OAIC Exposure Draft Children's Online Privacy Code

Australasian Society for Computers and Law (2026).
Office of the Australian Information Commissioner (OAIC).
AUSCL Policy Series PS-2026-01.

4 June 2026

OAIC Exposure Draft Children's Online Privacy Code

Submitted 4 June 2026

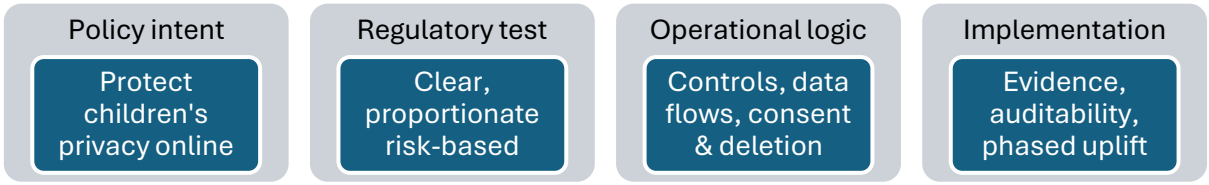
About us

AUSCL, the Australasian Society for Computers & Law, is an independent interdisciplinary think tank focused on law, technology and society. Its work supports the UN Sustainable Development Goals, with particular focus on SDG 16 (Peace, Justice and Strong Institutions) and SDG 17 (Partnerships for the Goals).

AUSCL brings together Australian and New Zealand societies for computers and law. The Society's patron is The Hon Michael Kirby AC CMG.

This response was prepared by expert members of AUSCL's Data Protection & Privacy Working Group and Future Law Working Group, with stakeholder input.

We focus on how regulatory design performs in practice: its effectiveness, its impact on stakeholders, and its readiness for digital and data-driven environments, by applying the following framework:



Consultation

The OAIC has invited feedback on the Exposure Draft Code and Draft Explanatory Statement, including any unintended consequences and drafting issues.

AUSCL has structured this response around the principal consultation issues: scope, age assurance, best interests, strict necessity, consent, transparency, destruction, PIAs, commencement, implementation guidance and regulatory coherence. Paragraphs are numbered for ease of reference.

Executive position

AUSCL supports the Exposure Draft in principle. It addresses a clear regulatory concern: children engage with online services that routinely collect, infer, use and disclose personal information, often without the capacity, agency or bargaining power to understand or control those practices.

The Draft Code is a constructive step beyond notice and consent, particularly through:

- privacy-by-default settings;

- age-appropriate transparency;
- stronger consent requirements;
- privacy impact assessments; and
- child-friendly access, correction, destruction and complaint mechanisms.

AUSCL suggests that targeted refinements would support effective implementation, including clearer guidance on proportionality, operational controls, audit evidence and product design processes.

Overall assessment

Strong policy intent is most effective with clear, practical guidance.

The Draft Code represents a significant regulatory intervention, applying child-specific protections not only to services primarily directed at children, but also to any service likely to be accessed by children. This scope is broad and potentially challenging to operationalise.

The examples in the draft and Explanatory Statement show that the Code extends beyond social media and entertainment platforms to early-childhood apps, family photo-sharing services, school management systems and connected devices. This reflects children's engagement with digital systems across home, education and social environments.

The draft Explanatory Statement sets ambitious objectives: strengthening privacy capability, increasing transparency, centring the best interests of the child and giving children greater control over their personal information. It also records extensive consultation with children, parents and carers, industry, civil society, academia, the eSafety Commissioner and the National Children's Commissioner.

In our view, from a regulatory design perspective, the **strongest elements** of the draft Code include:

- privacy-by-default settings,
- child-facing transparency requirements,
- restrictions on manipulative consent practices,
- annual reviews of privacy practices,
- mandatory privacy impact assessments,
- staff training obligations and
- strengthened destruction rights.

These features collectively support a proactive, risk-responsive approach to children's privacy.

The Code's **principal weaknesses** do not arise from policy intent but from implementation challenges. Several obligations rely on judgement-heavy concepts — including "reasonable steps", "strictly necessary", "best interests of the child" and "likely to be accessed by children".

These concepts are legitimate and necessary. Clear guidance, practical examples and evidentiary expectations would reduce inconsistent interpretation, over-defensive compliance and privacy-invasive practices adopted in the name of caution.

Recommendations

Recommendation 1 - Balance

AUSCL supports the Code in principle, while recommending targeted refinements to improve legal clarity, implementation certainty and proportionality

AUSCL recommends targeted refinements before registration, including clearer risk-tiered age assurance, a practical best interests assessment framework, specific guidance on AI and inferred data, staged implementation, and a regulatory coherence map across privacy, online safety, consumer protection and emerging AI governance obligations.

Issue Does the Exposure Draft strike the right balance between stronger children's privacy protection and practical implementation?

Response

1.1 AUSCL supports the Exposure Draft in principle. The Code responds to a clear policy problem: children increasingly participate in online environments where personal information is collected, inferred, profiled, used and disclosed in ways they may not understand or control.

1.2 The Code is consistent with the policy intent of the *Privacy Act 1988 (Cth)*, the Privacy Act Review reforms and the Privacy and Other Legislation Amendment Act 2024, by strengthening children's privacy protections through an APP Code applying in addition to the Australian Privacy Principles.

1.3 The Draft appropriately moves beyond a narrow notice-and-consent model and introduces privacy-by-default, age-appropriate transparency, stricter consent standards, child-friendly rights and privacy impact assessment obligations.

1.4 However, it is submitted that the final Code would benefit from clearer guidance, sector examples and phased implementation so that entities can translate the obligations into practical systems, product controls, records and audit evidence.

Recommendation 2 - Clarity

Drafting clarity

Publish companion guidance clarifying key operative concepts, including "likely to be accessed by children", "strictly necessary", "best interests", "reasonable steps", "age appropriate" and "current consent".

Issue Are any provisions unclear, ambiguous or likely to cause inconsistent interpretation?

Response

1.5 The Draft is directionally sound, but several operative concepts require clarification to avoid inconsistent or defensive compliance.

1.6 In particular, clarification is recommended for the concepts: "likely to be accessed by children", "strictly necessary", "best interests of the child", "reasonable steps", "age appropriate", "current consent", "person with

parental responsibility", "direct marketing" and "destruction". Note: Destruction in AI systems may be technically complex.

1.7 These concepts are legitimate in a principles-based privacy instrument, but they need implementation guidance, examples and evidentiary expectations.

