THE LAW SOCIETY
OF NEW SOUTH WALES

Our ref: PDL:JBml230725

23 July 2025

Dr James Popple
Chief Executive Officer
Law Council of Australia
PO Box 5350
Braddon ACT 2612

By email: natalie.cooper@lawcouncil.au

Dear Dr Popple,

CHILDREN'S ONLINE PRIVACY CODE

Thank you for the opportunity to contribute to the Law Council of Australia's submission in response to the consultation of the Office of the Australian Information Commissioner (**OAIC**) on the Children's Online Privacy Code (**Code**) Issues Paper (**Issues Paper**). The Law Society's Privacy and Data Law Committee contributed to this submission.

General comments

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.

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

Consent and default settings – onus to be shifted in view of children's vulnerability

As Recital 38 of the General Data Protection Regulation says, children's vulnerability means they may be less aware of the risks and consequences of sharing their personal data online:

> Children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data.[1]

Most OECD member countries give children's data special protections, often on the basis of consent from the child or their parent.

In our view, consent when it comes to data collection is a deficient model. We note that the age of majority is required for consent in other areas of law, except, it appears, privacy law. It is arguably legally untenable to shift the onus or responsibility for consenting to data processing to the child. It may also be observed that even a fully informed and mature adult may not be able to appreciate the full ramifications of consenting to

[1] European Union, 'Recital 38', *General Data Protection Regulation* (Web Page, 27 April 2016) available here.

their personal information being used or disclosed by an APP entity, especially potential future consequences, which tends to be difficult even for those highly trained in the areas of risk analysis.

The OECD reports child-specific protections in privacy and data protection laws often add to a "fragmented landscape" due to varied triggers for consent. 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.[2] We discuss our views on targeted marketing further below. The UK'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.[3] The lawful basis for processing the personal information of children under the age of 13 is parental consent.[4]

As the Australian Government has introduced an obligation on age-restricted social media platforms to prevent children under 16 years old from having accounts on their services by December 2025, we suggest alignment with the *Online Safety Act 2021* in considering age thresholds and capacity for consent. If parental consent is to be adopted in Australia, for example, for children under 16 years old for consistency with online safety laws, we suggest the OAIC considers guidance on the mechanism for obtaining parental consent such that it is meaningful. For example, Korea and the United States specify methods such as credit card authentication, email or text confirmation, or returning a consent form.[5]

We suggest that it is in the best interests of a child for the strictest privacy settings to be set as the default for services likely to be accessed by children. This shifts the onus for privacy protection to the entity providing the service, given that a child may not be capable of genuinely providing consent.

The UK Information Commissioner noted the following in her foreword to the UK Code:

> 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.[6]

We suggest the OAIC considers adopting similar requirements as Standards 7, 10, and 12 of the UK Code regarding "high privacy" by default, geolocation options to be off by default, and profiling to be off by default, taking account of the best interests of the child.

---

[2] OECD, 'The Legal and Policy Landscape of Age Assurance Online for Child Safety and Well-being' (2025) *OECD Publishing* 36, available here.
[3] Information Commission Office (UK), *Age Appropriate Design: A Code of Practice for Online Services* (2 September 2020), Annexure B, available here.
[4] Ibid.
[5] OECD Report, 36-37.
[6] Information Commission Office (UK), *Age Appropriate Design: A Code of Practice for Online Services* (2 September 2020), Foreword, available here.

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, which the Government agreed to in principle.[7] We also suggest consistency with the Online Safety (Basic Online Safety Expectations) Determination 2022.[8]

Best interests of the child

Determining the developmental capacities of different age cohorts and the risks inherent in different age assurance methods can be a complex undertaking. We support a principles-based approach that is as consistent as possible with existing Australian online safety laws. We also support introducing an overarching "best interests of the child" principle in the Code. This is consistent with Article 3 of the United Nations Convention on the Rights of the Child, to which Australia is a signatory.[9]

If an APP entity provides a service that is likely to be accessed by children, the best interests of the child should be a primary consideration that has to be balanced against other interests.[10] This should be the case even when children are not the intended primary users of the online service.

We suggest that the Code specifies that the Australian Privacy Principles (**APPs**), as they apply to children, should be implemented through the lens of what is in the best interests of the child. 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. This is consistent with section 26C(3)(a) of the *Privacy Act 1988*, which allows APP codes to "impose additional requirements … so long as the additional requirements are not contrary to, or inconsistent with" APPs.[11]

1. Scope of services covered by the Code

1.1 Are there additional APP entities, or a class of entities, that should be covered by the Code? Please provide reasons or evidence to support your view.

In addition to the APP entities set out by the Act, we suggest that consideration be given to clarifying that the following are included, or including APP entities that provide the following types of services:

- AI chatbots
- Online purchases
- Geolocation or GPS services
- Education providers

[7] Australian Government, *Government Response: Privacy Act Review Report* (Report, 2023) 26, available here.
[8] *Online Safety (Basic Online Safety Expectations) Determination 2022* (Cth).
[9] *Convention on the Rights of the Child,* opened for signature 20 November 1989, 1577 UNTS 3 (entered into force 2 September 1990) art 3.
[10] Information Commission Office (UK), *Age Appropriate Design: A Code of Practice for Online Services* (2 September 2020) available here; Proposal 16.5, Privacy Act Review Report (2023), available here.
[11] *Privacy Act 1988* (Cth) s 26C(3)(a).

