



SUBMISSION

EXPOSURE DRAFT

PRIVACY (CHILDREN'S ONLINE PRIVACY) CODE 2026

5 June 2026

CONTACT US



info@calabashsolutions.net



www.calabashsolutions.net



Follow us on LinkedIn

5 June 2026

Office of the Australian Information Commissioner

GPO Box 5288

Sydney NSW 2001

Submission: copc@oaic.gov.au

Dear Privacy Commissioner,

Calabash Solutions welcomes the opportunity to make a submission on the Exposure Draft *Privacy (Children's Online Privacy) Code 2026*.

We are available for additional discussion, questions, and comments on our submission. We consent to the publication of all or part of our submission responses to public fora.

Calabash Solutions

EXECUTIVE SUMMARY

Calabash Solutions welcomes the opportunity to provide comment on the *Exposure Draft of the Privacy (Children's Online Privacy) Code 2026* (the **Children's Online Privacy Code**),¹ drafted in response to concerns with the adequacy of existing privacy protections for children in the online environment.

We continue to hold the view that APP Codes (like the Children's Online Privacy Code) or legislation (like the *Online Safety Amendment (Social Media Minimum Age) Act 2024*), targeted specifically towards protections for children, are a distraction from much needed privacy reforms which seek to redress existing deficiencies in the current *Privacy Act 1988* (Cth) (**Privacy Act**). Focusing on one cohort of the Australian population, and only then, on specific services of an entity likely to be accessed by, or primarily concerned with, the activities of that cohort, does nothing to address wholesale privacy reforms that will uplift protections for all Australians.

That said, Calabash Solutions is supportive of the consultation process adopted by the Office of the Australian information Commissioner (**OAIC**), in drafting the Children's Online Privacy Code. The consultation, based on research, evidence and extensive consultation with key stakeholders, including engaging with children, parents and relevant organisations focused on children's welfare. Calabash Solutions commends the OAIC's PRISM team on their commitment to stakeholder engagement, and hopes their model will be replicated for similar types of legislative reforms in the future.

Finally, we have confined the comments in this submission to aspects of the Children's Online Privacy Code we believe could be better clarified, to assist entities in complying with their obligations.

¹ *Privacy (Children's Online Privacy) Code 2026*. https://www.oaic.gov.au/_data/assets/pdf_file/0020/262631/Exposure-Draft-Childrens-Online-Privacy-Code.pdf

SECTION 5 ADDITIONAL ENTITIES BOUND BY THIS CODE

Calabash Solutions recommends that, per section 26GC(11) of the Privacy Act, the Privacy Commissioner makes **written guidelines** that will assist entities in determining whether a service (i) is likely to be accessed by children for the purposes of subparagraph (5)(a)(ii) of section 26 GC of the Privacy Act, or (ii) is primarily concerned with the activities of children for the purposes of subsection 5(b) of the Children's Online Privacy Code.

SECTION 8 ASCERTAINING THE AGE OF END-USERS OF AN ENTITY'S SERVICE

Subsection 8(1) of the Children's Online Privacy Code provides that, subject to subsection 8(3), before an entity collects personal information about an end-user of the entity's service, the entity must take steps that are reasonable in the circumstances to ascertain the age of the end-user.

Calabash Solutions is generally not supportive of requirements that seek to collect more personal information, and that seek to collect sensitive information in particular, from end-users, for the purpose of ascertaining their eligibility to use a particular service. Additional recommendations made against section 8 assume the age assurance requirements remain in place.

We recommend that subsection 8(1) be **strengthened to introduce a test of proportionality**. In its current drafting, it is unclear whether the collection of personal information for age assurance purposes is needed for end-users who are children, or for end-users who are not children. For example, if 5% of an entity's services are targeted at end-users that are children, it would be reasonable to expect that age assurance should not be needed for 95% of end-users who are not children. As currently drafted, subsection 8(1) appears to afford entities discretion as to which cohort of end-user age assurance is necessary. Absent clearly defined obligations that the collection of personal information to satisfy age assurance should be confined to the smallest cohort of end-user, a risk exists that entities collect personal information that is neither proportionate nor necessary. Confining principles such as necessity and proportionality to guidance material, such as the *Privacy guidance on age assurance technologies*,² does little to mandate compliance. This, coupled with the current drafting of subsection 8(4), could lead to the over-collection and over-retention of personal information by entities, which weakens privacy obligations generally for all end-users.

