SUBMISSION ON THE EXPOSURE DRAFT OF

THE CHILDREN'S ONLINE PRIVACY CODE

5 June 2026

Office of the Australian Information Commissioner
By email: copc@oaic.gov.au

Thank you for the invitation to make a submission on the Exposure Draft ('ED') of the Children's Online Privacy Code ('COPC'), in development under the *Privacy Act 1988* (Cth), section 26GC.

The authors of this submission are some of the members of the UNSW Public Interest Law & Tech Initiative, namely [redacted]

The UNSW Public Interest Law & Tech Initiative is an independent community of scholars focused on the interaction of law and technology to advance the public interest. We aim to provide an inclusive forum for discussion, debate, and deliberation on the interaction of law and tech, informing policy and building networks and understanding in these areas from our diverse expertise, disciplines, and perspectives. We facilitate engagement with stakeholders from academia, civil society, government agencies, media, industry, and the broader public. Our focus is also on the next generation, as we learn from, include and mentor students, higher degree research candidates and early career researchers.

The views expressed in this submission are not an institutional position, but our own views as researchers. This submission can be made public.

At the outset, we mention three overarching factors that, in our view, must inform the drafting, and expectations, of the COPC in general:

1) There is a strong consensus that the existing privacy protections created by the *Privacy Act 1988* (Cth) ('Act') and the Australian Privacy Principles ('APPs') are inadequate for children and adults alike, and that fundamental reforms are required to improve these protections. This situation will not be altered by the introduction of the COPC but will depend on anticipated 'second tranche' reforms to the Act as a whole. For instance, the COPC is necessarily based on

the same under-inclusive definition of 'personal information' that applies under the Act. The recognised inadequacy of these existing legislated protections shapes the privacy impacts of the COPC for both children and adults.

2) The capacity of the COPC to improve privacy protections for children is restricted by the fact that the COPC 'must set out how one or more of the [APPs] are to be applied or complied with in relation to the privacy of children',[1] and may, 'in relation to the privacy of children', 'impose additional requirements to those imposed by one or more of the [APPs], so long as the additional requirements are not contrary to, or inconsistent with, those [APPs]'.[2] Accordingly, the COPC privacy protections for children are constrained by the limitations of the existing APP framework: the Commissioner does not have a blank slate to create new online privacy rules for children.

3) The COPC may also *degrade* privacy protections for people over the age of 18 if it requires or incentivises APP entities to collect additional personal information, including sensitive information, about people over the age of 18, such as personal information collected for the purposes of age assurance or establishing parental responsibility. Since the COPC must create rules 'about the online privacy of children' and can impose additional requirements 'in relation to the privacy of children',[3] it is arguable that it cannot impose obligations about how APP entities must treat the additional personal information collected about adults as a result of the COPC. People over the age of 18 will likely be left with the existing inadequate protections of the Act in respect of personal information collected as a result of the COPC. Accordingly, any COPC provisions that would create an obligation or incentive for APP entities to collect personal information about individuals over the age of 18 should be strictly minimised.

We appreciate that these factors and others create complexity in the development of the COPC. We make suggestions and recommendations concerning specific drafting of provisions in the ED below.

1. 'Entity' versus 'APP entity': ED, section 4

The term 'entity' is used throughout the ED to refer to entities covered by the COPC. The note to section 4 of the ED states that several expressions used in this instrument are defined in section 6 of the Act, including 'entity'.

'Entity' is defined as 'an agency, an organisation or a small business operator' in subsection 6(1) of the Act, in contrast to an 'APP entity' which is defined as 'an agency or organisation' in the same

[1] *Privacy Act 1988* (Cth) ('*Privacy Act*'), s 26GC(3).
[2] *Privacy Act*, s 26GC(4).
[3] *Privacy Act*, ss 26GC(3)-(4).

subsection. Accordingly, the use of 'entity' in the ED creates the impression that the application of the COPC is extended to small business operators.

It does not seem that it was Parliament's, or the Commissioner's, intention to extend the COPC to small business operators. Aside from the APP entities covered by virtue of paragraph 26GC(5)(a) of the Act, the COPC can only apply to 'an APP entity, or an APP entity in a class of entities, specified in the code for the purposes of this paragraph' under paragraph 26GC(5)(b).[4]

In our view, 'APP entity' is the more appropriate term for entities with obligations under the COPC, unless an additional defined term is created.

2. Services 'primarily concerned with the activities of children': ED, section 5

We understand that, in accordance with paragraph 26GC(5)(b) of the Act, section 5 of the ED is intended to extend the application of the COPC to additional APP entities beyond those covered by virtue of paragraph 26GC(5)(a) of the Act. The latter provides:

> "Subject to subsection (7), an APP entity is bound by the Children's Online Privacy Code if:
> (a) all of the following apply:
> i. the entity is a provider of a social media service, relevant electronic service or designated internet service (all within the meaning of the *Online Safety Act 2021*);
> ii. the service is likely to be accessed by children;
> iii. the entity is not providing a health service; or
> (b) the entity is an APP entity, or an APP entity in a class of entities, specified in the code for the purposes of this paragraph."