1.8 AUSCL recommends that the OAIC publish a companion obligation-to-control map that identifies each obligation, the relevant APP, trigger, control, record, and implementation owner. AUSCL can work with the OAIC to achieve this valuable output.

Recommendation 3 - Scope

Clear scope guidance

Provide clear scope guidance for mixed-audience services, including practical indicators for determining when a service is "likely to be accessed by children" or "primarily concerned with children's activities".

Issue Is the scope of services "likely to be accessed by children" or "primarily concerned with the activities of children" sufficiently clear?

Response

1.9 The Code's scope is broad and appropriately reflects the fact that children's privacy risks arise across social media, gaming, education technology, connected devices, family apps and child-related services.

1.10 AUSCL supports the inclusion of services likely to be accessed by children and services primarily concerned with children's activities.

1.11 The final guidance to clarify how mixed-audience services assess likely child access, including by reference to actual users, design features, marketing, content, analytics, complaints and reasonably foreseeable use.

1.12 The Draft could usefully clarify that a service may avoid unnecessary age assurance where it applies Code-level protections to all users, consistent with s 8(5).

Recommendation 4 – Age assurance

Tiered approach

Adopt a risk-tiered, privacy-preserving age assurance framework that permits low-friction methods for low-risk services and avoids unnecessary collection or retention of identity, biometric or sensitive information.

Issue Are the age-assurance obligations workable, proportionate and privacy-preserving?

Response

1.13 AUSCL supports a risk-based age assurance obligation, provided it does not cause over-collection of identity, biometric or sensitive information.

1.14 Section 8 correctly requires reasonable steps having regard to risk of harm, and permits entities to avoid age assurance where child-level protections are applied to all users.

1.15 OAIC guidance could usefully distinguish between self-declaration, age-banding, parental attestation, age estimation, tokenised assurance and formal age verification.

1.16 Higher assurance is best reserved for higher-risk services or higher-risk data practices; low-risk services are best not pushed into collecting more personal information than necessary.

1.17 The Code could expressly prefer data-minimised age signals, such as an age range or "under/over threshold" flag, rather than retention of underlying identity evidence.

Recommendation 5 - Best interests of the child

Publish template

Publish a best interests assessment template to help entities assess purpose, necessity, proportionality, risk of harm, vulnerable cohorts, alternatives, safeguards and evidence.

Issue Is the "best interests" obligation sufficiently clear for product, privacy, data, marketing and AI decision-making?

Response

1.18 AUSCL supports centring the best interests of the child as a primary privacy-design principle.

1.19 Sections 10 and 11 appropriately connect the collection, use and disclosure of personal information with the child's best interests.

1.20 The final Code would be strengthened by confirming that the best interests test is an operational assessment, not a general value statement.

1.21 AUSCL recommends a practical best interests assessment template covering:

- purpose, necessity and proportionality;
- likely harm and affected cohorts;
- less intrusive alternatives;
- safeguards and child agency; and
- evidence supporting the assessment.

1.22 The Explanatory Statement already identifies relevant factors, including exploitation risk, mental, physical and developmental impacts, identity, autonomy, association, play, education and disproportionate impacts on particular groups of children.

Recommendation 6 - Strict necessary / privacy by default

Drafting clarity

Clarify the distinction between data handling that is strictly necessary to deliver the core service and optional processing for personalisation, analytics, advertising, service improvement or AI model development.

Issue Is the requirement to collect, use or disclose children's personal information by default only where "strictly necessary" clear and implementable?

Response

1.23 AUSCL supports the "strictly necessary" threshold for default settings, as it gives practical effect to data minimisation and privacy-by-design.

1.24 Section 9 is appropriately retained. Final guidance would be strengthened by distinguishing between:

- core service delivery; and
- optional processing, including analytics, personalisation, advertising, AI model development and product improvement.

1.25 Sector examples would assist implementation across account creation, messaging, safety, fraud prevention, recommender systems, analytics, advertising, AI model improvement and product development.

1.26 Processing for marketing, profiling, behavioural advertising or general service improvement is unlikely to be strictly necessary to provide a child-facing service.

1.27 Clear guidance on this distinction would reduce ambiguity between what is necessary for the child-facing service and what is commercially useful for the provider.

Recommendation 7 - Consent

Provide examples

Retain the strengthened consent requirements, but support them with practical examples, consent dashboards, annual privacy check-ups and renewal mechanisms that are understandable and manageable for children and parents.

Issue

Are the consent, parental consent, assent, withdrawal and renewal requirements workable in practice?

Response

1.28 AUSCL supports stronger consent standards for children, including requirements that consent be voluntary, informed, current, specific and unambiguous.

1.29 The Draft appropriately rejects bundled consent, manipulative consent practices, pre-ticked boxes and consent inferred from continued use.

1.30 The 12-month maximum consent period is protective, but OAIC guidance could allow practical mechanisms such as annual privacy check-ups, consent dashboards and consolidated renewal flows.

1.31 Consent is not an appropriate basis to legitimise high-risk or harmful data practices that are inconsistent with the best interests of the child.

1.32 For children under 15, parental consent and child assent can be implemented in ways that preserve the child's participation, privacy literacy and ability to withdraw.

Recommendation 8 - Parental consent and parental responsibility

Drafting clarity

Apply a proportionate "reasonable steps" approach to parental responsibility verification, with safeguards for separated families, children in care, family violence contexts and children seeking confidential legal or health support.

Issue How online services can obtain consent from a person with parental responsibility where a child is under 15, without creating rigid, unsafe or impractical verification requirements?

Response

1.33 AUSCL supports obtaining consent from a person with parental responsibility where a child is under 15, subject to appropriate safeguards.

1.34 The final Code would be strengthened by avoiding rigid proofing requirements that may be unrealistic or unsafe in contexts involving separated families, kinship care, foster care, family violence or children seeking confidential support.

1.35 OAIC guidance would be most effective if based on a proportionate “reasonable steps” model, calibrated to risk and context.

1.36 Examples such as account-based confirmation, school or trusted-provider tokens, customer-service verification and government digital ID are best framed as optional pathways, not mandatory requirements.

1.37 The Code would be strengthened by preserving exceptions where involving a parent or carer may undermine a child’s safety, privacy, or access to legal or health-related support.

Recommendation 9 – Direct marketing

Guidance

Strengthen guidance on direct marketing to children by expressly addressing behavioural advertising, profiling, recommender systems, influencer-style targeting, lookalike audiences and cross-context tracking.

