or de-identify the information as soon as practicable, provided it is lawful and reasonable to do so.

101. The automatic destruction of unsolicited personal information about children—even if it could have been collected under APP 3—will enhance privacy protections for children, acknowledge their vulnerability, and recognise the need for stricter safeguards. This destruction may also reduce risks of misuse or mishandling of sensitive information.

102. We acknowledge that this proposed approach may create a stricter standard than what currently applies under APP 4, and could lead to inconsistency in compliance practices, and challenges for entities trying to reconcile their obligations under APPs 3 and 4.

103. However, paragraph 26C(a) of the Privacy Act allows APP codes to impose additional requirements that are consistent with the APPs. This is also consistent with our argument earlier in this submission that only the minimum amount of data should be collected and retained. The collection of unsolicited information appears to be at odds with that position.

104. As an alternative to enforcing automatic destruction, a clearer guidance framework could be developed that encourages entities to critically assess unsolicited information about children, and requires explicit justification for retaining such data, even if it meets APP 3 criteria. This approach would promote transparency and accountability in handling children's personal information.

105. In respect of how an APP entity may identify that the unsolicited personal information relates to children, methods should be considered such as assessing the content, language cues, metadata, or the source of the information.

106. If there is any doubt, the Law Council prefers the minimisation of risk through destruction or de-identification of the unsolicited information. There is a need for entities to develop guidelines and processes to:

- flag the unsolicited information for review;
- include criteria for identifying child-related information; and
- train staff to recognise and handle information appropriately, in the best interests of the child.

APP 6—Use or disclosure of personal information

Question 9.2: What safeguards should APP entities put in place to prevent the misuse of children's personal information for secondary purposes without appropriate consent or where other exceptions apply?

107. The use or disclosure of children's personal information for broad 'secondary purposes' (especially targeting, profiling, and other related activities) pose particular risks. Nonetheless, we acknowledge the legal exceptions to APP 6, and the complexities involved in identifying if information is, indeed, personal information of a child. We also recognise other countries' allowance of disclosure for secondary purposes, based on consent.[70]

108. In light of the above, the OAIC should conduct further consultation on secondary uses of children's personal information, noting that many uses are not controversial and support the delivery of services, including to children. In this respect, it should be recognised that the core purpose of the Code is to support the interpretation of the APPs, rather than introduce new mechanisms for privacy compliance.

109. As a starting point, the Law Council suggests consideration be given to limiting the scope of permitted secondary uses for children's personal information, or clarifying the scope of how relevant exceptions for the use and disclosure for secondary purposes should operate. These approaches would ensure that a higher standard for any secondary use is applied. For example, this may involve clarifying that the scope of the 'reasonable expectation' exemption could be determined on the basis that any reasonable expectation would need to be consistent with the best interests of the child.

110. In some circumstances, it may be appropriate for APP entities to carry out the following actions prior to using a child's personal information for a secondary purpose:

- undertake a child-specific Privacy Impact Assessment before any secondary uses of child-related information take place;
- obtain documented informed consent by a parent or guardian, or a child over a certain age; and/or
- implement a flagging or data filter system to identify any child-related personal information.

[70] Organisation for Economic Cooperation and Development ('OECD'), *The legal and policy landscape of age assurance online for child safety and well-being* (June 2025) 36.

Question 9.3: What secondary uses or disclosures of personal information could be reasonably expected by children, and how should these expectations vary by age and stage of development?

111. As discussed above at Question 9.2, the Law Council considers that a higher standard should be applied to the application of the 'reasonable expectation' exemption in the context of the use and disclosure of personal information of a child. What a child can reasonably expect as a secondary purpose would vary greatly, not only by age cohorts, but also by environmental and socio-economic factors, education, exposure to social media, digital maturity, and experiences online.

APP 7—Direct marketing

Question 10.1: Can an APP entity ensure that it creates a 'reasonable expectation' that it may use or disclose children's personal information for the purposes of direct marketing? And if so, how?