Calabash Solutions recommends that subsection 8(1) be amended to **more clearly articulate data minimisation principles** in addressing which cohort of end-user an entity targets when collecting personal information for age assurance purposes.

Subsection 8(4) provides that an entity must, as soon as practicable after complying with subsection 8(1), destroy sensitive information that is collected, subject to permitted exceptions. It is our view that requirements under subsection 8(4) should **not be confined to sensitive information only**. Rather, an entity should destroy all personal information that it collects under subsection 8(1), subject to permitted exceptions.

² Office of the Australian Information Commissioner. *Privacy Guidance on age assurance technologies*.
https://www.oaic.gov.au/_data/assets/pdf_file/0017/262043/OAIC-privacy-guidance-on-age-assurance-technologies.pdf

SECTION 9 ENTITIES MAY COLLECT ETC. PERSONAL INFORMATION ABOUT A CHILD BY DEFAULT ONLY IF STRICTLY NECESSARY

Section 9 of the Children's Online Privacy Code introduces a requirement for entities to establish privacy protections by default in the design of their online services.

Specifically, subsection 9(1) provides a double obligation for entities to (i) implement technical and organisational measures, and (ii) only collect, use or disclose personal information about a child that is strictly necessary to provide the entity's service.

Subsection 9(2) outlines what entities should do in those circumstances when they collect, use or disclose personal information about a child **that is not strictly necessary** for the provision of the entity's service.

Read together, subsections 9(1) and 9(2) can be seen to be less about an obligation to implement technical and organisational measures by default, and more about how an entity can collect, use or disclose personal information about a child that is **not** strictly necessary to provide the entity's service.

Calabash Solutions recommends that **requirements under section 9 be reviewed**, such that the entity must implement technical and organisational measures that ensure that, by default, the entity **only** collects, uses or discloses personal information about a child that is strictly necessary to provide the entity's service, with no allowable pathways for entities to lessen this obligation.

SECTION 10 COLLECTION OF PERSONAL INFORMATION ABOUT A CHILD MUST BE CONSISTENT WITH BEST INTERESTS OF THE CHILD

Calabash Solutions is generally supportive of section 10 of the Children's Online Privacy Code which introduces additional requirements for entities to collect children's personal information in ways that are consistent with the best interests of the child.

Considered together, requirements under the Privacy Act and the Children's Online Privacy Code introduce the following three obligations regarding the collection of personal information (other than sensitive information):

- Per Australian Privacy Principle 3.2 of the Privacy Act, the entity must not collect personal information (other than sensitive information) unless the information is **reasonably necessary** for one or more of the entity's functions or activities.
- Per subsection 10(1) of the Children's Online Privacy Code, an entity must not collect personal information (other than sensitive information) about a child unless the collection of the information is consistent with the **best interests of the child**.
- Per subsection 9(1) of the Children's Online Privacy Code, an entity must, in addition to implementing technical and organisational measures, only collect (and use or disclose) personal information about a child that is **strictly necessary** to provide the entity's service.

Together, these provisions provide three distinct tests on the collection of personal information: '**reasonably necessary**', '**best interests**', and '**strictly necessary**'.

Obligations under the Privacy Act and the Children's Online Privacy Code introduce these, plus the following additional requirement, on the collection of sensitive information:

- Per Australian Privacy Principle 3.3(a) of the Privacy Act, **consent** must be sought.

For entities wanting to do the right thing, Calabash Solutions recommends that **clear guidance be provided** on how to satisfy each of the distinct requirements, to outline what the Privacy Commissioner would consider acceptable under each provision.

SECTION 11 USE OR DISCLOSURE OF PERSONAL INFORMATION ABOUT A CHILD MUST BE CONSISTENT WITH BEST INTERESTS OF THE CHILD

Calabash Solutions is generally supportive of section 11 of the Children's Online Privacy Code which introduces requirements on the use or disclosure of children's personal information.