Issue Are the proposed direct marketing restrictions clear and sufficiently protective?

Response

1.38 AUSCL supports stronger limits on direct marketing to children.

1.39 The Draft appropriately requires direct marketing uses and disclosures under APP 7 to be based on consent and consistent with the child’s best interests.

1.40 Final guidance would be strengthened by identifying the following as high-risk practices for children:

- behavioural advertising;
- profiling;
- influencer-style targeting;
- lookalike audiences; and
- cross-context tracking.

1.41 Opt-out controls need to be prominent, age appropriate and easy to use.

1.42 Clearer guidance on the relationship between direct marketing, personalised recommendations and recommender systems would assist, as children may not distinguish between advertising, content ranking and platform nudges.

Recommendation 10 – Transparency

Templates

Publish model child-facing privacy notices that are layered, visual, age-appropriate and explain direct collection, inferred data, profiling, geolocation, third-party sharing and automated recommendation practices.

Issue Are the child-facing notice, privacy policy and explanation requirements likely to be effective?

Response

1.43 AUSCL supports child-facing transparency requirements, including a children's version of the APP privacy policy.

1.44 Transparency is most effective where it covers:

- information provided directly by a child;
- observed and inferred data;
- profiling and automated recommendations;
- geolocation;
- cross-border disclosure; and
- third-party sharing.

1.45 Notices are best presented in layered, visual and age-appropriate formats, and tested with children where practicable.

1.46 Model child-facing notices for different age ranges and service types would assist consistent implementation.

1.47 The Explanatory Statement records that children and young people want age-appropriate information about how their personal information is handled and how to seek help if there is a problem.

Recommendation 11 – Access, correction and information rights

Clarification

Clarify how children can exercise access, correction and explanation rights directly or with support, including where parental access may conflict with a child's safety, autonomy or privacy.

Issue Are the access, correction and explanation rights clear, age-appropriate and operationally feasible?

Response

1.48 AUSCL supports strengthened access, correction and explanation rights for children.

1.49 These rights are best designed to allow children to exercise them directly where developmentally appropriate, with support from parents or carers where appropriate.

1.50 Guidance on parental access would be valuable where it may conflict with a child's safety, privacy or autonomy.

1.51 Template responses for access, correction and explanation requests would support consistent, child-appropriate implementation.

1.52 Further clarification would assist on how these rights apply to:

- inferred information;
- profiles;
- recommender-system categories; and
- AI-generated assessments about a child

Recommendation 12 – Destruction

Practical guidance

Provide technical guidance on destruction requests, including treatment of backups, logs, legal holds, safety records, processors, derived data, de-identification and AI training or evaluation data.

Issue

Are the destruction rights workable in modern technical environments, including backups, logs, processors, legal holds and AI-derived data?

Response

1.53 AUSCL supports a meaningful right to request destruction of children's personal information.

1.54 Section 32 is important but requires technical guidance for modern systems.

1.55 Further guidance would assist on expectations for:

- active systems;
- backups and logs;
- legal holds and safety records;
- processor systems and cloud environments;
- derived data; and
- AI training or evaluation data.

1.56 The Code would be clearer if it distinguished between deletion, de-identification, suppression from future use and retention required by law.

1.57 The destruction right is best framed to preserve legitimate safety, dispute-resolution and legal-retention obligations, while avoiding incentives for providers to withdraw beneficial child-facing services.

Recommendation 13 – Monitoring and geolocation

Settings

Require clear, age-appropriate notice and default-off settings for monitoring and geolocation, except where the function is strictly necessary or demonstrably in the child's best interests.

Issue

Are the notification requirements for parental controls, monitoring and geolocation sufficient and safe?

Response

1.58 AUSCL supports notification requirements for mechanisms that monitor or control service use or monitor geolocation.

1.59 Children are best informed, in age-appropriate terms, when their activity, location or use of a service is being monitored or controlled.

1.60 The Code would be strengthened by recognising that parental controls may themselves become privacy-invasive or unsafe, particularly for:

- older children;
- children experiencing family violence; and
- children seeking confidential health or legal support.

1.61 Guidance distinguishing safety-oriented monitoring, commercial tracking, parental surveillance and geolocation features would support clearer implementation.

1.62 Monitoring and geolocation are best set to off by default unless strictly necessary or clearly justified in the child's best interests.

Recommendation 14 – Complaint

Settings

Publish model child-friendly inquiry and complaints pathways that are simple, accessible, trauma-informed and capable of being used by children without adult legal or technical knowledge.

Issue

Are the child-friendly complaints and inquiry obligations clear and effective?

Response

1.63 AUSCL supports child-friendly inquiry and complaints processes.

1.64 A child ought to be able to raise a privacy concern without navigating legalistic privacy policies or adult-facing complaint channels.

1.65 Complaints pathways are best made easy to find, age appropriate, trauma-informed and available through the service interface where practicable.

1.66 OAIC could consider publish model complaint pathways and wording for children, parents and carers.

1.67 Providers should record complaint themes and use them to improve privacy design, training and annual review processes.

Recommendation 15 – PIAs and registers

Template

Publish a child-privacy PIA template and public register format, including guidance on what must be disclosed and what may be withheld for security, safety, confidentiality or commercial sensitivity.

Issue

Are the privacy impact assessment and public register obligations proportionate and sufficiently specified?

Response

1.68 AUSCL supports mandatory privacy impact assessments for higher-risk child data handling.

1.69 Section 38 appropriately requires assessment of data flows, purposes, strict necessity, lawful and fair collection, best interests, compliance and risk of harm to children.

1.70 Section 39's public register obligation is useful, but guidance could usefully clarify what must be published and what may be withheld for security, safety, confidentiality or commercial sensitivity.

1.71 We recommend OAIC publish a child-privacy PIA template and register format.

1.72 PIAs are best not treated as static compliance documents; they can operate as product-governance gates before launch and when material changes occur.

Recommendation 16 – Training

Training design

Require practical, role-based training for staff involved in child-related data handling, including product, engineering, marketing, analytics, customer support, safety, legal, privacy and vendor-management teams.

Issue

Are the privacy education and training obligations adequate?

Response

1.73 AUSCL supports privacy education and training obligations.

1.74 Training could apply to personnel who design, manage, support or access child-related data flows, including product, engineering, marketing, analytics, customer support, safety, legal, privacy and vendor-management teams.

1.75 The training could cover children's privacy rights, best interests, consent, age assurance, direct marketing, complaints, destruction, AI/inferred data and escalation pathways.

