Submission in response to the Exposure Draft of the Children's Online Privacy Code

1. About DLC Legal

DLC Legal is a boutique provider of virtual and onsite legal, commercial, strategic sourcing, procurement and contract management services to State and Commonwealth government and private industry clients. We specialise in ICT and cyber security law, and our lawyers possess a deep understanding of the complex mosaic of the technology and digital legislative landscape. Our expertise extends to advising a diverse array of clients, ranging from emerging tech startups to established multinational corporations, on a broad spectrum of technology and cyber-related legal issues. This includes online safety, privacy, Artificial Intelligence (**AI**), data protection, governance and compliance with local and international cyber security standards, breach response and notification requirements, and the management of cyber risks in commercial contracts. We are proactive in supporting and assisting our clients to navigate the intricacies of the legislative framework, to safeguard their digital assets and intellectual property, while ensuring their operations align with current and emerging legal frameworks. DLC Legal is committed to being at the forefront of technological advancements and legislative changes and we understand the critical importance of online safety, in particular with respect to safeguarding the integrity of the personal information of children in today's interconnected world.

2. Executive summary

DLC supports the continuous improvement of children's online privacy and safety, and we consider that a dedicated Children's Online Privacy Code (**Code**) has potential to provide meaningful, practical standards that complement existing obligations under the *Privacy Act 1988 (Cth)* (**Privacy Act**) and the Australian Privacy Principles (**APPs**).

However, the exposure draft of the Code raises material social, technical and legal risks, particularly around age assurance, profiling, deidentification, consent architecture, enforcement, and interaction with the *Online Safety Act 2021 (Cth)* (**OSA**) and existing Privacy Act settings.

With some refinement, the Code has the potential to materially lift baseline privacy protections for children while maintaining a workable compliance pathway for regulated entities. Specifically, DLC proposes the following key recommendations for priority reform:

1. *Scope and interaction with other regimes*
   Clarify scope and boundary questions for mixed-audience and enterprise services, and include an express cross-reference confirming that compliance with OSA safety-by-design obligations does not displace obligations under this Code.

2. *Best interest test*
   Clarify that 'best interests of the child' is an objective standard, that child privacy/safety interests should prevail where in conflict with commercial interests, and provide non-exhaustive examples of practices generally inconsistent with the test (including deep fakes, exploiting vulnerabilities and sensitive-data manipulation or advertising).

3. *Age assurance standards*
   Adopt a clear hierarchy of age-assurance methods that prioritises privacy-preserving methodology; treat biometrics as a last resort; and prohibits repurposing of biometric age-assurance data (including for personalisation, filters, profiling, or LLM / AI model training). Encourage OAIC benchmarks (for example with respect to error rates, bias testing).

4. *Profiling and commercial optimisation*
   Clarify to make it clear that profiling to exploit children's vulnerabilities is inconsistent with the best interests of the child. Require Privacy Impact Assessments (PIAs) to include a child-impact assessment of profiling. Specifically, the Code should make it explicit that, when an organisation does a Privacy Impact Assessment (PIA) for a service that uses profiling (building a model of a child's attributes, preferences or behaviour) or recommendation systems (algorithms that rank, curate, or suggest content/contacts/features), the PIA must specifically assess how those systems are likely to affect children, not just whether the data handling is "lawful" in a narrow sense.

5. *Deletion not deidentification*
   For destruction requests:

a. The default position should be deletion rather than deidentification unless a clearly defined exception applies.
b. *organisations must not be permitted to treat broad categories of analytics or "nice to have" data as necessary*. 'Strictly necessary' should *not* cover things like general product analytics, engagement optimisation, advertising measurement, or model training, merely because they are useful to the business. Rather, 'strictly necessary' should be confined to what is genuinely required for purposes such as:
    i. security and integrity (e.g., preventing account takeover)
    ii. fraud prevention
    iii. legal compliance (statutory retention)
    iv. dispute resolution and auditability, and only **to the minimum extent and minimum duration** needed
c. PIAs must require documentation of deidentification methods (and any reidentification risk).

6. *Consent architecture*
Refine consent settings to reflect family and social complexity and risk. This should include calibrating consent duration (up to 12 months) to risk. IN addition we recommend clarifying the application of exceptions for legal/health services (including whether reasonable necessary ancillary features should apply and in what circumstances).

7. *Parental controls and monitoring*
Include an explicit expectation that parental-control and monitoring features are assessed against best interests factors over time, for example taking into account high-conflict and domestic violence risks.

8. *Cross border disclosures*
    a. Treat APP 8.2(b) consent as a limited exception.
    b. Presume APP 8.1 style safeguards as the default for children.
    c. Require PIAs to document cross-border transfers, including safeguards and residual risk to the child.