Concerns have been raised in the media about AI therapy chatbots accessed by children, which have provided morally objectionable and alarming advice to users seeking therapy.[12] We suggest the Code explicitly includes AI chatbot services to avoid them being inadvertently excluded as a "health service provider", which they are not, given the chatbot behind the AI persona is not a human trained in counselling or psychotherapy or psychology. It is also unclear whether AI chatbot services fall under "relevant electronic service", given they do not facilitate communication between humans as messaging apps do. Given the high likelihood that personal information would be inputted into an online interaction with an AI chatbot, we suggest express inclusion of entities that provide this type of service.

We also suggest the Code clarifies that online purchase services are included, as it is unclear whether they fall under "designated internet service". More benign examples are online shopping platforms that inevitably require personal information such as a home address. More harmful examples are platforms that offer potentially illegal items for purchase, such as alcohol or weapons.

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 helpful to have clarity on whether they fall under the types of services prescribed by the Act.

While schools generally do not provide an internet service, we believe education providers should be covered by the Code. We recognise that private or independent schools and education providers with an annual turnover of over $3 million are APP entities. However, we suggest consideration be given to covering all schools under the Code. Schools often use internet services and communication apps on a child's behalf through posting a child's personal information on public online platforms. This includes regularly posting photos of children, along with their names, classes, and achievements, or entire school newsletters on social media.

Many parents are signing the school consent forms without 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 means their children would be excluded from group photos. 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 the feedback from OAIC's initial consultation with children, where "Some children also raised that consent provided by a child's school on behalf of them should be critically analysed and should not override the child's consent."[13]

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

[12] Andrew Chow and Angela Haupt, 'A Psychiatrist Posed as a Teen with Therapy Chatbots. The Conversations Were Alarming', *Time* (online, 12 June 2025) available here; April McLennan, 'Young Australians using AI bots for therapy', ABC News (online, 18 May 2025), available here.
[13] Reset.Tech Australia, Consultation with young people about children's Online Privacy Code and consent and agency, 5.

APP specific questions

4. APP 1 – open and transparent management of personal information

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

Given children's evolving developmental capacities, we reiterate our earlier suggestion that the age threshold for capacity for consent in children should be consistent with the age restrictions in online safety laws.

Privacy policies for adult users already tend to be lengthy and technical. We suggest that 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, to facilitate consistency and harmonisation of communicating privacy policies to children.

We refer the OAIC to the child-friendly privacy policies of the following companies:

- Lego: https://kids.lego.com/en-au/legal/privacy-policy
- Paramount: https://privacy.paramount.com/en/childrens-short?r=www.nick.com

4.2 How should APP entities ensure APP1 obligations are met when their services are used by both adults and children, particularly when children are not the intended primary users?

We suggest that the Code should provide specific guidance that drills down on how the APPs should be applied in a children's online safety context, similar to the level of specificity provided by the current APP Guidelines.

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

As a general principle, we support consistency in implementation. If certain APP entities have children accessing their service as well as adults, the vulnerability of children should be prioritised in the "reasonable steps", and if this results in stricter internal practices, procedures and systems, these should cover both children's and adult's personal information. That is, as soon as there is the likelihood that children may access the service, the "best interests of children" should be the main 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. There should not be a requirement for two sets of practices for handling the information of adult and child users.

We suggest that the Code provides specific guidance on openness and transparency. In the context of schools, for example, the "reasonable steps" should include consideration as to whether social media is an appropriate forum to post regular updates about the students and how internal procedures could be improved to minimise giving children's personal information to a public online platform.

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?

In our view, the current APP standard does not change, but the communication should be tailored to an audience that involves children.

APP 2 – anonymity and pseudonymity

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?

Our general position is that data minimisation should be prioritised, so APP entities need to consider whether the information collected is necessary. For example, is it necessary to collect details about a child's residential address if the service is simply a messaging service?

Whether a child can be easily identified also depends on the number of 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

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?

In our view, if the service can be delivered with less information, the APP entity should collect less information. We suggest consistency with the UK Code that only "the minimum amount of personal data should be collected and retained". 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.[14]

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?

In our view, collection of children's personal information may be lawful, but not fair. We note that the Government agreed to a "fair and reasonable test" in its response to the *Privacy Act Review Report*,[15] which may form tranche 2 of the privacy law reform.

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

The collection of children's personal information would not be fair if providing personal information is the only way to gain initial or continued access to the service.

It is also 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

[14] Information Commission Office (UK), *Age Appropriate Design: A Code of Practice for Online Services* (2 September 2020) available here.
[15] Australian Government, *Government Response: Privacy Act Review Report* (Report, 2023) 8, available here.

graphical interfaces. Many 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, and unfairly, persuasive.