112. As a starting point, and for the reasons stated above, children's personal information should not be used or disclosed for targeted marketing. Further, children do not have the adequate capacity to understand how far their data will travel. However, consideration should be given to whether there are circumstances in which targeted marketing activities are in the best interests of the child (e.g., access to certain media services).

113. The Law Council, therefore, supports a strict approach to targeted advertising directed at children in the Code. The Code should, at a minimum:

- require explicit, specific, informed consent for both the collection and use of children's data for targeted advertising; and
- prohibit direct marketing to children unless it is consistent with their best interests, and is subject to clear-time limited consent that does not continue once a child reaches 18 years of age.

Question 10.2: How can APP entities ensure mechanisms are in place for children to opt-out of receiving direct marketing communications, in a simple and accessible way?

114. The opt-out model is inappropriate for children. The default setting should require direct marketing communications and non-essential cookies for behavioural advertising to be turned off for children, with an opt-in option allowed after a certain age.

Question 10.3: Do you have any specific views on how APP 7 should be applied or complied with in relation to the privacy of children?

115. APP 7 does not apply to the extent that the *Do Not Call Register Act 2006* (Cth) (which regulates outbound telemarketing phone calls, unless exempt), the *Spam Act 2003* (Cth) (which regulates commercial electronic messages such as email, text messages, and instant messages), or any other legislation prescribed by the regulations apply.

116. This may mean that the Code (if its application is linked to APP 7) may not apply to direct marketing activities that are regulated under the Do Not Call Register Act or the Spam Act. Such a carve-out, if applicable, may be inappropriate. Consideration

should be given as to whether all direct marketing practices to children should be captured by the Code.

APP 8—Cross-border disclosure of personal information

Question 11.1: How can APP entities ensure that cross-border transfers of children's personal information are conducted in a way that protects children's privacy rights, especially when laws in other countries may not offer equivalent protections?

117. There is the potential for risks to arise when cross-border disclosure of children's personal information occurs. In this regard, we note that APP 8 provides a framework requiring APP entities to take reasonable steps to ensure that overseas recipients, in countries that do not provide equivalent protections, do not breach the APPs.

118. This may well be a suitable framework if applied appropriately, and could be supplemented by way of OAIC guidance as to any specific considerations that should be taken into account in relation to children and compliance with the Code.

APP 10—Quality of personal information

Question 12.1: What does 'accurate', 'up-to-date', 'complete' and 'relevant' mean in the context of children's personal information? How should these terms be applied specifically for children, given their evolving development and digital engagement stages?

119. Applying data minimisation across APP 10 will assist in protecting children's information across their stages of development and digital engagement. Although the APP 10 standards should be as rigorous for adults and children, the level of rigour in applying the steps depends on the circumstances, consistent with Chapter 10 of the APP Guidelines.[71]

120. The Code should require APP entities to undertake more frequent reasonable steps to check the accuracy and currency of the personal information, where there is a greater likelihood of the information being incorrect or having changed. As children's personal information often changes more frequently (e.g., school year, health status) and may become more sensitive (e.g., health, family situation), there is greater potential for harm if the information is mishandled. There is also a need for stricter relevance checks.

121. While the standard is the same, the application of that standard should be more rigorous for children—not because they are treated differently under APP 10, but because the circumstances require it. Again, these additional requirements would be in line with what is permitted under paragraph 26C(3)(a) of the Privacy Act.

[71] OAIC, *Australian Privacy Principles guidelines* (December 2022).

Question 12.2: How can APP entities effectively ensure that the personal information they collect from children remains accurate and up-to-date, considering the dynamic nature of a child's life and the potential challenges in maintaining this data?

122. Given the dynamic nature of a child's life, consideration should be given to whether their personal data should be deleted after a certain period of inactivity, especially after the purpose for collection has finished, or the user has reached adulthood.

123. Consideration should also be given to whether photos and data posted by a child's school should be deleted, and if so, at what frequency.

124. Users should have the ability to request that their personal data collected during childhood be deleted, in a similar way to the right to be forgotten in Article 17 of the EU General Data Protection Regulation.