SUBMISSION · JUNE 2026

Children's Online Privacy Code

Scyne's submission to the Office of the Australian Information Commissioner on the exposure draft

About Scyne

Scyne provides professional services across critical sectors that serve the public interest. With three core practice areas, we bring deep sector knowledge and a collaborative mindset to every engagement. Our approach is technology-led and outcomes-driven - we combine strategic insight with digital innovation to help our clients solve complex challenges, modernise services, and deliver better outcomes for communities. This submission draws on our specialists across cyber security, risk, data governance, compliance, ethics and AI governance, and on our experience helping organisations turn privacy and security obligations into working practice.

Executive summary

Scyne supports the Children's Online Privacy Code. It reflects community expectations of control, transparency, fairness and accountability, and it sets the protections children need online.

Our main area for further consideration is implementation. The Code demands capabilities most organisations don't yet have end-to-end data lineage, data classification, consent traceability and lifecycle management.

Public and for-purpose organisations are furthest behind. Without practical guidance, realistic timeframes and alignment with existing frameworks, implementation will be inconsistent and the Code's intent will be lost in compliance activity.

The Code also raises a bigger question. Its protections aren't child-specific in substance. They reflect what most Australians want for their personal information at any age, which means individuals lose practical protections the day they turn 18. We encourage the OAIC to treat the Code as a template for broader privacy reform.

We make nine recommendations across four themes.

Our recommendations at a glance

Nine recommendations across four themes

Make it proportionate

- **1** Tiered, risk-based obligations
- **8** Phased rollout with clear timelines

Make it fit the system

- **2** Align with broader privacy reform
- **9** Co-regulate and keep consulting

Make it clear

- **3** Define best interests in practice
- **6** Risk-based age assurance

Make it practical

- **4** Privacy by design and by default
- **5** Standard templates and patterns
- **7** Transparency over profiling

Numbers refer to the recommendations detailed in this submission.

Our recommendations

After a careful reading of code, while Scyne is in broad agreement with the requirements, we have noted several recommendations we feel would help ensure the effective implementation and ongoing management of the code We have summarised these below. Details of these recommendations are included in our detailed section-by-section response in the Appendix of this document.

1. Adopt tiered, risk-based obligations

Not all services present the same risk to children. Services directed at children, accessed by children at scale, or built on high-risk practices such as profiling, geolocation and behavioural tracking should carry the strongest obligations. Scyne recommends stricter defaults, stronger transparency and tighter governance. OAIC guidance should set out the risk indicators, thresholds and worked examples.

2. Align the Code with broader reform

We recommend that the Code should operate cohesively with the Privacy Act reforms, the Online Safety framework and international codes such as the UK Age-Appropriate Design Code. Align definitions of child, consent and targeting, and reuse interoperable concepts like privacy by design. Misalignment means duplicated obligations and compliance complexity, particularly for entities operating across jurisdictions.

3. Define best interests of the child in practice

The best interests test is the right safeguard; however, it is Scyne's recommendation that entities be provided with decision-making frameworks, illustrative scenarios across industries, and the factors to consider such as age, maturity, context of use and potential harm. Without them, application will be inconsistent, or so conservative it blocks beneficial services.

4. Require privacy by design and by default

Syne's recommendation is that digital services accessed by children should default to the most privacy-protective settings, limit collection to what's necessary and proportionate, and disable profiling, tracking and content personalisation by default. Privacy impact assessments should be standard for high-risk features, with ongoing review of whether data practices remain fair and, in the child's, best interests.

5. Publish standard templates and design patterns

The OAIC should publish standard patterns for child-friendly privacy notices, consent mechanisms and privacy controls: layered notices, visual aids and age-specific formats. Develop them with child development experts. Standardisation lifts children's comprehension and cuts design cost for every entity.

6. Take a risk-based approach to age assurance and consent

Current age verification technology has limits. Prescriptive requirements create new privacy risks and will be infeasible for some entities. Scyne recommends that the Code should let entities adopt proportionate solutions, recognise varying certainty in age estimation, and provide guidance on when parental involvement is necessary.

7. Strengthen transparency over algorithms and profiling

To help strengthen the need for transparency, it is Scyne's recommendation that children and their guardians should know what data feeds automated decisions, recommendations and profiling, how outcomes affect them, and what controls they hold. Explanations must be accessible and matched to the child's comprehension.