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

As stated above, we believe consent is a deficient model for the collection of 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.

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 such as ethnicity or criminal record would not be "reasonably necessary" for a service accessed by a child.

7. APP 4 – dealing with unsolicited personal information

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

Currently, if an APP entity receives personal information 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.

In our view, 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, recognise their vulnerability, and the need for stricter safeguards. It may reduce risks of misuse or mishandling of sensitive information. We recognise that this approach may create a stricter standard than what currently applies under APP 4, and could lead to confusion or inconsistency in compliance practices, and challenges for entities trying to reconcile APP 3 and APP 4 obligations. However, we note again that section 26C(3)(a) of the *Privacy Act* allows APP codes to impose additional requirements that are consistent with the APPs. This is also consistent with our view above that the minimum amount of data should be collected and retained, which the collection of unsolicited information would appear to be at odds with.

As an alternative to enforcing automatic destruction, a clearer framework or guidance 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 promotes transparency and accountability in handling children's personal information.

In relation to how an APP entity may identify that the unsolicited personal information relates to children, we suggest methods such as assessing the content, language cues and identifiers, the metadata, or the source of the information (e.g. school or kids' services).

If there is any doubt, we prefer 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 the information appropriately, in the best interests of the child.

8. APP 5 – notification of the collection of personal information

See our response to Question 4.1.

9. APP 6 – use or disclosure of personal information

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?

In our view, use or disclosure of children's personal information *only* for the primary purpose provides strong protections to vulnerable individuals, simplifies compliance – since there is no need to assess the exceptions or "reasonable expectations" of a child at any age, reduces the risk of misuse or further disclosure, and aligns with the principle of "best interests of the child".

However, we acknowledge the legal exceptions to APP 6 and the complexities involved in identifying if it is indeed personal information of a child. We also recognise other countries' allowance of disclosure for secondary purposes based on consent.[16]

In the alternative, we suggest a presumption of non-disclosure unless disclosure is required by the law or clearly justified for compelling reasons. If an APP entity must, in the limited circumstances, use children's personal information for a secondary purpose, we suggest requiring APP entities to:

- 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
- implement a flagging or data filter system to identify any child related personal information.

We believe a higher standard of protection should be applied, such that children's personal information should not be used or disclosed for any secondary purpose, including targeted marketing. In our view, that should be the default standard for all APP entities.

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?

We believe a higher standard of protection should be applied such that children's personal information should not be used or disclosed for any secondary purpose, as what a child can reasonably expect as a secondary purpose would vary greatly not only by age cohorts, but also by environmental and social-economic factors, education, exposure to social media, digital maturity, and experiences online.

[16] OECD, 'The Legal and Policy Landscape of Age Assurance Online for Child Safety and Well-being' (2025) *OECD Publishing* 36, available here.

In our view, there should be little reason for secondary disclosure, and it would be in the best interests of the child for there to be a default position that there is no secondary use or disclosure without informed consent.

10. APP 7 – direct marketing

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?

For the reasons stated above, children's personal information should not be used or disclosed for targeted marketing. Children's data should not be for sale. Further, children do not have the adequate capacity to understand how far their data will travel.

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?

The opt-out model is inappropriate for children, and in our view, 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 after a certain age.

11. APP 8 – cross-border disclosure of personal information

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?

We suggest that it is in the best interests of a child not to transfer their personal information to overseas jurisdictions, particularly given the risk that other countries may not offer equivalent protections.

The risk of cross-border disclosure often stems from a failure to conduct a proper Privacy Impact Assessment. In many cases, by virtue of the technology platforms being used (even where the collection entity and the user are both Australian based), personal information will be transmitted overseas. Further, many organisations and government agencies may fail to conduct thorough exercises to understand exactly how data flows are occurring, and instead seek to rely on contractual prohibitions which may not mirror the practical reality. This not only leads to unrealistic expectations about data handling, but also leads to unnecessary tension between service providers and APP entities as they focus on the supposed location of the personal information, rather than how it is being protected, and how individuals can enforce their rights under the *Privacy Act*.

We suggest that one solution might be implementing model clauses for data transfers, which will at least bind the parties, and perhaps allow an individual user to enforce rights under those model clauses, given the phased pace of legislative reform.

12. APP 10 – quality of personal information

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 developmental and digital engagement stages?

Applying data minimisation across APP 10 will assist with protecting children's information across the developmental and digital engagement stages. 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.

We suggest that the Code requires 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.

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 section 26C(3)(a).

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?

Given the dynamic nature of a child's life, 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. Photos and data posted by the school should be deleted at a minimum after the child finishes school, or better, deleted at the end of each age cohort, for example, every three years (Years K-2, 3-6, 7-9, and 10-12). 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 GDPR.

If you have any queries about the items above, or would like further information, please contact Mimi Lee, Policy Lawyer, on 02 9926 0174 or mimi.lee@lawsociety.com.au.

Yours sincerely,

Jennifer Ball

Jennifer Ball
President