Section 5 of the ED specifies an additional class of entities that will be bound by the COPC, stating:

> "For the purposes of paragraph 26GC(5)(b) of the Act, entities to which all of the following apply are specified:
> (a) the entity is a provider of a social media service, a relevant electronic service or a designated internet service;
> (b) the service is primarily concerned with the activities of children;
> (c) the entity is not providing a health service."

It seems clear that the wording in paragraph (b) – 'the service is primarily concerned with the activities of children' – is intended to do the heavy lifting in terms of extending the application of the COPC beyond APP entities providing social media services, relevant electronic services and designated internet services that are likely to be accessed by children, bearing in mind that parents, guardians

[4] This position is reinforced by the fact that the obligation to comply with an APP Code applies to APP entities, according to section 26A of the Act.

and/or educators will sometimes be the end users of services that handle personal information about a child with no likely access by children.

However, this wording seems overly narrow. For example, the note to section 5 of the ED mentions that this is intended to capture providers of services such as 'family photo sharing applications'. A family photo sharing app would likely contain vast quantities of personal information about children, including biometric information about children,[5] but it does not seem apt to characterise it as a service that is 'primarily concerned with the activities of children' on the basis that adults use it to share photos of children. Similarly, one might ask whether co-parenting apps used by divorced parents are primarily concerned with the activities of children or primarily concerned with the parents' respective responsibilities and communications while collecting substantial amounts of information about a child? It seems that the object of this stipulation may be to capture services that are intended or expected to collect, use and/or disclose substantial amounts of information about a child.

3. Overbroad 'health service' provider carve-out: ED, section 5

The exclusion of entities 'providing a health service' from the scope of the COPC is a major weakness in the ED.

The exclusion of APP entities 'providing a health service' occurs both in subparagraph 26GC(5)(a)(iii) of the Act and in respect of the additional entities bound by the COPC according to section 5 of the ED.[6] In our view, the exclusion from the COPC of any APP entity that provides a health service is not required or inevitable. The Act[7] leaves it open for the Commissioner to specify further classes of APP entities to which the COPC applies and does not specify that this must exclude entities that provide a health service.[8]

According to the Explanatory Memorandum to the Privacy & Other Legislation Amendment Bill (2024), the exclusion of entities 'providing a health service' under paragraph 26GC(5)(a) was intended to align with the UK Information Commissioner's Age Appropriate Design Code, and ensures that the COPC is 'not a barrier to providing essential services to children', mentioning 'counselling, advice and telehealth' as apparent examples of these.[9] However, the Explanatory Memorandum also states that 'more general health, fitness or wellbeing apps or services may be covered by the COP Code'.[10]

---

[5] Although only 'biometric information that is to be used for the purpose of automated biometric verification or biometric identification' falls within the definition of 'sensitive information' under the *Privacy Act*, s 6(1).

[6] Pursuant to paragraph *Privacy Act*, 26GC(5)(b).

[7] Subparagraph 26GC(5)(b).

[8] The Explanatory Memorandum to the Privacy and Other Legislation Amendment Bill 2024 (Cth) ('Explanatory Memorandum') specifies that the intention of paragraph 26GC(5)(b) and subsection 26GC(7) is to provide flexibility, including that the COPC 'may specify that ... a provider of a health service is bound' by the Code.

[9] Explanatory Memorandum, para 85.

[10] Explanatory Memorandum, para 85.

In our view, the exclusion of providers of 'health services' under section 5 of the ED should be deleted for the following reasons.

(a) This exclusion establishes a broad carve-out at the entity level rather than the activity level, creating the potential for an APP entity to avoid COPC obligations by adding any health service to the services it provides. If, for example, the provider of a behavioural monitoring app for schools[11] also provides a mental health app marketed to adults with a screening tests for depression, it could thereby provide a 'health service' and, accordingly, the provider would not be an APP entity covered by the COPC and would not need to comply with the COPC obligations in respect of the behavioural monitoring app for schools.