8. Phase the rollout

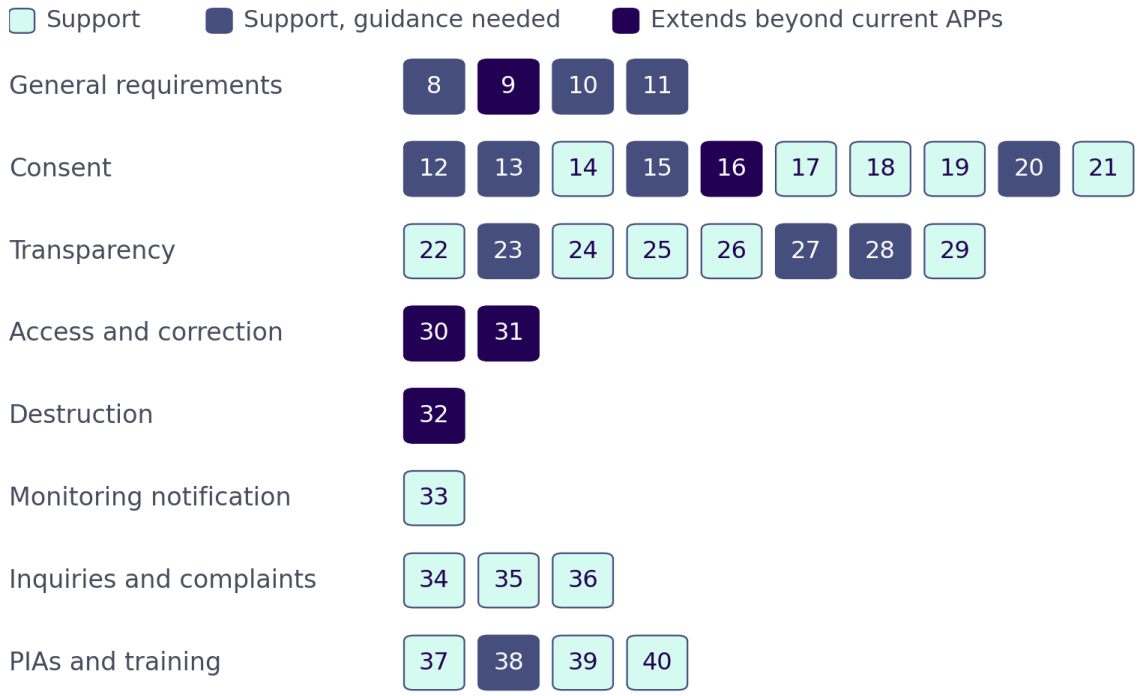
It is Scyne option that the code should be implemented in stages: high-risk obligations first, clear transition timelines and milestone-based compliance expectations. This gives entities time to build the underlying capability and gives the OAIC room to refine guidance from early feedback. It will also be important to ensure there is sustained focus from the OAIC on ensuring organisations are meeting the code requirements beyond the initial phases.

9. Co-regulate and keep consulting

Develop and refine the Code with industry, child rights and welfare experts, regulators and the community, so it stays fit for purpose as technology and behaviour change.

Our position on the draft Code

We reviewed all 33 sections of the exposure draft. We support 17 outright. The remaining 16 fall into two groups: sections that need practical guidance to land, and sections that extend beyond the current Australian Privacy Principles and need a clear policy rationale and alignment plan.



Numbers are section references in the exposure draft. Commentary follows for highlighted sections only.

Where guidance is needed

Eleven sections set the right obligation but leave entities guessing on how to meet it. The common fix is the same: worked examples and proportionate implementation guidance from the OAIC.