Regarding requirements related to Australian Privacy Principle 7 of the Privacy Act (see subsections 11(3) and 11(4)), it is unclear whether "**strictly necessary**" obligations from subsection 9(1) – an entity must, in addition to implementing technical and organisational measures, only (collect and) use or disclose personal information about a child that is strictly necessary to provide the entity's service - also apply, or whether Australian Privacy Principle 6.7 would exclude the "**strictly necessary**" obligation from subsection 9(1) from applying to the use or disclosure of personal information for direct marketing purposes. We recommend amendments to clarify how these obligations work together.

Assuming the "**strictly necessary**" obligation from subsection 9(1) does apply to all section 11 use and disclosure requirements, it would be difficult to conceive that the use or disclosure of personal information of a child for direct marketing purposes could ever meet the threshold of being **strictly necessary** and **in the best interests of a child**.

If the intent of section 11 is not to prohibit the use or disclosure of a child's personal information for direct marketing purposes, Calabash Solutions recommends the **addition of a new Note 3** under subsection 11(3) providing an example showing when direct marketing to a child would be both strictly necessary and in the best interest of the child.

Calabash Solutions makes the same recommendation against subsection 11(4) for the use or disclosure of sensitive information about a child for the purpose of direct marketing.

Note 1 under subsection 11(3) provides that the exception in Australia Privacy Principle 7.3 does not apply at all. This would imply that an entity is prohibited from using or disclosing personal information that is not sensitive information for direct marketing purposes where either (i) the information has been collected from the child and the child would not reasonably expect the organisation to use or disclose their information for that purpose, or (ii) the information has been collected from someone other than the child. The Australian Privacy Principle 7.3 exclusion implies that subsection 11(3) would only permit the use or disclosure of a child's personal information that is not sensitive information if the information was collected **from the child only** and not from a person with parental responsibility for the child. Amendment may be needed if this interpretation is inaccurate.

SECTION 13 CONSENT GIVEN BY CHILD OR PERSON WITH PARENTAL RESPONSIBILITY

Calabash Solutions is generally supportive of section 13 of the Children's Online Privacy Code pertaining to consent given by a child or person with parental responsibility for the child.

Subsection 13(2)(b) provides that the entity must take reasonable steps to confirm that the person who gives consent is a person with parental responsibility for the child. Section 13 of the *Exposure Draft Explanatory Statement Privacy (Children's Online Privacy Code) Code 2026*³ provides some examples of reasonable steps an entity may take to verify the person giving the consent is a person with parental responsibility for the child, and lists the provision of a form of government digital ID.

Calabash Solutions recommends that subsection 13(3) be **strengthened to align** with requirements under subsection 8(4), requiring entities to, as soon as practicable after verifying the person giving the consent is a person with parental responsibility for the child, destroy sensitive information that is collected for this purpose if (a) the information is not contained in a Commonwealth record, and (b) the entity is not required by or under an Australian law, or a court/tribunal order, to retain the information.

To assist entities meet their obligations under subsection 13(3), we recommend that the Privacy Commissioner develops a **children's consent notice template** or publishes children's consent notice **examples** to outline the OAIC's expectations of what good looks like.

Calabash Solutions further notes that if the Children's Online Privacy Code commenced the day after registration on 11 December 2026, section 13 requirements as currently drafted may take entities **longer to implement**. This could prove particularly challenging for entities:

- that have never had to contemplate consent provisions, under the current Privacy Act regime; or
- whose existing consent mechanisms do not extend to additional requirements imposed under subsection 15(4).

SECTION 14 CONSENT MUST BE VOLUNTARY

Calabash Solutions is generally supportive of section 14 of the Children's Online Privacy Code providing that consent to the collection, use or disclosure of personal information about a child must be voluntary.

We note that consent for the collection of personal information of a child is only required for personal information that is sensitive information. Thus, all provisions under Division 2 pertain to the collection of sensitive information only, about a child.

Taken together, subsection 14(3)(c) requirements - which introduce " **strictly necessary**" provisions - and subsection 9(2)(a) requirements - which gives entities the option of collecting personal information when it is not strictly necessary for the provision of the entity's service - appear contradictory.

³ Office of the Australian Information Commissioner. *Exposure Draft Explanatory Statement Privacy (Children's Online Privacy) Code 2026*. https://www.oaic.gov.au/_data/assets/pdf_file/0019/262630/Draft-Explanatory-Statement-Exposure-Draft-Childrens-Online-Privacy-Code.pdf

Calabash Solutions recommends that **one or both requirement/s be reviewed**, to ensure that entities looking for a loophole in their compliance obligations, are prevented from non-compliance with section 14 in its entirety.

