Queensland Law Society

Law Society House, 179 Ann Street, Brisbane Qld 4000, Australia
GPO Box 1785, Brisbane Qld 4001 | ABN 33 423 389 441
[redacted] | [redacted] qls.com.au

Office of the President

24 July 2025

Our ref: KS:PDTIP

Dr James Popple
Chief Executive Officer
Law Council of Australia
Level 1, MODE 3
24 Lonsdale Street
Braddon ACT 2612

By email: [redacted]

Dear Dr Popple

Children's Online Privacy Code: Issues Paper

Thank you for the opportunity to provide feedback on the issues paper, Children's Online Privacy Code (Issues paper).

This response has been compiled with the assistance of the QLS Privacy, Data, Technology and Intellectual Property Law Committee, whose members have substantial expertise in this area. The submission has also been reviewed by members of our Children's Law Committee.

Background

QLS supports the development and registration of a Children's Online Privacy Code under the *Privacy Act 1988* (Cth) (the Code) to strengthen privacy protections for children online.

Broadly, the Code should seek to protect children from arbitrary or unlawful interference with their privacy when using online services, consistent with Article 16 of the Convention on the Rights of the Child.[1] In developing the Code, there is also an opportunity to encourage harmonisation with current international regulatory approaches, enabling businesses to align with, and be supported in complying with, increasing regulatory responses to these issues.

The Code also plays an important role in complementing the existing eSafety regime, including the social media age restrictions.

What Children and Young People have said

Children should be given the opportunity to express their views in relation to matters that will affect them.

We note consultations led by the Office of the Australian Information Commissioner (OAIC) have placed children and young people at the centre of the development of the Children's Online

[1] Convention on the Rights of the Child | OHCHR

Privacy Code.[2] These consultations have identified several privacy issues that young people consider especially important.

We support ongoing consultation with children and young people, as well as their parents and carers. QLS also supports funding for education and accessible resource initiatives to support their awareness and decision making when interacting with online services.

Our submission raises the following issues for consideration in preparing the Law Council's response.

Issue 1: Scope of Services Covered by the Code

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

The United Kingdom's Age appropriate design code (the UK Code), established a broad framework that encompasses a wide range of online services that process personal data and are likely to be accessed by children.[3] 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.[4]

As foreshadowed in the Explanatory Notes to the *Privacy and Other Legislation Amendment Act* 2024 (Cth) (Privacy and Other Legislation Amendment Act), in principle, we consider the Code should align with the broad scope established by the UK Code. Other jurisdictions have also adopted the UK approach.[5] Adopting this as a starting point for the Code would support international alignment and harmonisation. A comparable approach in Australia would also support compliance for businesses operating across multiple jurisdictions.

However, we would caution that as the UK model has been in place since 2021, the OAIC should publish its assessment of learnings from the UK. For example, our members are of the view 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 model provided greater specificity, so companies and legal practitioners have clear guidance on compliance.

The UK Code is relatively high-level and may present difficulties for some entities seeking to operationalise the requirements in practice. Since 2021, there have also been significant shifts in public understanding and expectations around privacy, with recognition of the particular vulnerability for children online, highlighting the need for more detailed, practical requirements.

By way of example, the UK has recently legislated new requirements through its *Data (Use and Access) Act 2025*, introducing an explicit requirement for online services likely to be accessed by children to consider children's needs when determining how their personal information is used.[6] The UK Information Commissioner is currently reviewing and updating

---

[2] Sunshine and double rainbows – building a better online environment for children and young people | OAIC

[3] This includes online products or services (including apps, programs, websites, games or community environments, and connected toys or devices with or without a screen): About this code | ICO

[4] Services covered by this code | ICO

[5] Fundamentals for a Child-Oriented Approach to Data Processing_FINAL_EN.pdf; Bill Text - AB-2273 The California Age-Appropriate Design Code Act.

[6] Data (Use and Access) Act 2025: data protection and privacy changes - GOV.UK

guidance on the UK Code to reflect these new legal obligations, following the Act's commencement on 19 June 2025.[7]

This ongoing reform process highlights the importance of regulatory frameworks that are both robust and guide effective compliance.