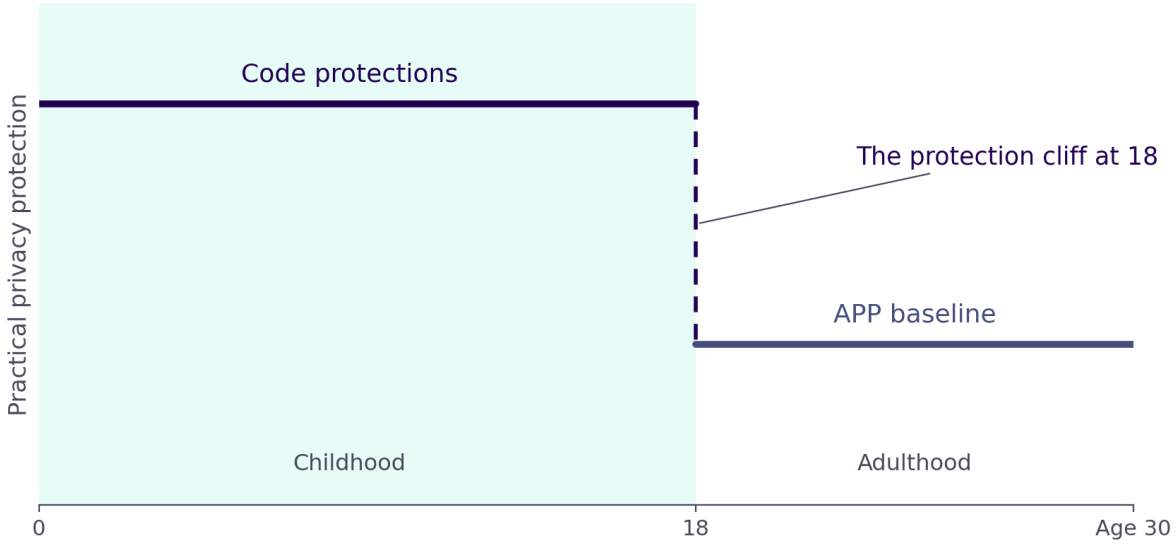
- **Age and identity (ss 8, 13, 20).** Entities need to know what reasonable steps for age assurance look like, and how to run parental consent and child assent processes without over-collecting. Worked examples should show how to balance accuracy against data minimisation.
- **Best interests (ss 10, 11).** The test applies to collection, use and disclosure. Entities need criteria and examples to apply it consistently and defensibly.
- **Consent scope and lifecycle (ss 12, 15).** Confirm whether consent is required for all collection of children's personal information or only in circumstances consistent with the APPs. Set proportionate expectations for consent refresh at scale.
- **Age-appropriate communication (ss 23, 27, 28).** Define what age-appropriate means in practice for privacy policies, access responses and information requests, so implementation is consistent across the ecosystem.
- **Privacy impact assessments (s 38).** Update the existing OAIC PIA templates with child-specific guidance rather than leaving entities to build their own.

Where the Code extends beyond the current APPs

Five sections give children stronger rights than adults hold today: prescriptive collection controls (s 9), mandated consent refresh timeframes (s 16), stronger access and correction rights (ss 30, 31) and a right to request destruction (s 32). We don't oppose them. But each needs a stated policy rationale, and the OAIC should explain how they interact with the wider privacy framework. They also create the problem below.

The protection cliff

The Code's protections reflect what most Australians want for their personal information at any age: genuine control, plain communication, current consent and the ability to have information destroyed. Under the draft, a person holds these rights at 17 and loses most of them at 18.



Practical protections under the Code end at adulthood, dropping to the APP baseline.

That cliff matters for two reasons. First, it will be visible. A generation raised on clear consent and meaningful control will notice when it disappears. Second, it's an opportunity. The Code can serve as the working template for broader Privacy Act reform, so protections mature with the individual instead of expiring.

Authors

James Calder, Managing Director and National Cyber and Technology Risk Leader

Peter Johnson, Managing Director, Cyber and Technology Risk

Richard Harris, Manager, Cyber and Technology Risk

Tadiwa Muwidzi, Associate, Cyber and Technology Risk

Appendix – Code Section - Scyne Comments

Division 1 – General Requirements

Code Section	Scyne Response
8 - Ascertaining the age of end-users of an entity's service	Scyne supports this provision. Further guidance would help clarify what "reasonable steps" looks like in practice, particularly as organisations will need to balance accurate age assurance with data minimisation.
9 - Entities may collect etc. personal information about a child by default only if strictly necessary	Scyne supports this provision. However, the more prescriptive requirement for technical and organisational controls may increase compliance complexity, and it is worth considering whether further guidance within the existing framework could achieve the same outcome with greater flexibility.
10 Collection of personal information about a child must be consistent with best interests of the child	Scyne supports this provision. Further guidance on how to apply the best interests test in practice, including clear criteria or examples, would support more consistent and practical implementation.
11 Use or disclosure of personal information about a child must be consistent with best interests of the child	Scyne supports this provision. As with Section 10, additional guidance would help organisations assess and demonstrate how specific uses or disclosures meet this requirement in practice.