SECTION 15 CONSENT MUST BE INFORMED

Calabash Solutions is generally supportive of section 15 of the Children's Online Privacy Code regarding informed consent.

Calabash Solutions notes that the obligation under subsection 15(5) – that a written consent notice provided to a child must be provided in terms and in a format that is simple, easy to understand and age appropriate – is absent from section 13. The subsection 15(5) requirement could be **added as a new requirement** under section 13, with the amendment *“when the notice is provided to a child”*.

SECTION 17 CONSENT CAN BE WITHDRAWN

Calabash Solutions is generally supportive of Section 17 of the Children's Online Privacy Code regarding the withdrawal of consent.

Absent in the current drafting of section 17 requirements is the ability of a child to withdraw their consent to the collection, use or disclosure of their personal information in situations where consent was initially provided by a person with parental responsibility for the child. Calabash Solutions **recommends that this scenario is clarified**, either through amendments to the current drafting of subsection 17(1), or through the addition of a section 17 note.

SECTION 20 ASSENT OF CHILD UNDER 15 YEARS MUST BE OBTAINED IN CERTAIN CIRCUMSTANCES

Calabash Solutions notes that if the Children's Online Privacy Code commences the day after registration on 11 December 2026, section 20 requirements as currently drafted may take entities **longer to implement**, due to technical constraints and the creation and retention of evidentiary documents to show this requirement has been met.

SECTION 23 APP PRIVACY POLICY REQUIREMENTS

Calabash Solutions is generally supportive of section 23 of the Children's Online Privacy Code, which outlines additional requirements for an APP privacy policy for services likely to be accessed by children.

To assist entities meet their obligations under subsections 23(3) and 23(6), we recommend that the Privacy Commissioner develops a **children's privacy policy template** or publishes privacy policy **examples** to outline the OAIC's expectations of what good looks like.

SECTION 24 NOTIFICATION OF THE COLLECTION OF PERSONAL INFORMATION

Similar to our observations made under section 23, Calabash Solutions recommends that the Privacy Commissioner develops a **children's privacy collection notice template** or publishes privacy collection notice **examples** to help entities meet their obligations under subsection 24(2).

SECTION 26 CONSENT TO CROSS BORDER DISCLOSURES

Subsection 26(1) provides that an entity must comply with section 26 in expressly informing a child of the matter in Australian Privacy Principle 8.2(b)(i).

As written, the current drafting of subsection 26(1) does not apply to expressly inform a person with parental responsibility for the child, of the matter in Australian Privacy Principle 8.2(b)(i). **Amendments may be required** if this interpretation is inaccurate.

To assist entities meet their obligations under subsections 26(2) and 26(4), we recommend that the Privacy Commissioner **develops a children's notice template** or publishes notification **examples** to outline the OAIC's expectations of what good looks like.

SECTION 28 RIGHT TO REQUEST INFORMATION ABOUT HANDLING OF PERSONAL INFORMATION

Calabash Solutions notes that subsection 28(2)(g) introduces the term "**profiling**", without an accompanying definition of this term in the Privacy Act nor Section 4 of the Children's Online Privacy Code.

To assist entities meet their obligations under subsection 28(2)(g) of the Children's Online Privacy Code, we recommend that a **definition is provided** to explain the term "profiling".

As written, the current drafting of subsection 28(5)(b) provides that an entity's response to a request made under subsection 28(1) **must** contain an explanation of the steps taken to comply with Australian Privacy Principle 8.1, if the child's personal information has been disclosed to an overseas recipient.

In contrast, subsection 28(2) list the types of information that **may** be requested by an individual.

This difference – the "**may**" provisions under subsection 28(2), compared with the "**must**" provisions under subsection 28(5)(b) - suggest the inclusion of subsection 28(5)(b) content is **always** required, even when not requested by the child or by the person with parental responsibility for the child. Calabash Solutions recommends that **the requirement under subsection 28(5)(b) be amended**, so that an explanation of the steps taken to comply with Australian Privacy Principle 8.1 **is only provided when requested**.