1.1 Additional entities which should be covered

The Privacy and Other Legislation Amendment Act sets out that the Code will apply to APP entities if the entity is a social media service, relevant electronic service or designated internet service (within the meaning of the *Online Safety Act* 2021). We note the OAIC may specify additional entities, or a class of entities required to comply with the Code.

The Society recommends there should be clear and comprehensive guidance on which entities are intended to be captured in this regard.

In addition, QLS suggests the OAIC should consider the application of the Code to the following entities.

Entities captured by pending second tranche Privacy Act reforms

Firstly, we note there are recommendations from the Privacy Act Review which have not yet progressed in the legislative agenda. Specifically:

1. Codification of current OAIC guidance that valid consent must be given with capacity (noting an entity may assume an individual over the age of 15 has capacity, unless there is something to suggest otherwise);
2. Right to erasure (discussed below); and
3. Eventual removal of the small business exemption.

If the small business exemption reforms are progressed, entities that are currently outside the scope of the Privacy Act could become subject to the Code if they meet the relevant thresholds.

QLS suggests that these reform proposals will need to be considered with the potential Code changes in mind.

Additionally, QLS suggests that third parties who require, recommend, or approve the use of a service covered by the Code should be obliged to ensure Code compliance before making such recommendations or requirements.

EdTech, AI and data brokers

The use and reliance on education technologies (or "EdTech") by Australian schools markedly increased during the COVID19 pandemic and remains a key component of the digital classroom.[8] Despite the benefits of EdTech for schools and children, the collection, use and disclosure of children's personal information through EdTech has significant implications for children's privacy, particularly given their vulnerability to privacy risks and harm online.[9] The Code must adequately address these risks.

---

[7] For the public | ICO
[8] Evaluating the evidence for educational technology - Part 2
[9] Assessing the privacy of digital products in Australian schools: Protecting the digital rights of children and young people - ScienceDirect

In particular, the increasing use of artificial intelligence (AI) and data brokering within EdTech and other online service platforms presents additional risks for children, such as 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.[10]

Internationally, the UK has taken steps towards the development of specific standards for EdTech, AI, and Automated Decision-Making (ADM) under the *Data Use and Access Act 2025*, with the government committing to develop codes of practice specifically for these technologies.[11]

QLS recommends that the OAIC consider adopting similar risk-based responses to address the potential harms children may face when using these technologies. QLS further recommends that guidance be given to education service providers, particularly schools, when procuring and using third party EdTech tools.

Interaction with State agencies and departments

Lastly, QLS has previously advocated for national consistency and whilst acknowledging constitutional limitations, suggests consideration be given to coverage of State Government agencies under the Code to align with this position. This may form part of discussions with the Council of Attorneys-General. This issue arises for example in the context of EdTech where a State or Territory education department mandates use of a particular service or application.

QLS recommends aligning State and Commonwealth privacy frameworks to ensure consistent protection of student privacy and data security in the use of EdTech.

Issue 2: What guidance or specificity is needed in the Code to support practical implementation?

2.1 When and how the Code should apply to Australian Privacy Principle (APP) entities

Best interests test

QLS supports best interest as a primary consideration of online services designed and developed for (and likely to be accessed by) children. However, we suggest a clear framework is needed for how businesses can operationalise the "best interests" test in their decision-making.

The UK Information Commissioner's Office (ICO) provides a useful resource in the form of the "Best interests of the child self-assessment", which offers practical guidance and assessment tools to help organisations evaluate and demonstrate how their online services align with the best interests of child users.[12] It would be of assistance for the OAIC to develop or endorse similar self-assessment tools and guidance to assist businesses in embedding the best interests principle into the design, development, and management of digital services likely to be accessed by children. We consider it important to ensure children have access to online services, and that regulatory uncertainty does not result in services not being made available. Clear guidance from the OAIC will be key to ensuring this.

[10] Roundtable on targeted advertising and the COPC: raw memo
[11] The Data Use and Access Act 2025 (DUAA) - what does it mean for organisations? | ICO
[12] Best interests of the child self-assessment | ICO

"Likely to be accessed" test

Whilst in some circumstances this threshold will be easily ascertainable, given the nature of online service accessibility, especially for older children, for some services, the test will be less clear.