Division 2 – Consent

Code Section	Scyne Response
12 Purpose of this Division	Scyne supports this provision. It would be helpful to clarify whether consent is required for all collection of children's personal information under the Code, or only in circumstances consistent with the Australian Privacy Principles, as this has implications for how organisations design their data handling processes.
13 Consent given by child or person with parental responsibility	Scyne supports this provision. In practice, it introduces additional complexity because organisations will need to determine age, manage parental consent processes, and provide age-appropriate notices. Guidance on applying these requirements in a proportionate and practical way would be helpful.

Code Section	Scyne Response
14 Consent must be voluntary	No comment.
15 Consent must be informed	Scyne supports this provision. However, managing consent duration and refresh processes may increase operational complexity, particularly for large-scale services, and organisations would benefit from guidance on proportionate implementation.
16 Consent must be current	Scyne supports this provision. However, the requirement to refresh consent within defined timeframes goes beyond existing expectations under the Australian Privacy Principles and may introduce additional operational overhead. Guidance on managing consent lifecycle requirements in a practical and proportionate way would assist implementation.
17 Consent can be withdrawn	No comment.
18 Consent must be specific	No comment.
19 Consent must be unambiguous	No comment.
20 Assent of child under 15 years must be obtained in certain circumstances	Scyne supports this provision. In practice, it introduces additional complexity for organisations in identifying age, managing parental consent, and capturing assent. Guidance on implementation in a proportionate and practical way would be helpful.
21 Consent must not be obtained by coercion etc.	No comment.

Division 3 – Transparency

Code Section	Scyne Response
22 Purpose of this Division	No comment.
23 APP privacy policy requirements	Scyne supports this provision. However, developing and maintaining tailored materials may increase operational effort, and organisations would benefit from guidance on how to implement these requirements in a proportionate and practical way.

Code Section	Scyne Response
24 Notification of the collection of personal information	No comment.
25 Review of privacy practices etc.	No comment.
26 Consent to cross-border disclosures	No comment.
27 Accessing personal information	Scyne supports this provision. Further guidance on what "age appropriate" looks like in practice would support more consistent implementation.
28 Right to request information about handling of personal information	Scyne supports this provision. However, the scope of information required may increase operational complexity, and organisations would benefit from guidance on how to respond in a proportionate and practical way.
29 Opting out of direct marketing	No comment.

Division 4 - Access to, and correction of, personal information about children

Code Section	Scyne Response
30 Dealing with requests for access to personal information about children	Scyne supports this provision. However, the more prescriptive requirements go beyond current expectations under the Australian Privacy Principles and may result in stronger access rights for children than adults, raising a broader question about alignment with the wider privacy framework.
31 Dealing with requests to correct personal information about children	Scyne supports this provision. As with Section 30, the more prescriptive approach may create divergence from existing requirements under the Australian Privacy Principles and highlights the need for alignment across the broader privacy framework.

Division 5 – Destruction of personal information about children

Code Section	Scyne Response
32 Request to destroy personal information about a child	Scyne supports this provision. However, introducing a general right to erasure goes beyond current obligations under the Australian Privacy Principles and may increase implementation complexity. Guidance on how organisations should assess and respond to these requests in practice would assist implementation.

Division 6 - Notification requirements for control or monitoring mechanisms

Code Section	Scyne Response
33 Notification of mechanisms that monitor or control service use or monitor geolocation	No comment.

Division 7 – Making inquiries and complaints

Code Section	Scyne Response
34 Purpose of this Division	No comment.
35 Information about children's privacy rights	No comment.
36 Child-friendly inquiry and complaints processes	No comment.

Division 8 - Privacy impact assessments and privacy education and training

Code Section	Scyne Response
37 Purpose of this Division	No comment.
38 Privacy impact assessments	Scyne supports this provision. Consideration should be given to updating existing OAIC templates or providing child-specific guidance to support consistent and practical implementation.
39 Register of privacy impact assessments	No comment.

Code Section	Scyne Response
40 Privacy education and training	No comment.