

Submission on the exposure draft

Online Safety Amendment (Digital Duty of Care) Bill 2026

Oiva Developments Pty Ltd | ACN 693 621 457

To: Department of Infrastructure, Transport, Regional Development, Communications, Sport and the Arts

Date: 22 September 2026

Contact: John Hutchison, Chief Technology Officer | john@oiva.com.au

Our position

Oiva supports an enforceable digital duty of care. Children and families should be protected through the design and operation of online services, including services that hold information about children who never use those services themselves.

We seek practical requirements that developers can implement and regulators can enforce. We do not seek a sector exemption. A closed education and care platform should demonstrate that it manages its actual risks, with the depth of its assessment and evidence proportionate to those risks.

Our principal requests are to:

- provide a streamlined assessment pathway while retaining meaningful annual review;
- clarify responsibility across software providers and their business customers;
- distinguish essential safety and care functions from features that encourage harmful engagement;
- coordinate online safety, privacy and education requirements; and
- place clear safeguards around research access, assumed identities and public reporting involving children's information.

About Oiva and the service being developed

Oiva is a small Australian company developing software for early childhood education and care. The platform is intended to support enrolments, Child Care Subsidy administration, regulatory compliance, educator documentation and communication with families.

Our intended model uses provider-managed accounts for identified educators, staff and parents or guardians, with access limited by role and authority. Learning observations, photographs and incident information are intended for authorised recipients. Educator drafting tools are being designed to require human review and approval before material is released to families.

This model requires careful assessment of account misuse, inappropriate access, incorrect family permissions and disclosure of children's information. Any users under 18, including young parents or trainees, also need to be considered. Account restrictions alone cannot establish that a service is safe.

Scope of this submission

Our detailed recommendations concern Schedule 2 and its implementation in education and care. We ask eSafety to provide worked examples showing how section 25A applies to integrated business software, including messaging, access to records and generative drafting tools. Classification should identify the relevant service boundaries and duties without assuming that overlapping functions necessarily require duplicate assessments.

Section references below are to the proposed provisions in the September 2026 exposure draft.[1]

1. Make proportionality practical

Sections 25H and 26A

Section 25H already calibrates the duty to risk, available measures, cost and privacy. Section 26A requires annual written assessments. The implementation question is how a smaller service can provide sufficient evidence without unnecessary duplication.

We recommend a streamlined assessment template for services with restricted membership, defined purposes and limited distribution. Eligibility should depend on demonstrated controls and actual risks, rather than company size or a label such as "closed platform". The template should cover access permissions, misuse by authorised accounts, incident response and the sensitivity of children's records.

Annual review should remain meaningful. A provider should be able to update a maintained assessment and record the effectiveness of its controls, rather than rewrite unchanged material. More extensive analysis should be required where the service introduces public discovery, wider sharing, direct interaction with children or other significant risks.

2. Allocate responsibility according to actual control

Sections 25A(2), 26 and 26A

The definition of responsibility includes provision and day-to-day control. Guidance should distinguish control of a platform from control of an individual customer's environment.

For a software provider, relevant responsibilities may include system design, access mechanisms, security, audit facilities and response to technical incidents. For an education provider, they may include account authorisation, staff access, family permissions, approval of records and local complaints handling. Some tasks require cooperation.

We recommend that the legislation and guidance:

- explain when a business customer has sufficient control to be a responsible person, and avoid treating an ordinary staff role as conclusive;
- allow a shared assessment with a clear responsibility matrix and customer-specific additions; and
- direct information requests and remedial action to the entities able to supply the information or implement the remedy.

Contracts should record operational responsibilities without allowing statutory duties to be transferred away. A common assessment should also identify who owns each action and how the entities will respond when a problem crosses their respective areas of control.

3. Address children whose records are held by adult users

Sections 25B, 25E and 26A

Section 25E already accommodates harm involving non-users. We recommend practical guidance for applying that protection to children whose images and records are handled by adults.