(b) The 'health service' provider carve-out adopts an existing term that was defined broadly in the Act to *increase* the coverage of the Act and instead uses it to *reduce* the coverage of the COPC. Parliament defined the term 'health service' so that otherwise excluded small business operators would be brought back *into* the scope of the Act given their likely dealings with sensitive information as health service providers.[12] The ED and paragraph 26GC(5)(a) adopt this term as the basis on which APP entities should be left *out* of the scope of the COPC. In our view, this is not necessary to achieve the aim of protecting essential health services, which are a much narrower class than the defined 'health services'. 'Health services', as defined in section 6FB of the Act, would extend even to services provided via an app or website that 'record the individual's health for the purposes of assessing, maintaining, improving or managing their health'. Consider, for example, the period-tracking app that markets itself as 'the #1 OB-GYN recommended app', backed by 'a team of over 140 doctors and health experts' and including a 'Symptom Checker' which is 'designed to assist patients in recognizing common symptoms' associated with conditions like endometriosis and polycystic ovarian syndrome.[13] These commercial apps which likely come within the broad definition of 'health services' should be captured by the COPC.

(c) The privacy impact of the carve-out in both subparagraph 26GC(5)(a)(iii) of the Act and section 5 of the ED is magnified since it removes the protections of the COPC for APP entities handling sensitive information in the form of health information about a child, which potentially carries some of the most serious privacy risks for children. For example, this could include the wide range of health information and other sensitive information collected by period tracking apps, such as information about the child's menstrual cycles, daily moods, digestive system, illnesses, contraceptive use and sexual activities. These practices should be covered by the COPC in the interests of children's privacy, which is not adequately protected by the existing obligations on health service providers under the Act.[14]

[11] These apps can, eg, track student 'behavioural incidents', record school responses and analyse this data for trends and patterns.
[12] *Privacy Act*, s 6D(4)(b).
[13] See Flo, 'Elevating Female Health with Science and Technology' (Webpage, undated) https://med.flo.health/about-flo
[14] Katharine Kemp, 'Your Body, Our Data: Unfair and Unsafe Privacy Practices of Popular Fertility Apps' (Report, March 2023) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4396029

(d) In our view, the goal of protecting essential health services for children can be achieved by amending the wording of section 7 of the ED in respect of the online *activities* to which the COPC applies. In this respect, it is important to remember that the COPC will impose no obligations in respect of essential services provided in person by hospitals, GPs, paramedics, pharmacists, and mental health professionals since none of these are social media services, etc.

The stated intention of the exclusion of health services was to protect children's access to essential health services, and to align with the UK Age Appropriate Design Code. The UK Code only excludes 'preventive or counselling services' from the covered 'information society services'. The COPC should reduce the excluded health service activities to a similar category of essential health services under section 7 of the ED, and avoid any carve-out based on the much broader concept of entities providing 'health services'.

4. Reducing the privacy risks created by age checks: ED, section 8

The purpose of section 8 of the ED is to require covered APP entities to determine which end-users of the relevant services are children since many of the COPC obligations apply in respect of end-users who are children. However, section 8 of the ED incidentally reduces the privacy of some end-users by requiring APP entities to collect personal information that might not otherwise be collected.

In our view, the current wording of section 8 of the ED creates unnecessary and disproportionate privacy risks for child and adult end-users of the relevant services for the following reasons:

(a) Subsection 8(1) requires the APP entity to 'take steps that are reasonable in the circumstances to ascertain the age of the end-user'. Given that the object of this provision is to determine whether the end-user is a child, it is unnecessary for the entity to collect personal information to 'ascertain the age' of any end-user who is not a child. It is sufficient to ascertain that such an end-user is not a child: whether they are 18 or 80 is irrelevant. Despite the qualification that the entity need only 'take steps that are reasonable in the circumstances', the plain meaning of subsection is to create an obligation to 'ascertain the age' of every user. The provision should be amended to require covered APP entities to take reasonable steps to ascertain whether the end-user is a child, and if so, ascertain the age of the end-user.[15]

(b) Subsection 8(4) requires the APP entity to 'destroy sensitive information' that is collected to comply with subsection 8(1). Implicitly, the APP entity is not required to destroy other personal information that is collected to comply with this provision. It is not clear why the APP entity is

[15] On the basis that the latter information is necessary to comply with the different COPC obligations applying in respect of children of different ages.

not required to destroy personal information collected for the purpose of complying with section 8, insofar as it is not strictly necessary to provide the relevant service, as soon as it has complied with subsection 8(1).

(c) Section 8 should be amended to expressly prohibit the use or disclosure of personal information collected for the purpose of complying with subsection 8(1) for any other purpose, unless the same information is strictly necessary for the provision of the relevant service. For example, it should be unlawful for the entity to simultaneously use personal information collected to comply with subsection 8(1) to group end users into targeted marketing 'audiences' on the basis of their age range or apparent gender or ethnicity.

(d) It is arguable that the COPC cannot validly impose obligations in respect of the use, disclosure or destruction of personal information about an individual over the age of 18 collected by an APP entity to comply with subsection 8(1), since this would not be a rule in respect of the privacy of children. Given the risk that the COPC cannot mandate privacy-by-design obligations in respect of such information, it is vital to strictly minimise the personal information collected about individuals over the age of 18 in the age assurance process.

