



Submission to the OAIC

Privacy (Children's Online Privacy) Code 2026

Exposure Draft Consultation

Submitted by: Skillo App (skillo.au and skilloapp.com.au)

Date: May 2026

Consent to publication: Granted.

1. Executive Summary

Skillo App is an Australian student assessment and practice platform for Years 3 to 9, covering literacy and numeracy across the full primary-to-secondary transition. The service is offered free to students and families, and as a subscription product to Australian schools. Skillo App was designed from inception to comply with the proposed Children's Online Privacy Code (the Code).

This submission supports the Code in its current form. It is offered as evidence that a privacy-first architecture is achievable for Australian EdTech today, without compromising on product utility or commercial viability — and to provide an implementer's perspective on five specific provisions where additional OAIC guidance would meaningfully assist small Australian operators.

2. Scope and Applicability

Skillo App is squarely within the scope of the Code. Note 1 to Section 5 of the Exposure Draft expressly identifies 'online school management systems that monitor student performance' as services primarily concerned with the activities of children. The Skillo App school product is exactly such a service. We accept that we are an entity bound by the Code and have built accordingly.

Skillo App replaces a category of educational tools currently used by most Australian schools — standardised assessment platforms and weekly practice products. The market is mainstream, not niche. This submission therefore reflects practical implementation experience relevant to a wider category of Australian EdTech, not a single boutique service.

3. Position Summary

We support the Code as drafted. We particularly support:

- The best interests of the child standard in Sections 10 and 11.
- The default-minimisation requirement in Section 9.
- The strict consent provisions in Division 2, especially the prohibition on bundled consent in Section 14.
- The right to request destruction in Section 32.

- The mandatory privacy impact assessments in Section 38, with a public register under Section 39.

Our concerns are operational rather than principled. They relate to ambiguity around age assurance (Section 8), verification of parental responsibility (Section 13), and the format of the public register of privacy impact assessments (Section 39). These are addressed in our recommendations at the end of this submission.

4. Implementer's Perspective — Meeting the Code in Practice

This section maps the major Code requirements to specific implementation decisions. It is offered as a worked example, not as a recommended approach for all entities. Larger services with installed user bases face different constraints than newer services that can make foundational architectural decisions.

Section 8 — Ascertaining age of end-users

The free product requires no account, no email, and no age input. Anonymous practice is the default state. No personal information is collected unless and until a user voluntarily creates an account, which eliminates most age-assurance obligations at the point of entry.

In the school product, students do not self-register. They are added to a class by a teacher who has independently verified the student's year level through the school enrolment system. Age is ascertained through an established institutional process rather than user self-declaration.

Section 9 — Strict necessity by default

The free product collects zero personal information from children by default. The school product collects only: first name, last initial, year level, and class membership. No surname, no date of birth, no email, no address, no phone, no photograph, no voice recording, no biometric, no geolocation, no behavioural advertising identifier, and no device fingerprint is collected from any student.

Where personal information is collected, it is encrypted at the application layer (AES-256-GCM) with searchable fields handled through HMAC blind indexing so plaintext never appears in database queries or query plans. We submit that the strict-necessity requirement in Section 9 is best implemented at the data layer, not merely in policy language.

Sections 10 and 11 — Best interests of the child

Several design choices reflect the best-interests standard:

- No advertising, no behavioural tracking, no third-party trackers, no resale of any data, no cross-context behavioural advertising.
- Revenue comes entirely from school subscriptions and direct family subscriptions.
- No social features. Students cannot message each other, cannot see other students' scores, and cannot be contacted by anyone outside their class.
- No compulsive-use mechanics. Practice streaks reset humanely. No notifications outside school hours. Sessions have natural completion points.
- Age-appropriate UI throughout. Consent prompts, error messages, and explanatory text are tested for readability at the youngest age in each target range.

Division 2 — Consent

For students under 15, consent is collected from the school under existing parental consent arrangements for educational technology use, consistent with Section 13(2). Teachers receive a clear written notice covering each element required by Section 15(3) before adding any student to a class.

