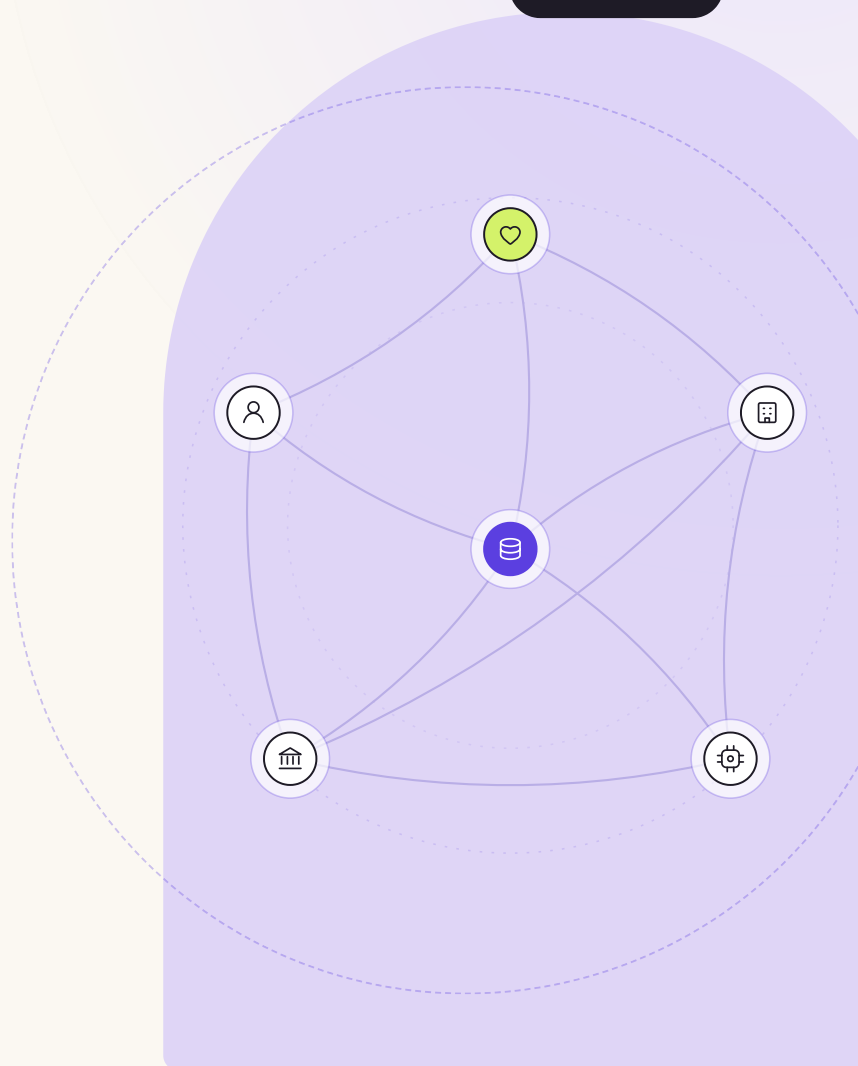




FREE GUIDE



CHECKLIST · PRIVACY & DATA PROTECTION

Children's privacy readiness checklist

A readiness checklist for online services likely to be accessed by children, ahead of the OAIC's Children's Online Privacy Code.

Updated 17 October 2026

Consultation

lexoraai.com.au

The Privacy and Other Legislation Amendment Act 2024 inserted section 26GC into the Privacy Act, requiring the Information Commissioner to develop and register a Children's Online Privacy Code within 24 months of Royal Assent, which means by **10 December 2026**. The code will set out how the Australian Privacy Principles (APPs) apply to children's privacy.

Where things stand. The OAIC released an exposure draft of the code on 31 March 2026, and public submissions closed on 5 June 2026. The OAIC says it is working towards registering the code by 10 December 2026. The final code may differ from the draft, so treat the points below as readiness steps, not final requirements.

Who the code is expected to cover

Under section 26GC, the code binds APP entities that provide a social media service, relevant electronic service or designated internet service (as defined in the Online Safety Act 2021), where the service is likely to be accessed by children and the entity is not providing a health service. The code itself can also include or exclude specified entities. The OAIC's media release describes the draft as also covering services primarily concerned with children's activities.

The phrase "likely to be accessed by children" is broader than "designed for children". General audience apps, games, platforms and websites may be caught.