A sector template should address incorrect recipient selection, excessive staff access, retained access after employment ends, misuse by an authorised adult, disputed parental authority and the extraction or resharing of photographs. It should also address grooming or coercive conduct through family communication channels.

Worked examples should show how to assess the likelihood and consequences of these events, select proportionate controls and test whether those controls work. They should consider affected children and families even when neither holds an account, and include practical reporting and escalation pathways.

4. Recognise relevant controls under existing child safety laws

Section 25H and implementation guidance

Education and care providers operate within an existing child safety framework. Regulation 168 requirements concerning digital technology policies commenced in September 2025.[2] Further device restrictions commenced in February 2026, with jurisdictional differences and commencement details that providers must check.[3]

We recommend that eSafety, ACECQA, state and territory regulatory authorities and the OAIC develop consistent examples of evidence that can support compliance across their respective regimes. These could include image authorisations, access controls, staff training, incident procedures and records of how controls are applied.

Compliance with another law should be relevant evidence, assessed for its effectiveness against the risk in question. It should not automatically establish compliance with the digital duty. The objective is to reuse reliable evidence while identifying any additional online safety action needed.

5. Distinguish essential functions from harmful engagement design

Sections 25B, 25F, 25G and 26

The logged-in definition in section 25F(3) concerns account access to endless-feed, feedback or time-limited features. Authentication alone does not satisfy that definition. The express under-16 restriction in section 25B(1)(c) concerns social media services; broader safety duties remain relevant elsewhere.

We recommend clearer drafting and worked examples for ordinary education functions. In particular, clarify whether selecting a child's records for an authorised guardian falls within the broad recommender definition, and whether a private acknowledgement that an incident notice has been read is a feedback feature.

These examples should distinguish access control and task completion from mechanisms intended to increase attention or engagement. A functional distinction is preferable to a blanket exemption for everything labelled educational or essential.

Any user empowerment requirements should preserve secure authentication, effective delivery of legally required notices and necessary safety records. They should allow reasonable choices about delivery methods without preventing a provider from discharging its legal obligations. Such protections should be explicit when instruments are developed, rather than left for individual software businesses to infer.

6. Recognise meaningful human review of generated drafts

Sections 25H and 26A

We recommend that guidance recognise human review as a risk control where it is supported by an effective workflow. A reviewer should have suitable knowledge, sufficient time, access to the underlying record and authority to correct or reject the output.

Useful evidence includes approval records, clear responsibility for release and checks that a draft relates to the correct child. Guidance should also address harmful output seen by the reviewer, inaccurate statements, inappropriate language, disclosure to an external processor and material copied from another child's record.

Review should be assessed for effectiveness rather than treated as an exemption for generative tools. Oiva's intended approach requires educator approval before a generated draft is shared with a family. We would welcome worked examples showing what evidence is sufficient to demonstrate that this control is operating as intended.

7. Assess education and care communications in context

Sections 25C, 25D and 26

An incident report, developmental observation or health notice may describe injury, distress or behaviour because an authorised recipient needs that information to protect a child. Safety measures should account for purpose, audience, necessity and access restrictions.

We recommend guidance on lawful educational and care records, including communications required by law. It should explain when contextual review, restricted access or an appropriate warning is preferable to withholding information.

An educational label must not shield abusive, exploitative or unnecessary material. Equally, automated moderation should not prevent a family or regulator from receiving information needed for a child's care. Services need a clear escalation route when a safety filter blocks a legitimate notice.

8. Permit proportionate assessment of software changes

Section 26A(3)(a)(ii)

We recommend a documented screening process for releases, linked to the maintained risk assessment. The process should identify whether a change could create or increase a risk and record the reasons for that conclusion.

Where a change affects risk, a targeted assessment should update the relevant controls and evidence before release. It should not require unrelated parts of an otherwise current assessment to be rewritten. Examples should distinguish changes to sharing permissions, recipient selection or model behaviour from a correction that has no relevant effect on risk.