1.76 Records of training could be maintained and available to the Commissioner on request.

1.77 Training is most effective when practical and scenario-based, not limited to general privacy awareness.

1.78 AUSCL is a registered educational charity with substantial experience in education and professional training. AUSCL would welcome the opportunity to provide further input on the appropriate structure, syllabus and content of any training program or supporting materials.

Recommendation 17 – Commencement

Phased approach

Adopt phased commencement or staged regulatory expectations, with earlier implementation for governance and transparency controls and longer lead times for age assurance, consent architecture, deletion workflows and AI controls.

Issue What commencement date or phased implementation period is appropriate?

Response

1.79 AUSCL recommends phased commencement or staged regulatory expectations.

1.80 Governance, privacy policy uplift, child-facing notices, complaints processes, direct marketing controls and initial training can be implemented earlier.

1.81 More complex technical obligations — age assurance, parental responsibility verification, consent architecture, deletion workflows, processor remediation and AI/profiling controls — require additional implementation time.

1.82 The commencement date could allow entities to complete data mapping, product redesign, vendor review, system changes and staff training.

1.83 A phased model would better serve the policy intent by improving real compliance rather than encouraging superficial or defensive responses. AUSCL's Data Protection and Privacy Working Group would welcome the opportunity to provide further input or guidance on implementation timeframes through surveying its members and/or conducting roundtable discussions with privacy and compliance officers across industry stakeholder groups.

Recommendation 18 – Regulatory coherence

Strategic mapping

Publish a regulatory coherence map explaining how the Code interacts with the Privacy Act, APPs, Online Safety Act, eSafety requirements, consumer protection law, direct marketing rules and emerging AI governance frameworks and standards.

Issue How can the Code interact with the Privacy Act, APPs, Online Safety Act, eSafety requirements, consumer law and emerging AI governance frameworks?

Response

1.84 The Code can operate as a child-specific privacy overlay, rather than as an isolated regulatory regime.

1.85 OAIC guidance could map the Code against the Privacy Act, APPs, Online Safety Act 2021, eSafety requirements, consumer protection law, direct marketing rules and emerging AI governance expectations.

1.86 Attention is needed where the Code intersects with age assurance under online safety reforms, unfair or manipulative design practices, AI-enabled profiling and cross-border data flows.

1.87 The Explanatory Statement confirms that APP codes operate in addition to the APPs and may impose additional requirements, provided they are not contrary to or inconsistent with the APPs.

1.88 A regulatory coherence map would reduce duplication, improve implementation certainty and support consistent enforcement.

Recommendation 19 – Planning for unintended consequences

Risk-tiered guidance

Address unintended-consequence risks through risk-tiered guidance, safe-harbour examples and proportional implementation pathways, particularly to prevent over-collection, excessive identity proofing and exclusion from beneficial services.

Issue Could the Code cause over-collection of age data, exclusion from beneficial services, excessive parental proofing, defensive compliance, or inconsistent sectoral implementation?

Response

1.89 The main unintended consequence risk is the over-collection of personal information for age assurance or parental verification.

1.90 Other risks include exclusion of children from beneficial services, excessive identity proofing, fragmented sectoral interpretation, defensive withdrawal of child-facing features, over-reliance on parental surveillance and superficial compliance documentation.

1.91 The Code may also create uncertainty for schools, edtech providers, health-adjacent services, charities, support services and mixed-audience platforms unless sector examples are provided.

1.92 These risks can be managed without weakening the Code by using risk-tiered guidance, safe-harbour examples, model controls and phased implementation.

1.93 AUSCL identifies age assurance, best interests, parental consent, destruction requests and PIAs as areas where privacy benefits are high, but implementation burden or unintended-consequence risk is also material.

Recommendation 20 – Comprehensive guidance

Implementation package

Release a comprehensive implementation package alongside the final Code, including decision trees, templates, sector examples, control maps, evidence artefacts and a non-binding digital legislative twin.

Issue What OAIC guidance, templates, decision trees, sector examples or safe-harbour examples are needed?

Response

1.94 It would be helpful if the OAIC published companion guidance at or before the Code is finalised.

1.95 The guidance package could include:

(a) scope and applicability decision trees;

(b) risk-tiered age assurance framework;

(c) best interests' assessment template;

(d) strict necessity purpose taxonomy;

(e) child-facing model notices;

(f) consent and assent examples;

(g) parental responsibility verification examples;

(h) destruction and retention guidance;

(i) AI, profiling and inferred-data guidance;

(j) child-privacy PIA template;

(k) public register template;

(l) sector-specific examples; and

(m) regulatory coherence map.

Recommendation 21 – Digital by design

Future-proof the Code by deploying a digital twin

Release a non-binding digital legislative twin incorporating the outputs from Recommendation 21. See Appendix A

Issue

Translating the Code into practical, consistent and auditable compliance requirements and enforcement practice?

Response

1.96 AUSCL also recommends that OAIC publish a non-binding digital legislative twin of the Code, mapping obligations, actors, triggers, data objects, exceptions, controls, evidence artefacts, decision trees and conformance scenarios.

1.97 This recommendation addresses the risk that regulated entities may interpret and implement the Code inconsistently unless the OAIC provides structured, operational guidance. A non-binding digital legislative twin would help translate the Code's legal obligations into practical compliance logic, including actors, triggers, data objects, exceptions, controls, evidence artefacts, decision trees and conformance scenarios.

1.98 This would improve consistency, reduce duplicated interpretation costs and help entities embed the Code into service design, data governance and assurance processes.

1.99 Creation of a digital twin would allow for early scenario testing and serve as an exceptional tool for ensuring the Code's impact is regularly assessed and changes are modelled to identify and mitigate unintended consequences.

1.100 AUSCL's Future Law Working Group includes experts in regulatory digital twins and related implementation models. AUSCL would welcome the opportunity to workshop these ideas with the OAIC and explore the design of a potential pilot program.

APPENDIX A

Digital legislative twin proposal for the Children's Online Privacy Code

This Appendix provides further detail in support of **Recommendation 21 – Digital by design**.

Recommendation A - AUSCL recommends that the OAIC consider publishing a non-binding digital legislative twin of the final Children's Online Privacy Code to support consistent compliance, practical implementation and effective regulatory design.

The twin could map obligations, actors, triggers, data objects, exceptions, controls and evidence artefacts, and include decision trees and conformance scenarios for the highest-risk obligations. This would improve regulatory certainty, support consistent compliance, reduce duplicated interpretation costs and help the Code operate effectively in digital environments.