Bundled consent is not used. Pre-ticked boxes are not used. Consent is granular per data category and per purpose. Access is not conditional on consent to non-essential collection — because non-essential collection does not occur.

Division 3 — Transparency

Two versions of the privacy policy are maintained: one written for adults, and one written for children aged 10–12 years (the default age under the Code's 'age appropriate' definition). Both use non-text elements to support comprehension and avoid legal or technical terminology where possible.

Annual review of privacy practices under Section 25 is committed to, and records of those reviews are kept.

Division 4 — Access and correction

Students access all personal information held about them through their own account. Teachers and school administrators have appropriate read access for students in their classes. Access and correction requests are handled within 30 days as required by Sections 30 and 31, through a self-service flow rather than a manual ticket process — consistent with the spirit of the child-friendly access requirement in Section 27.

Division 5 — Destruction

A one-click destruction flow is provided. Students, parents or school administrators can request destruction; data is destroyed within the 30-day window required by Section 32(7). Only an audit log entry recording that destruction occurred is retained. Retention schedules are published online.

Division 8 — Privacy impact assessments

A privacy impact assessment has been completed and is maintained on a public register, addressing each element required by Section 38(2): nature, scope, context, flow and purposes of personal information handling; strict-necessity justification; lawfulness analysis; best-interests assessment with reasoning; specific compliance information; and a documented risk-of-harm assessment.

Section 39's public-register requirement is one of the most valuable provisions in the Code. It transforms privacy impact assessment from a private compliance artefact into a public accountability mechanism. We strongly support this provision and have published our register in advance of the Code commencing.

5. Recommendations

Five recommendations are offered for the OAIC's consideration as the Code moves toward registration.

Recommendation 1 — Small-entity implementation guide

The Code applies equally to multinational platforms and to small Australian operators. Compliance burden does not scale proportionately. Many small Australian EdTech operators are unaware the Code

applies to them. We recommend the OAIC publish a plain-language implementation guide for small entities, with example PIA templates, example child-friendly privacy policies, and example consent notices. This would substantially raise compliance among small operators without further regulatory action.

Recommendation 2 — Clarify age-assurance for school-mediated services

Section 8 requires reasonable steps to ascertain end-user age before collecting personal information. For services where age is ascertained through a school enrolment process, the Code does not explicitly recognise institutional verification as a reasonable step. We recommend the Explanatory Statement confirm that age verified through an established school enrolment process satisfies Section 8 for entities providing services through a school relationship.

Recommendation 3 — Clarify parental responsibility verification for school enrolments

Section 13(2)(b) requires the entity to take reasonable steps to confirm that the person giving consent has parental responsibility. For school-mediated services, parental consent is captured through the school's enrolment paperwork before any digital tool is used. We recommend the Explanatory Statement confirm that an EdTech service may rely on the school's certification that parental consent has been obtained, as a reasonable step under Section 13(2)(b). Without this, every EdTech service must build parallel consent capture that duplicates the school's process without privacy benefit.

Recommendation 4 — Template for the Section 39 register

Section 39 requires entities to publish a register of privacy impact assessments. The Exposure Draft does not specify a format, schema, or required fields. We recommend the OAIC publish a non-binding template for the register. A consistent format would also make the register useful to researchers, journalists, and parents comparing practices across services.

Recommendation 5 — Tiered commencement for smaller Australian operators

The Code must be registered by 10 December 2026. The commencement date is not yet set. We suggest the OAIC consider a tiered commencement: immediate for entities above a defined size threshold, with a 12-month grace period for smaller Australian operators below that threshold. This protects the Code's integrity for large platforms while giving smaller operators time to comply — reducing the risk that the Australian market is effectively ceded to overseas operators with larger compliance budgets.

6. Closing

Australia has the opportunity to set a global benchmark for children's online privacy. The Code as drafted is strong, workable and proportionate to the privacy risks it addresses. We thank the OAIC for the depth of consultation conducted to date. Skillo App is available to discuss any aspect of this submission with the OAIC.

 Founder and CEO, Skillo App, info@skillo.au
skillo.au • skilloapp.com.au