We suggest a list of non-exhaustive factors will be of assistance, consistent with the legislative intention, however the Code should also emphasise proactive assessment by service providers regardless of whether they are child targeted.[13] If age cannot be reasonably determined, we suggest the Code's protections should reasonably be applied to all users.

Guidance for Health service provider exclusion

The exclusion of health service providers under the Privacy and Other Legislation Amendment Act from the Code is broad. The intention, as set out in the Explanatory Notes, is to ensure that the Code does not become a barrier to providing essential health services to children.[14] This approach is intended to align with the UK Code in preserving access to necessary health services for children.[15]

Guidance from the OAIC clarifies that 'health service' providers include online health services such as counselling, advice, and telehealth.[16] However, more general health, fitness, or wellbeing apps or services may still be covered by the Code, depending on their functions and offerings.[17]

QLS recommends that the exclusion for health service providers 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 protections, including some that may not be providing essential health services. We suggest that the exclusion should be narrowly defined and consistent with the legislative intention.

Even if health services are excluded from the Code, there is a strong argument for considering the application of certain aspects of the Code, particularly those relating to the concept of consent, to health service providers. For example, the principles around consent are fundamental to protecting children's privacy and autonomy, and it may be appropriate for these requirements to apply even where a broader exclusion exists.

2.2 What steps should captured APP entities be required to take?

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 evolving risks and privacy defaults where vulnerabilities are known or emerge.

Privacy by design

At a broad level, QLS supports high privacy defaults for children, reflecting both feedback from young people and the approach taken in the California Age-Appropriate Design Code (CA

[13] EN at p 41. JC014082.pdf;fileType=application/pdf
[14] EN at p 41. JC014082.pdf;fileType=application/pdf
[15] JC014082.pdf;fileType=application/pdf 85 b I
[16] JC014082.pdf;fileType=application/pdf p 42
[17] Guide to health privacy

AADC), which requires businesses to configure default privacy settings for children to the highest level of privacy available unless a compelling reason exists to do otherwise.[18]

Child-Specific Privacy Impact Assessments

QLS further recommends that any online product, service, or system likely to be accessed by children require child-specific privacy impact assessments. This approach is consistent with the CA AADC and the UK Code's requirement for Data Protection Impact Assessments (DPIAs) before offering services likely to be accessed by children.[19]

Consent

As referenced above, Proposal 16.2 of the Privacy Act review relates to capacity and consent. It will also be important for consent to be voluntary, current and specific, and informed.

We suggest clarity will be needed as to what valid consent will mean in the Code. Some members support additional consent requirements in certain circumstances. In particular, the imposition of strict consent requirement for all uses and disclosures which may now, or in the foreseeable future involve direct marketing (see discussion below) or biased decision making.

A relevant entity should also be required to satisfy consent has been validly obtained.

We also 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 law and beyond the scope of the Privacy Act or Code. Unless they are 'contracts for 'necessaries' may not be enforceable against a person who is under 18.

Privacy Policies and Collection Notices for Children

Privacy policies and collection notices directed at children should be clear, concise and tailored to the relevant age group.[20] This will also be important when seeking consent.

To aid comprehension, the use of standardised templates, layouts, terminology, and icons is recommended, consistent with Proposals 10.1, 10.3, and 16.3 of the Privacy Act Review Report.[21]

Despite this, QLS 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 layouts cannot transform a child into an adult. Such an approach fails to reflect the fact that consent is likely to arise where a large corporation is seeking to harvest data. Even if consent is sought in a clear and understandable way, it is difficult to see how the power imbalance could ever be overcome.

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

---

[18] Today's Law As Amended - AB-2273 The California Age-Appropriate Design Code Act. S 1(8)
[19] The California Age-Appropriate Design Code Act - California Lawyers Association; 2. Data protection impact assessments | ICO
[20] OAIC Children's Online Privacy Code Executive Summary
[21] Privacy Act Review Report

Online services should not be permitted to shift the burden of determining whether the service is "privacy safe" to children through a policy and notice; the service provider should still be required to ensure the service meets the requirements of the Code and the APPs more generally.

Erasure rights

Processes for requesting the deletion of personal data must be simple, age-appropriate, and responsive to the needs of children.[22] Entities should ensure that children and their guardians can easily understand and navigate these processes, providing clear guidance and support throughout. This approach aligns with the recommendations from the Privacy Act Review, which emphasise the importance of making privacy rights accessible and actionable for children and their families.[23]

Issue 3: Should age range-specific guidance be provided?