9. *PIA quality, transparency and OAIC oversight*

a. Strengthen PIA requirements (including tangible mitigations and treatment of residual risk).
b. Encourage OAIC pre-launch notification for high privacy risk services.
c. Provide guidance on minimum content for public PIA summaries.

10. Dark patterns

Expand examples of prohibited dark patterns and require that usability testing of consent settings flows with representative child cohorts, and are documented through PIAs

3. General observations: legal and regulatory design

Alignment with Privacy Act principles

Central to ensuring online safety of minors is that the Code aligns with core privacy principles, including:

- data minimisation and necessity (collection and use only as needed),
- purpose limitation,
- transparency and meaningful choice,
- reasonable steps for security and governance,
- accountability for cross-border disclosures.

DLC recommends the Code expressly anchor key operational duties to principles of necessity and proportionality**.** In particular, to help regulated entities identify the 'least intrusive' means of compliance (particularly in age assurance and monitoring design) and to improve legal certainty.

Interaction with the Online Safety Act and other regimes

In addition, consider how the exposure draft would benefit from clearer articulation of how obligations under the draft Code interact with:

- OSA safety-by-design expectations,
- eSafety guidance and enforcement approaches,

- consumer protection settings (including dark patterns / unfair practices themes).

DLC proposes including an express cross-reference confirming that OSA-aligned safety-by-design compliance does not displace privacy duties under the Code. We also encourage coordinating guidance to avoid duplication and inconsistent messaging across the legislative frameworks.

4. Scope and definitions

The draft Code would benefit from clearer guidance or examples in the Explanatory Statement on the boundary between "likely to be accessed by children" and "primarily concerned with the activities of children", particularly for mixed-audience and enterprise services (for example, collaboration platforms used by both schools and businesses).

The exposure draft appears to create uncertainty for mixed-audience services and for enterprise tools that are sometimes used in educational settings.

DLC recommends that the Code provide clearer threshold criteria and illustrative examples for:

- mixed-audience services (including where child users are incidental rather than a target cohort),
- enterprise SaaS products marketed to organisations but capable of educational deployment,
- services with "child-facing" features but predominantly adult audiences.

High privacy risk services

The Code relies heavily on the concept of 'high privacy risk' as a trigger for enhanced obligations. Greater clarity is needed to reduce over- or under-capture.

We propose including a non-exhaustive list of risk indicators and practical use cases and examples, including providing clarity with respect to how a service transitions into or out of a 'high privacy risk. classification over time.

5. Best interests of the child

The ‘best interests of the child’ concept is foundational but risks uncertainty if not framed as an objective standard. DLC proposes an objective standard that links to provisions in the draft Code and which ensure that where commercial interests conflict with child privacy and safety, the interest of the child must always prevail.

DLC recommends the Code and supporting guidance material expressly state in the Code that:

- ‘best interests’ is to be applied objectively, by reference to factors in the Code (not an entity’s subjective view), and
- where commercial interests conflict with child privacy and safety interests, the child’s interests must always prevail**.**

DLC proposes including in the Code and supporting guidance material, non-exhaustive examples of practices that would be considered inconsistent with best interests of the child, including:

- profiling and recommendation techniques designed to exploit known child vulnerabilities
- targeted advertising based on sensitive information or sensitive inferences
- default settings that maximise data collection or sharing without clear necessity
- consent flows or interface designs that pressure disclosure.

6. Age assurance

Further, age assurance settings may improve child protections but risk normalising surveillance if not tightly bounded to checks and balances within the Code. With this in mind, we recommend that the Code include a clear hierarchy of age-assurance approaches, prioritising:

1. privacy-preserving and low-intrusion mechanisms
2. risk-based design that reduces need for identification / retention of personal biometric data of minors
3. higher-intrusion methods to be used only where strictly necessary and proportionate.

Specifically, biometric measures used to verify a child's age require strong guardrails to address the risk of function creep. They should be used as a last resort and must require strict limitation to purpose within the Code. DLC recommends strengthening the Code to include clear guardrails that ensure when sensitive biometric information is used for age assurance, that data:

- must be limited to that purpose,
- must not be repurposed for content filters, personalisation, profiling, advertising, analytics, or model training,
- must be subject to strong retention limits and security controls.

Age assurance may produce disparate error rates across demographics, which in turn creates a risk of bias. DLC recommends that the OAIC publish benchmark guidance (for example, acceptable error rates, bias assessments, and testing expectations) to mitigate the very real risk of discrimination, discriminatory impacts.