Note: This would not alter the legal effect of the Code. It would translate the Code into implementation logic that can be understood by legal, privacy, product, engineering, data governance and assurance teams.

Guidance. AUSCL suggests that the final Code registered together with an ancillary non-binding digital legislative twin package, including:

- a plain-language obligations map;
- decision-tree diagrams;
- model controls;
- a machine-readable schema;
- evidence artefacts;
- sample conformance scenarios; and
- a version/change-log process.

This ancillary package could help improve legal certainty, reduce duplicated interpretation costs and support consistent child protection across sectors, without replacing the Code's legal force or the Commissioner's supervisory discretion.

Purpose. A digital legislative twin could support implementation of the final Code. Its purpose would not be to automate legal judgment, but to make the Code easier to implement, audit and embed into digital service design.

Definition. A digital legislative twin is a structured companion representation of the Code. It maps:

- regulated entities;
- obligation triggers;
- relevant data objects;
- exceptions;
- expected controls;
- evidence requirements; and
- common conformance scenarios.

Regulatory design value. A digital legislative twin would address a key implementation challenge: Principled requirements that are difficult to translate into operational systems. It would reduce fragmented interpretation, support small and medium providers, promote consistent implementation and give regulators a clearer evidence base for supervision.

Preliminary guidance

A1. Proposed digital twin elements

Twin element	What it could contain	Why it matters for the Code
Scope model	Service type, likely child access, primarily child-related activities, exclusions and mixed offline/online services.	Reduces uncertainty about whether and when the Code applies.
Age assurance logic	Risk tiers, accepted methods, data minimisation rules, non-retention expectations and examples.	Prevents over-collection caused by defensive age verification.
Strict necessity rules	A purpose taxonomy distinguishing core service, safety, analytics, personalisation, marketing, AI training and optional features.	Supports privacy-by-default implementation under s 9.
Best interests assessment	A documented decision model covering necessity, proportionality, harm, vulnerable cohorts, alternatives and safeguards.	Makes ss 10-11 operational and auditable.
Consent and parental responsibility model	Role logic for child, parent, guardian, authorised carer, school, hospital or referrer; consent expiry; withdrawal; assent.	Supports workable and inclusive consent under ss 13-20.
Third-party and cross-border model	Processor categories, offshore recipients, onward-use restrictions, deletion flow-down and APP 8 controls.	Addresses downstream data risk and regulatory coherence.
Deletion and retention model	Rules for active systems, backups, logs, legal holds, safety records, processors and AI-derived artefacts.	Makes s32 feasible in modern architectures.
AI and inferred-data model	Treatment of inferred data, profiling, recommender systems, chatbot interactions, model training and explainability.	Addresses a critical gap in the draft Code.

Twin element	What it could contain	Why it matters for the Code
Evidence and audit model	Records expected for PIAs, annual review, training, consent, complaints, destruction, vendor controls and assurance testing.	Supports enforceability and reduces superficial compliance.

A2. Proposed digital legislative twin artefacts

- **Human-readable obligation map:** A table mapping each section of the Code to the APP it modifies, the relevant actor, trigger, control, evidence and implementation owner.
- **Machine-readable schema:** A structured representation, for example JSON or equivalent, of obligation logic, data categories, consent states, age assurance states and exception pathways.
- **Decision-tree diagrams:** Visual logic for key high-risk areas: scope, age assurance, strict necessity, best interests, parental consent, direct marketing and deletion.
- **Scenario library:** Worked examples for social media, gaming, edtech, health-adjacent services, child charities, AI chatbots, peer-support communities and connected devices.
- **Conformance test cases:** Sample test cases that allow providers to assess whether a service design, data flow or vendor arrangement would likely meet the Code.
- **Version control and change log:** A transparent mechanism for updating the twin when the Code, OAIC guidance, APP guidelines or related online safety requirements change.

Digital legislative twin component	Function in implementation	Code relevance
Obligation model	Breaks the Code into discrete obligations, permissions, prohibitions and exceptions.	Supports APP-linked obligations across ss 8-40.
Actor and service model	Identifies child, parent/carer, provider, processor, regulator and service type.	Supports scope analysis under ss 5-7 and consent under ss 13-20.
Data object model	Classifies personal information, sensitive information, inferred data, age assurance data, geolocation, content and metadata.	Supports minimisation, transparency, access and destruction obligations.
Decision trees	Provides structured logic for age assurance, strict necessity, best interests, consent, direct marketing and deletion requests.	Improves consistency for ss 8-11, 13-21, 29 and 32.
Control and evidence map	Links each obligation to system controls, policies, records, logs, training and audit evidence.	Supports PIAs, annual review, training and regulator-ready evidence.
Scenario and conformance tests	Allows providers and regulators to test common implementation scenarios before launch.	Supports predictable, proportionate and auditable implementation.

Step	Question	Recommended logic	Evidence
1	Is the service likely to be accessed by children, or is it primarily concerned with children's activities?	If no, record basis. If yes or uncertain, proceed to risk assessment.	Applicability assessment.
2	Does the service apply child-level protections to all users?	If yes, age assurance may not be required for Code compliance, subject to specific legal requirements.	Product control record.
3	What is the risk of harm from collection, use or disclosure?	Low-risk services may use self-declaration or age-banding; higher-risk services may require stronger assurance.	Risk assessment.
4	What is the least privacy-invasive method available?	Prefer data minimisation, age-range result and non-retention of identity documents or sensitive data.	Assurance method record.
5	What data is to be retained?	Retain only what is necessary to evidence compliance; destroy sensitive information as soon as practicable unless an exception applies.	Retention/deletion log.

A3. Additional explanatory notes

A digital legislative twin would provide a testable, version-controlled companion representation of the final Code. It would not replace the legislative instrument; it would translate the Code into structured obligation logic for product, privacy, engineering, legal, audit and regulatory teams.

For the Children's Online Privacy Code, the twin could model the regulated service, relevant actors, child status, age assurance result, personal information category, purpose of handling, consent status, parental responsibility pathway, best interests' assessment, exceptions, controls and evidence artefacts. This would allow organisations to test proposed features, data flows and third-party disclosures before deployment.

The twin could be designed as both a regulatory design tool and a legal informatics artefact, supporting human-readable guidance, machine-readable rules, decision trees, control mappings, sample data-flow scenarios and conformance test cases. This would make the Code more operationally certain without reducing the Commissioner's discretion or regulated entities' accountability.