1. Know your users

- ☐ Assess whether children are likely to use your service, using evidence such as audience data, marketing, app store ratings and complaints.
- ☐ Record the assessment, the evidence used and who made the decision.
- ☐ Consider how you would establish a user's age, and how much personal information that process would itself collect.
- ☐ Decide whether it is simpler to apply child-appropriate protections to all users.

2. Settings and defaults

- ☐ List every setting that affects how personal information is collected, used, shared or made visible to others.

- ☐ Identify which settings are on by default, and why.
- ☐ Check whether location sharing, public profiles, contact from strangers and data sharing with third parties are enabled by default.
- ☐ Consider how changes to defaults would apply to existing accounts, not just new ones.

Commentators, including Allens, describe the exposure draft as proposing that only strictly necessary handling occurs by default, with children able to control other handling through simple settings.

3. Notices and transparency

- ☐ Review whether privacy notices and policies could be understood by the children likely to use the service.
- ☐ Check that notices explain, in plain terms, what is collected, why, and who it is shared with.
- ☐ Identify where parents are asked to consent, and whether the child is told.
- ☐ Identify any parental monitoring or location-tracking features, and whether the child is told when they are being tracked.

The OAIC's media release says the draft proposes age-appropriate notices and that children be told when a parent consents for them and when others are tracking their location.

4. Data minimisation and retention

- ☐ Map the personal information collected from or about child users, including information inferred or generated by your systems.
- ☐ For each item, record why it is needed for the service.
- ☐ Remove collection that is not needed.
- ☐ Check how a child, or a parent, could ask for their information to be deleted, and how quickly you could act.

5. Profiling, personalisation and marketing

- ☐ Identify any profiling, recommender systems, behavioural analytics or targeted advertising that uses children's information.
- ☐ Identify any direct marketing to child users, and where the information used came from.
- ☐ Record whether each practice relies on consent, and how that consent is obtained.
- ☐ Remove pre-ticked boxes, bundled consents and design patterns that nudge users to share more.

The OAIC's media release says the draft proposes that direct marketing to children be permitted only with consent, where it is in the child's best interests and where the information was collected directly from the child, and that consent be required before children's information is used for targeted advertising.

6. Governance

- ☐ Name an owner for children's privacy readiness.
- ☐ Plan privacy impact assessments for new features likely to be used by children.
- ☐ Brief product, marketing and engineering teams on the "best interests of the child" principle in the draft.
- ☐ Set a date to review the final code once it is registered and update this checklist.

Next step

This checklist shows where your service stands today; the final code will set the actual requirements. Lexora's Privacy Governance Framework can help put the ownership and decision-making in place to respond when it is registered.

General information, not legal advice. The Children's Online Privacy Code has not yet been registered and its final content may differ from the exposure draft. Obtain legal advice on how it will apply to your service.

Sources

1. Privacy and Other Legislation Amendment Act 2024 (Cth), Schedule 1, Part 4 (section 26GC)
<https://www.legislation.gov.au/C2024A00128/asmade/text>
2. OAIC, OAIC releases exposure draft of the Children's Online Privacy Code (31 March 2026)
<https://www.oaic.gov.au/news/media-centre/oaic-releases-exposure-draft-of-the-childrens-online-privacy-code>
3. OAIC, Draft Children's Online Privacy Code consultation
<https://www.oaic.gov.au/engage-with-us/consultations/draft-childrens-online-privacy-code-consultation-for-industry,-civil-society,-academia>
4. Allens, Draft Children's Online Privacy Code (April 2026)
<https://www.allens.com.au/insights-news/insights/2026/04/draft-childrens-online-privacy-code-proposed-protections-to-have-material-impact-on-online-services/>



Better governance. *Greater confidence.*

Lexora is an Australian-first advisory business. We help organisations understand their privacy, data and AI obligations, assess risk, build governance frameworks and put practical controls in place.

OUR PRACTICES

Privacy & Data Protection

AI Governance & Responsible AI

Data Governance

Regulatory Readiness & Compliance

WAYS TO START

Privacy Health Check

AI Governance Readiness Assessment

Data Governance Review

Regulatory Readiness Consultation

DISCUSS YOUR GOVERNANCE NEEDS

lexoraai.com.au

info@lexoraai.com.au

More free guides: lexoraai.com.au/resources

This guide is general information, current at the date shown. It is not legal advice and does not take account of your circumstances. Lexora is not a law firm. Check the primary sources before relying on any date or requirement. © 2026 Lexora. You are welcome to share this guide unaltered, with this page attached.