7. Profiling, personalisation and commercial optimisation

Profiling presents heightened risk where it shapes content, is linked to commercial outcomes, advertising, engagement loops or other commercial drivers that exploit vulnerabilities. There is the risk that profiling is directly inconsistent with the best interest of the child test. Accordingly, DLC recommends that the Code and supporting guidance material clarify that the use of profiling to exploit known vulnerabilities of children is prohibited as it is not consistent with the best interests of the child, particularly where profiling is used to:

- increase compulsive engagement with a platform
- nudges disclosure
- targets sensitive inferences.

This can be further supported by including child impact assessments as part of overarching PIA obligations. DLC supports the strengthening of PIA expectations to require entities to assess and document:

- foreseeable impacts on children arising from profiling and recommendation systems,
- mitigation measures and residual risks,
- testing and monitoring plans post-deployment.

8. Consent architecture and parental responsibility

Verifying a person with parental responsibility may be difficult in complex family arrangements, including high-conflict contexts. DLC recommends providing more practical guidance and safe-harbour approaches that:

- recognise family complexity without unduly expanding surveillance
- support risk-based verification steps and
- reduce incentives to collect additional sensitive information.

Further, a default consent duration of up to 12 months may be too long for higher-risk processing and may entrench outdated settings. DLC supports a risk-based calibration of consent duration (up to 12 months) with the requirement of more frequent renewal where processing is high-risk, involves profiling, or materially changes.

In addition, with respect to legal and health exceptions DLC proposes that the Code clarify that any exception for legal/health support services extends to ancillary features that are reasonably necessary to deliver those services safely and effectively, without expanding the exception beyond its intended purpose.

9. Parental controls and monitoring

Monitoring and parental control features can support safety but may also undermine privacy, autonomy and wellbeing, particularly for adolescents. Consider the inclusion of an explicit expectation that entities assess whether parental-control and monitoring features are consistent with best interests factors over time, and:

- include friction or prompts where monitoring becomes unusually intensive or long-term,
- provide age-appropriate transparency to children about monitoring features,
- address risk in high-conflict family contexts.

Consent architecture and the 15-year threshold - Section 13 sets a bright-line age of 15 at which a child may consent to collection, use and disclosure of their personal information; below 15, consent must be obtained from a "person with parental responsibility", subject to narrow exceptions for children seeking legal or health-related information or where another law specifies a different age. Sections 15–19 impose robust conditions on consent (voluntary, informed, current, specific, unambiguous) and limit its duration to a maximum of 12 months. Section 20 introduces an "assent" mechanism for children under 15 who enable certain high-risk data uses (sensitive data collection, secondary uses or direct marketing), requiring the child's assent and parental consent and mandating clear, age-appropriate notices.

While this structure is carefully designed, there are legal and practical risks:

- In complex family structures (for example, shared parental responsibility, state care, kinship care), verifying "a person with parental responsibility" may be difficult, potentially excluding children from beneficial services or delaying access to support.
- The 12-month consent validity may be too long in high-risk contexts (for example, sensitive data for mental-health-related apps), or too short in low-risk contexts, leading to "consent fatigue" that paradoxically undermines meaningful decision-making.

Case study – Mental health support app for teenagers

A mental-health support app for teenagers offers anonymised chat and access to psycho-educational resources. A 14-year-old seeks help in relation to abuse by a parent. Section 13(4) rightly allows the child to consent without parental involvement for legal or health-related support "in connection with a person with parental responsibility". However, the app also offers optional tracking of mood over time and integration with wearable devices (highly sensitive data). It is unclear whether the app must treat the 14-year-old's consent as sufficient for these ancillary features, or whether parental consent is required, which would be inappropriate in this scenario. Recommendation:

- Clarify in the Statement that the s 13(4) exception extends to ancillary features reasonably necessary for the provision of legal or health-related support (for example, mood tracking within a counselling app) where involving a parent would undermine the purpose of the service.

Encourage entities, via OAIC guidance, to calibrate consent duration (up to 12 months) based on contextual risk, and to avoid unnecessary re-consent demands that would overwhelm children or parents.

10. Data minimisation, destruction and deidentification

The Code should mandate deletion upon requests for destruction and not allow deidentification. This is to mitigate the risk of reidentification, particularly where multiple datasets exist. If destruction is not feasible or practicable, consider permitting data deidentification as a permitted exception, subject to appropriate guardrails to mitigate reidentification risks. Permitted exceptions may occur where:

- retention is required by law
- for parliamentary inquiry / hearings
- retention is strictly necessary to protect the rights of the child
- retention is required to meet essential safety/security obligations (this exception must be interpreted narrowly and must not prioritise the technology over child safety).