APPENDIX B

Graphical stakeholder interests and adequacy gap analysis

This Appendix provides further information in support of **Recommendations 1 - 21**.

Purpose. This appendix incorporates two infographics that summarise AUSCL's consultation response.

(1) Stakeholder Interests and Adequacy Analysis; and

(2) The Limits, Risks and Adequacy Gap Analysis.

Recommendation B – AUSCL recommends the use of stakeholder interest mapping to inform the Final Code and for impact testing of both in draft and final form.

Set out below are diagrams and notes supporting the recommendations above. The proposed refinements are intended to preserve strong child-rights protections while improving certainty, proportionality, technical feasibility and regulatory coherence.

Direct stakeholder engagement would help verify and prioritise the issues identified. The analysis below is based on AUSCL's regulatory design assessment and would benefit from testing with affected stakeholders.

B1. Stakeholder Interests and Adequacy Analysis

Explanatory notes

- **Purpose of the diagram** Figure B1 maps the principal stakeholders affected by the draft Code and assesses whether the Exposure Draft adequately addresses their interests, taking account of the limits and implementation risks identified in the report.
- **Central regulatory design point** The draft Code appropriately centres children and young people. Practical protection will depend on whether regulated entities can translate obligations into usable notices, product settings, consent flows, data controls, deletion processes and child-friendly complaints pathways.
- **Adequacy assessment** The draft is strongest in principle for children and civil society because it introduces privacy-by-default, transparency, limits on direct marketing, anti-manipulation safeguards, destruction rights, complaint processes and PIAs. Adequacy is lower for service providers, schools, edtech and child-serving services because several obligations require operational interpretation and technical implementation.
- **Main stakeholder risk** Unclear obligations may produce inconsistent compliance. Providers may over-collect information for age assurance, withdraw beneficial child-facing services or implement superficial controls that do not materially improve children's privacy.

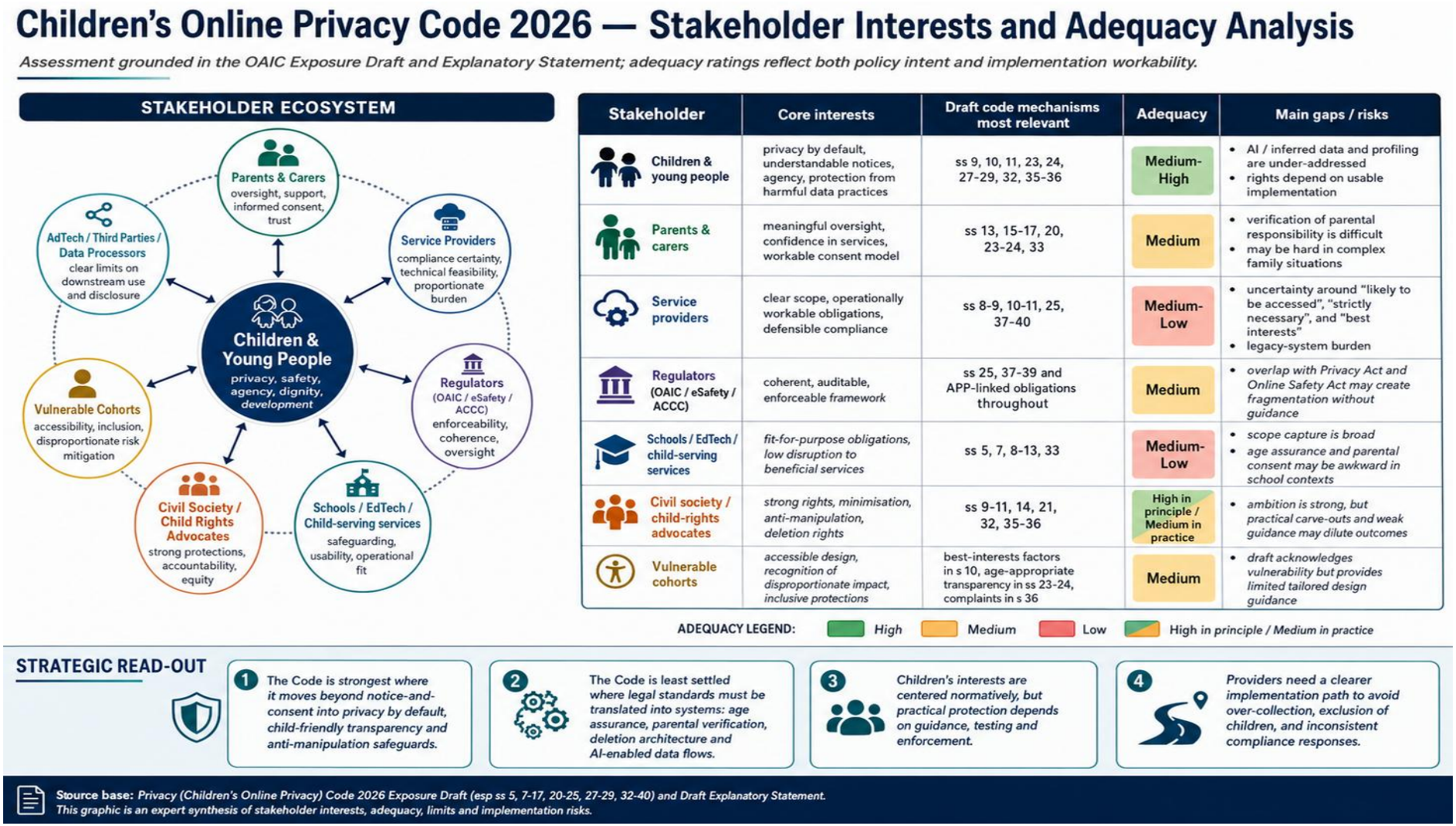


Figure B1. Stakeholder interests and adequacy analysis.

Stakeholder	Likely interest	Risk if unclear	Recommended OAIC support
Children and young people	Understanding, control, safety, autonomy and accessible remedies.	Notices remain unreadable; controls are nominal; complaints are hard to use.	Child-tested model notices, complaints, pathways and guidance for different age ranges.
Parents and carers	Ability to support children without excessive surveillance or identity proofing.	Parental consent becomes burdensome or otherwise excludes children from beneficial services.	Guidance on parental responsibility and proportional verification.
Industry and online services	Clear, implementable obligations and predictable enforcement expectations.	Over-collection for age assurance; fragmented controls; defensive service withdrawal.	Implementation checklists, safe-harbour examples and phased commencement.
Schools and edtech	Alignment with education, child safety, record retention and learning analytics.	Confusion over school-authorised services and student data controls.	Sector-specific examples for education technology and school management systems.
Civil society and child welfare bodies	Strong, enforceable protections and meaningful child participation.	Principles become diluted through weak implementation.	Public transparency on PIAs, complaint outcomes and regulatory guidance.
OAIC and peer regulators	Effective, enforceable, coherent regulatory framework.	Inconsistent enforcement and duplication with online safety and consumer regimes.	Regulatory coherence map and shared guidance with relevant regulators.