Guidance should explain how to handle urgent security fixes, including rapid assessment before deployment and prompt completion of supporting records. Any legislative clarification should preserve assessment of reasonably foreseeable risks while making clear that the depth of review is proportionate to the change.

9. Coordinate assessments, guidance and public reporting

Sections 26A, 26E, 192G and 192M

We recommend a common evidence structure for online safety and privacy assessments, with a clear mapping to each applicable legal requirement. Reuse should reduce duplicated work without treating different duties as interchangeable.

The draft Children's Online Privacy Code expressly addresses services primarily concerned with children's activities. Its proposed privacy assessment triggers include new services and significant changes to handling children's information; it proposes publication of an assessment register, not automatic publication of every assessment.[4] Implementation guidance should distinguish these requirements from the digital duty's requirements.

We recommend requiring core guidelines and assessment templates to be finalised at least six months before the duty commences, following consultation. Guidance should explain service boundaries, design-related harms, shared responsibility and the timing of initial assessments. Providers should have a clear implementation period after material requirements are settled.

Public reporting should disclose meaningful safety information while protecting children. Extend protections equivalent to section 192G expressly to provider publication under section 192M, and protect security-sensitive details. Redacted public summaries can be accompanied by fuller confidential information for the regulator where required.

Distinguish assessment retention from operational data retention. The six-year requirement in section 26A concerns assessments. Guidance should discourage copying identifiable records into them unnecessarily and address applicable retention and deletion duties for other records.

10. Safeguard research and assumed identities involving children

Part 14, particularly sections 205B to 205L

Independent research and regulatory investigation can expose serious failures. Closed membership should not prevent legitimate scrutiny. However, access to identifiable children's records deserves stronger safeguards than ordinary observation of public content.

We recommend express safeguards in the legislation and research access rules:

- **Necessity and minimisation:** prefer synthetic, aggregate or appropriately de-identified data where it can answer the research question. Assess re-identification risk, especially for photographs and small groups.
- **Additional authorisation:** require documented necessity, proportionality and independent authorisation before research or an assumed identity accesses identifiable children's information in a restricted service. Retain ethics approval and impose enforceable conditions appropriate to the proposed activity.
- **Controlled access:** use secure environments, limited permissions, time limits, access records, restrictions on downloading and resharing, and clear deletion requirements. Require a response process for accidental disclosure or discovery of a child safety risk.
- **Careful interaction:** prevent unnecessary contact with children, families or educators and avoid interference with care decisions, incident reports or family permissions. A research account should not falsely establish legal authority over a child.
- **Coordination where appropriate:** use supervised testing and coordinate with service operators where this would not compromise a legitimate investigation. Require reasons when covert access is necessary.

The assumed-identity authorisation and good-faith civil immunity are distinct. We recommend clearly defining the permitted activity and its limits, including how overriding provisions interact with child protection, privacy and confidentiality obligations. Authorisation should not displace protections unrelated to the authorised task.

These safeguards should enable useful scrutiny while avoiding unnecessary collection or exposure of children's information. A blanket exclusion for closed services would not achieve that balance.

Oiva's approach and further participation

Our design priorities include Australian hosting and processing, separation of provider environments, role-based access, recorded human approval before release of generated drafts, and audit records with retention appropriate to their purpose and legal requirements. We intend to maintain a written risk assessment from launch and update it through our release process.

We would welcome participation in developing education and care examples, a practical assessment template and coordinated implementation guidance. Clear requirements now will help Australian developers incorporate effective safeguards during product development.

Publication

This submission is provided on behalf of Oiva Developments Pty Ltd. We do not request confidential treatment. Please direct any questions to John Hutchison at john@oiva.com.au.

Sources

[1] Department of Infrastructure, [Exposure draft Bill, September 2026](#).

[2] ACECQA, [NQF child safety changes from September 2025 and January 2026](#).

[3] ACECQA, [Using digital devices in centre-based education and care services](#).

[4] OAIC, [Draft Children's Online Privacy Code](#), sections 5, 7, 38 and 39.