Behavioural analytics for unrelated product development or marketing should not be treated as strictly necessary. DLC strongly recommends that entities should adopt a narrow interpretation of which behavioural analytics, including logging, should be considered ‘strictly necessary’ and explicitly assess and document reidentification risk and justify data retention periods.

Guidance on refusals and explanations

Further, where destruction requests are refused due to one of the legitimate, approved exceptions, children and their guardians / parents should receive clear, explanation and timely notification. Accordingly, DLC suggests strengthening the explanatory guidance with respect to:

- how refusals must be explained

- what alternative options are available to the child and their parent / guardian (for example: restriction or deactivation) and
- the practical implications of data retention on the child.

11. Cross-border disclosures

Risks are amplified when children's data is transferred across borders or is stored offshore. Consider whether the current guardrails go far enough to mitigate the risk that technology providers will intentionally, or by default, harvest and offshore the storage of children's data. DLC Legal proposes treating APP 8.2(b) consent as a limited exception and an option of last resort for children's personal information. In addition, PIAs must include a mandatory obligation to assess where and how the data of children (and vulnerable people more broadly) is stored and transferred, whether the requirement to disclose cross-border disclosures, safeguards, and residual risk for children, including how foreign laws and practices may affect enforceability and redress.

Further, we propose establishing a presumption in favour of APP 8.1-style safeguards and due diligence as the default position.

12. Dark patterns and meaningful choice

The Code's examples of prohibited dark patterns go some way to illustrate risks to children. However, DLC strongly recommends these examples also require usability testing of key consent and settings flows with representative cohorts of children to ensure appropriate checks and balances are in place. For example:

- 'accept all' prominence without equivalent rejection
- repeated nudging after refusal
- confusing toggles and defaults that maximise disclosure
- bundling consent with non-essential features,

are all features that pose risks to child users of technology platforms and applications if unchecked.

The results and mitigations must also be documented in PIAs.

13. PIAs, transparency and regulatory oversight

PIAs are central to accountability. The draft Code would benefit from stronger expectations about content quality, follow-through, accountability and transparency. We recommend that PIAs be required to include:

- a clear description of processing and purposes
- identified child-specific risks
- mitigation measures and implementation status
- residual risk assessment and acceptance rationale
- monitoring and review arrangements.

In addition, the guidance material should provide guidance on what should be the minimum required content for public PIA summaries. The register must support meaningful transparency without requiring disclosure of security-sensitive details.

We also encourage notification to OAIC prior to launch or material change for high privacy risk services, to improve oversight and enable early engagement on mitigations.

14. Illustrative examples and international comparators

DLC supports the inclusion of practical, concrete examples of compliant implementations. For example, comparisons to the UK Age Appropriate Design Code) to illustrate application of:

- default settings and data minimisation
- profiling limitations
- age assurance hierarchy
- consent renewal and transparency measures.

For example, the sector-specific example of child-facing financial services, including banking and payment products, raises specific concerns around secondary use and cross-selling. DLC recommends:

- 'strictly necessary' in a financial context should not ordinarily include behavioural analytics for unrelated product development or marketing, and
- entities should not use children's transactional data to profile parents for cross-selling without separate parental consent and a clear best-interests assessment.

15. Conclusion

DLC Legal commends the OAIC for the exposure draft Code and accompanying explanatory documentation. The exposure draft represents a meaningful step toward a more child-centred privacy framework. We recommend refinements to the draft Code to further:

- clarify the scope of application and refine key definitions;
- strengthen practical guidance on how the best-interests principle is to be applied and evidenced;
- adopt a privacy-preserving hierarchy of methods;
- strengthen controls on profiling and recommender practices;
- improve workability and versatility of consent settings;
- include safeguards to ensure monitoring tools remain consistent with best interests over time;
- adopt data deletion as the default approach, with deidentification used only for clearly justified exceptions;
- strengthen the restrictions on cross-border disclosure;
- create usable and easy to understand key consent and settings flows;
- strengthen required PIA inclusions around accountability and transparency;
- expand illustrative examples to improve consistency of application, including by reference to equivalent international provisions, to clarify intended operation in common scenarios.

Implementing these refinements would materially reduce social, technical and legal risks—particularly in age assurance, profiling, deletion/deidentification, and cross-border accountability—while preserving the Code's central aim of improving children's online privacy outcomes.

We welcome the opportunity to participate in further co-design of guidance material and supporting artefacts. In our view, the ultimate Effectiveness of the framework will depend not just the drafting of the Code, but on how the Coded is interpreted and operationalised in practice.