B2. Limits, Risks and Adequacy Gap Analysis

Explanatory notes

- **Purpose of the diagram** Figure B2 identifies the highest-priority issues for finalising the Code and presents a heatmap of adequacy against core implementation risks.
- **Priority matrix interpretation** The most important unresolved issues are technically complex: age assurance, best interests operationalisation, deletion architecture and AI/inferred data/profiling. These issues require guidance capable of being translated into systems, controls and evidence.
- **Heatmap interpretation** The draft Code is most robust where obligations can be implemented through governance, content, notices, training and complaint processes. It is most fragile where

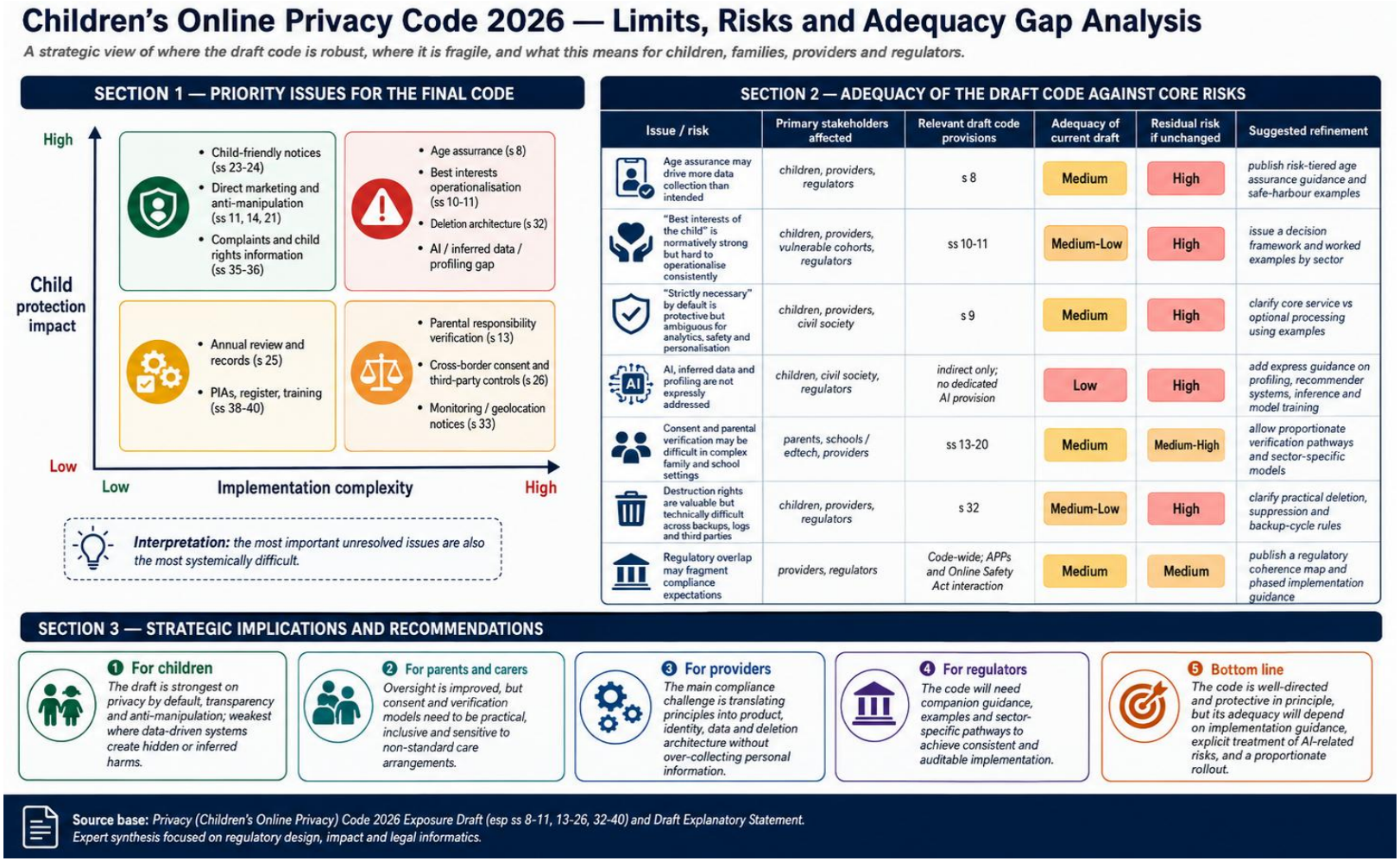


Figure B2. Limits, risks and adequacy gap analysis.

- obligations interact with identity systems, product architecture, parental verification, third-party processors, backups, logs, recommender systems and AI-enabled data flows.
- **Regulatory implication** The final Code would benefit from risk-tiered guidance, model decision frameworks, safe-harbour examples, sector-specific implementation models and a regulatory coherence map. These materials would strengthen the Code by making it more consistently enforceable and operationally credible.

B3. Consolidated recommendations aligned with Figures B1 and B2

Set out below are Recommendations 1-18 represented in Figures B1 and B2 above. These recommendations and supporting Regulatory Design Rationale (**Rationale**) support the key recommendations set out in the body of AUSCL's submission.