SECTION 30 DEALING WITH REQUESTS FOR ACCESS TO PERSONAL INFORMATION ABOUT CHILDREN

Calabash Solutions is generally supportive of section 30 of the Children's Online Privacy Code relating to timeframes for responding to access requests made under Australian Privacy Principle 12.

In its current drafting, subsection 30(1) applies when a child requests access to their personal information from an entity that is an organisation. The requirement is silent on timeframes when the request is made by a person with parental responsibility for the child.

Calabash Solutions recommends that subsection 30(1) (and potentially subsection 30(2)(b)) be amended to clarify whether **the same timeframes** would apply, when the request is made by a person with parental responsibility for a child.

SECTION 31 DEALING WITH REQUESTS TO CORRECT PERSONAL INFORMATION ABOUT CHILDREN

Similar to our observations made under section 30, Calabash Solutions recommends that subsection 31(1) (and potentially subsection 31(2)(b)) be amended to clarify whether **the same timeframes** would apply, when the request is made by a person with parental responsibility for a child.

SECTION 32 REQUEST TO DESTROY PERSONAL INFORMATION ABOUT A CHILD

Calabash Solutions is generally supportive of section 32 of the Children's Online Privacy Code relating to right to request the destruction of personal information about a child.

We note, however, that should the Children's Online Privacy Code commence the day after registration on 11 December 2026, section 32 requirements as currently drafted may take entities **longer to implement**, due to technical constraints, documentation requirements, third-party coordination, identification and documentation of legal exceptions, verification of identity and other factors contributing to deletion complexity.

SECTION 33 NOTIFICATION OF MECHANISMS THAT MONITOR OR CONTROL SERVICE USE OR MONITOR GEOLOCATION

Calabash Solutions is generally supportive of section 33 of the Children's Online Privacy Code for the notification of mechanisms that monitor or control service use or monitor geolocation.

To assist entities meet their obligations under subsections 33(2) and 33(3), we recommend that the Privacy Commissioner develops a **notification template** or publishes notification **examples** to outline the OAIC's expectations of what good looks like.

SECTION 38 PRIVACY IMPACT ASSESSMENTS

Calabash Solutions is generally supportive of section 38 of the Children's Online Privacy Code requiring entities to undertake a privacy impact assessment for new or changed services or activities.

To assist entities meet their obligations under subsection 38(2), Calabash Solutions recommends that the Privacy Commissioner develops a **privacy impact assessment template** to outline the OAIC's expectations of what good looks like.



OUR VISION

Healthy. Safe. Respected. Free.

We believe in a world where all people are healthy, safe, free, and respected.

OUR MISSION

Helping Others.

The best versions of ourselves emerge when we help others to be the best versions of themselves.

OUR APPROACH

Listen. Support. Analyse. Discover

- We value patient privacy, and work with health service providers to assure and implement compliant privacy programs.
- We listen to patients and carers as they talk about their journeys through all systems of care.
- We develop and deliver Continuous Professional Development (CPD) for clinicians, support staff, and practice managers.
- We work with small and medium datasets to understand what inhibits or enables treatment compliance within unique patient cohorts.
- We embrace solutions that work, from technology to the creative arts, to cultivate health systems that deliver patient-centred care.

OUR PRIVACY SERVICE OFFERINGS

Online Privacy Training

Designed specifically for private sector health care workers. Offers a commonsense, practical view of the Australian Privacy Principles. Demonstrates how to apply the Australian Privacy Principles in Australian private health care sector.

Face-to-Face Training

Register for face-to-face training delivered at your practice, for your team.

Face-to-face training lets you and your team discuss your practice-specific privacy questions, concerns.

Privacy Compliance Assessment

Does your practice comply with the Australian Privacy Act?

We assess your practice's compliance with the privacy principles using our privacy compliance assessment tools. Onsite visit and review of your privacy systems, processes, and practices against the thirteen Australian Privacy Principles contained in the Privacy Act.

Privacy Compliance Heat Map

After the privacy compliance assessment, we produce your unique privacy compliance heat map showing areas of strong and weak compliance against the thirteen Australian Privacy Principles.

Templated Privacy Processes

Use our privacy compliance heat map to uncover your areas of weak compliance.

We work with you to strengthen the gaps and create privacy processes for your practice

CONTACT CALABASH SOLUTIONS

W www.calabashsolutions.net

E info@calabashsolutions.net