UNICEF's guidelines recommend implementing age-appropriate privacy settings and controls, recognising the importance of adapting protections to suit different age groups and abilities.[24] There is a significant difference in digital literacy between a young person aged 12-15, and a child under the age of 5.

Additionally, the Code should consider the needs of children with disability or specific vulnerabilities which companies should be alive to. This necessarily involves engagement with those sectors and people with lived experience throughout the consultation process.

QLS also suggests a risk-based approach with specific requirements to address high-risk areas, such as direct marketing, particularly online targeted advertising, to children.

However, we emphasise that the purpose of such age-appropriate settings and controls should be to empower the user. There remains the risk that online businesses may see such requirements as minimum thresholds which, once met, will allow them to exploit children's data.

Issue 4: High risk practices

Targeted advertising

QLS supports a strict approach to targeted advertising directed at children in the Code. The Code should require explicit, specific, informed consent for both the collection and use of children's data for targeted advertising and should prohibit direct marketing to children unless it is demonstrably in their best interests and subject to clear, time-limited consent that does not continue once a child turns 18. This aligns with previous QLS submissions advocating for robust restrictions on direct marketing to minors.

Direct marketing

APP 7 Direct marketing, does not apply to the extent that the *Do Not Call Register Act 2006* (which regulates outbound telemarketing phone calls, unless exempt), the *Spam Act 2003*

[22] Reset.Tech Australia, Results from a survey with young people about the Children's Online Privacy Code, page 7
[23] Privacy Act Review Report 2022 Recommendation 16.5
[24] Online privacy checklist for parents | UNICEF Parenting

(which regulates commercial electronic messages such as email, text messages and instant messages), or any other legislation prescribed by the regulations apply.

This may mean that the Code (if its application is linked to APP 7) may not apply to direct marketing activities regulated under the Spam Act or Do Not Call Register Act.

QLS suggests such carve-out, if applicable, is inappropriate and that all direct marketing practices to children should be captured by the Code.

Issue 5: Implementation and compliance

Practicality and workability

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. The 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.[25] However, the trial also highlights concerns about some providers collecting and retaining more personal data than necessary, which raises privacy risks.[26] QLS is also aware of some testing resulting in inconsistent results.

As Australia awaits the final outcomes of its age assurance technology trial, 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 technology across different regulatory regimes to ensure clarity and fairness for both users and service providers.

Compliance and enforcement

Breaches of the Code may result in enforcement and potentially significant penalties under the eSafety and privacy regimes.

However, barriers to enforcement, such as jurisdictional challenges with overseas platforms and the complexity of monitoring harmful content, have been acknowledged.[27]

Ultimately, clear guidance in the Code must be supported by proactive compliance support. Ongoing education, industry engagement, and transparent enforcement by regulators are essential to ensure the Code is effective in protecting children online.

Issue 6: Overlay of other legislative reform proposals

Digital duty of care

Finally, QLS recommends the Code be drafted with the existing legislative landscape in mind including the second tranche of the Privacy Act review reforms and commitments to a digital duty of care for digital platforms. We acknowledge the Federal Government's commitment to implementing a digital duty of care.[28] We also recognise recent initiatives, including the

[25] News-Release-Preliminary-Findings-for-publication-20250620.pdf
[26] News-Release-Preliminary-Findings-for-publication-20250620.pdf p 6
[27] UK organisations stand to benefit from new data protection laws | ICO
[28] https://minister.infrastructure.gov.au/rowland/media-release/new-duty-care-obligations-platforms-will-keep-australians-safer-online

expanded penalty and enforcement regime under the Privacy Act and the establishment of minimum age requirements for social media platforms, as important steps toward enhancing online safety and accountability.

The Code may serve as a benchmark for determining whether minimum requirements have been satisfied. The degree of compliance with the Code, as well as corresponding regulatory responses, will also be important factors in assessing overall effectiveness.

If you have any queries regarding the contents of this letter, please do not hesitate to contact our Legal Policy team via policy@qls.com.au or by phone on [redacted]

Yours faithfully

[redacted]

Genevieve Dee
President