Recommendation	Detail	Rationale
1 - B1 Children and young people	Strengthen protection against hidden data practices and inferred harms	Require child-appropriate explanations of direct collection, observed data, inferred data, profiling, personalisation, AI training and automated decision-making, including how children or parents/carers can control or object to those practices.
2 - B1 Parents and carers	Improve parental and carer oversight without creating exclusion or inappropriate disclosure risks	Support parental involvement while recognising that parental involvement is not always simple or always in the child's best interests. Guidance could address family violence, care arrangements, separated families, hospital contexts and confidential support services.
3 - B1 Parents and carers	Improve parental and carer oversight without creating exclusion or inappropriate disclosure risks	Support parental involvement while recognising that parental involvement is not always simple or always in the child's best interests. Guidance could address family violence, care arrangements, separated families, hospital contexts and confidential support services
4 - B1 Service providers	Improve certainty through implementation-ready guidance, decision trees and evidence standards	Clarify threshold concepts, including likely child access, service/activity boundaries, strictly necessary processing, unknown-age users, legacy accounts and expected compliance evidence
5 - B1 Regulators	Support enforceability through defined	Specify expected artefacts such as applicability assessments, children's data inventories, age assurance risk assessments, strict necessity registers, best

Recommendation	Detail	Rationale
	compliance artefacts and auditable evidence requirements	interests assessments, consent registers, PIA registers, destruction request logs, vendor registers and training records
6 - B1 Schools, edtech and child-serving services	Provide tailored guidance for schools, edtech, hospital-based services, child charities and youth organisations	Address school authorisation, hospital referrals, mixed offline/online delivery, moderated child communities, safeguarding records, student data, learning analytics and services delivered to children through institutions or professionals
7 - B1 Civil society and child-rights advocates	Preserve strong child-rights protections while clarifying practical implementation	Do not dilute core protections. Instead, make them more effective by setting clear standards, model controls, examples, evidence requirements and proportionate implementation pathways
8 - B1 Vulnerable cohorts	Strengthen protections through inclusive design guidance	Explain how notices, controls, complaints pathways and consent processes are best made accessible to children with disability, neurodivergent children, Aboriginal and Torres Strait Islander children, culturally and linguistically diverse children, children in care, children experiencing illness or trauma, and children in regional or remote communities
9 - B1 Third parties, adtech and processors	Clarify downstream obligations for third-party recipients and processors	Require entities to identify downstream recipients, restrict secondary use, flow down deletion and withdrawal obligations, control cross-border disclosures and prevent repurposing for profiling, behavioural advertising or unrelated commercial purposes
10 - B1 Beneficial child-facing charities and wellbeing services	Provide a proportionate pathway for child-facing charities, hospital-adjacent services, wellbeing programs and peer-support communities	Distinguish exploitative data practices from proportionate data handling needed for safeguarding, eligibility, moderation, wellbeing support, accessibility, service delivery and child-safe community management

Recommendation	Detail	Rationale
11 - B2 Age assurance	Publish risk-tiered age assurance guidance and safe-harbour examples	Clarify when self-declaration, age-banding, parental attestation, estimation, verification or applying Code-level protections to all users will be sufficient. The guidance can prevent age assurance from becoming a driver of excessive collection of personal identity or sensitive information
12 - B2 Best Interests of the Child	Issue a best interests decision framework with worked sector examples	Translate the standard into a practical assessment covering purpose, necessity, proportionality, child benefit, likely harm, affected cohorts, less intrusive alternatives, transparency, control and safeguards.
13 - B2 Strictly necessary by default	Clarify the distinction between core service delivery and optional processing	Provide examples distinguishing account creation, security, moderation and core functionality from optional analytics, personalisation, advertising, fundraising, service improvement, recommender systems and AI model development.
14 – B2 AI, profiling and inferred data	Add express guidance on AI-enabled processing, recommender systems, profiling, inference and model training	Confirm that inferred information about a child may constitute personal information where the child is reasonably identifiable, and assess AI-enabled practices against privacy-by-default, best interests, transparency, consent, PIA, access and destruction obligations
15 – B2 Parental consent and verification	Allow proportionate parental verification pathways and sector-specific consent models	Recognise separated families, kinship care, out-of-home care, school-authorised services, hospital-based services, disability contexts and mature-minor scenarios. Permit reasonable reliance on institutional, professional or authorised-referrer confirmation where appropriate
16 – B2 Destruction rights	Clarify practical deletion, suppression and backup-cycle rules	Explain how destruction applies to active systems, backups, logs, audit trails, safeguarding records, legal holds, processors, derived data and AI-related data. Recognise deletion, irreversible de-identification, suppression from active use and deletion through documented backup cycles where appropriate
17 – B2 Regulatory coherence	Publish a regulatory coherence map and phased	Map the Code against the Privacy Act, APPs, Online Safety Act, eSafety initiatives, Australian Consumer Law, direct marketing rules, child safety frameworks and AI

Recommendation	Detail	Rationale
	implementation guidance	governance expectations. Provide a practical implementation sequence
18 – B2 Digital legislative twin / legal informatics implementation model	Publish a regulatory coherence map and phased implementation guidance	Map the Code against the Privacy Act, APPs, Online Safety Act, eSafety initiatives, Australian Consumer Law, direct marketing rules, child safety frameworks and AI governance expectations. Provide a practical implementation sequence
19 – B2 Digital legislative twin / legal informatics implementation model	Publish a non-binding digital legislative twin of the final Code, including obligation logic, decision trees, model controls, evidence artefacts and conformance scenarios	This would make the Code more implementation-ready, reduce interpretive fragmentation, and support auditability and regulatory coherence without weakening child protections

About AUSCL

The Australasian Society for Computers and Law (AUSCL) is a multidisciplinary association bringing together professionals from law, technology, government, academia and industry to advance the responsible development, governance and regulation of digital technologies.

AUSCL contributes to public policy, professional education and thought leadership across areas including artificial intelligence, privacy, cyber security, digital identity, computational law, digital government, critical infrastructure and emerging technologies.

Contributors

AUSCL Data and Privacy Working Group

AUSCL Future Law Working Group

Contact Details

contact@auscl.org

Attention: AUSCL Lead Policy Analyst

Disclaimer

This submission has been prepared by the Australasian Society for Computers and Law (AUSCL) for the purpose of contributing to public policy, law reform and regulatory discussions.

The views and recommendations expressed in this submission do not necessarily reflect the views of any individual member, contributor, employer, client, government agency, academic institution or other organisation with which a contributor may be associated.

This submission is intended to provide general information and policy analysis only. It does not constitute legal advice, professional advice or any other form of advice and should not be relied upon as such. Readers should obtain independent professional advice appropriate to their circumstances.

This submission has been informed by the expertise of AUSCL members and working groups across law, technology, government, academia and industry. Participation in the development of this submission does not imply endorsement of every view, recommendation or conclusion contained within it.

While reasonable care has been taken in the preparation of this submission, AUSCL makes no representation or warranty as to the completeness, accuracy or currency of the information contained in it and accepts no liability for any loss or damage arising from reliance upon its contents.

Suggested citation

Australasian Society for Computers and Law (2026). Office of the Australian Information Commissioner (OAIC). AUSCL Policy Series PS-2026-01.