5. Clarifying permissible collection etc of personal information about a child: ED, s 9

While section 9 of the ED appears a relatively short and direct provision, its meaning is ambiguous and the Explanatory Statement contains a complex explanation concerning the intended effect of this provision, which is not always clear or consistent. The explanation introduces terms and concepts that are not included in the wording of section 9, such as 'the service to which the Code applies', 'the core service', and 'actively enabled'.

As drafted, section 9 of the ED is concerned with what collection, use or disclosure of personal information about a child is permissible by default. It provides that only collection, use or disclosure 'that is strictly necessary to provide the entity's service' is permissible by default.

Some matters remain unclear from the current drafting, including:

(a) What is 'the entity's service' for the purpose of subsection 9(1)? The concept is not defined in section 9 or in the ED more broadly. The Explanatory Statement describes this as 'the Service to which the Code applies' at one point, as the 'core service' at another, and 'the service the child has signed up for'. The more broadly this term is defined, the wider the permission for entities to collect, use and disclose personal information about children by default. For example, if an APP entity provides a social media app that includes both a free version that shows targeted ads and a paid version that does not show advertisements, is 'the entity's service' the paid version used by the child or the entire social media app including its analysis of users' online behaviour to inform its targeted advertising?

UNSW SYDNEY

(b) On what conditions can an APP entity collect personal information about a child if that information is not strictly necessary for provision of the entity's service? The meaning of the explanation provided by the Explanatory Statement in this respect is obscure. Subsection 9(1) of the ED provides that 'by default' the entity can only collect personal information about a child if it is 'strictly necessary to provide the entity's service' and that the entity must implement measures to ensure this. Section 9 does not include a substantive provision about the conditions on which the entity can collect information that is not strictly necessary for the relevant purpose. Subsection 9(2) only provides that the measures implemented to ensure the restricted default collection must 'enable an end-user of the entity's service who is a child to control whether [the information is collected] if that information is not strictly necessary for the provision of the entity's service' (emphasis added). This arguably introduces an implied substantive provision through an ostensibly procedural provision.

The Explanatory Statement indicates that 'other optional elements of the service that rely on personal information handling must be actively enabled' and the 'child must take an active step to opt in to collection' but states that the COPC does not include any obligation on the entity to obtain consent for collection of such personal information. It argues that section 9 'does not require additional consent when a child actively chooses to depart from those default settings'. This argument may be driven by the fact that the COPC can 'impose additional requirements to those imposed by one or more of the [APPs], so long as the additional requirements are not contrary to, or inconsistent with, those [APPs]'.[16] The distinction between consent and active choice requires significant clarification.

6. Clarifying 'best interests' obligations concerning collection of personal information: ED, s 10

We support the general requirement that an APP entity should only collect personal information about a child where that collection is consistent with the best interests of the child. In case there is any doubt, that protection should not be reduced to collection that is 'reasonably consistent' with the best interests of the child (wording that is used in the headings of the Explanatory Statement).

As to the wording of section 10 of the ED, for internal consistency and consistency with the wording of APPs 3.2 and 3.3, the 'must not' / 'unless' phrasing should be used in both subsection 10(1) and 10(2). It is not clear why subsection 10(2) currently uses the alternative 'may' / 'only if' phrasing.

The object of subsection 10(4) of the ED seems unclear. Subsection 10(3) provides that, in complying with APP 3.5, an entity does not collect personal information about a child through lawful and fair means if the entity collects the information in a way that is not consistent with the best interests of

[16] *Privacy Act*, s 26GC(4).

the child. According to subsection 10(4), subsection 10(3) 'does not limit the circumstances in which an entity collects, or does not collect, personal information through lawful and fair means'. However, subsection 10(3) does and should limit or restrictively clarify the circumstances in which an entity collects personal information about a child through lawful and fair means.

Subsection 10(5) of the ED provides that '[i]n complying with [APP] 3.6(b), an entity may collect personal information about a child only if the collection of the information is consistent with the best interests of the child'. APP 3.6(b) provides that an APP entity 'must collect personal information about an individual only from the individual unless … it is unreasonable or impracticable to do so'. APP 3.6(b) provides an important privacy protection against collection of personal information from third parties, including data brokers,[17] although it has been widely and inexplicably ignored. It is important that subsection 10(5) should not weaken it further. In particular, section 10 should not create permission for an APP entity to collect personal information about children from third-party organisations (including data brokers) based on the APP entity's potentially self-serving interpretation that this is consistent with the best interests of the child.

7. Use or disclosure of personal information about a child: ED, s 11

We support the general requirement that, in complying with APP 6.1, an APP entity should not use or disclose personal information about a child unless the child has consented to use or disclosure and it is consistent with the best interests of the child, save for the exceptions in subsection 11(2) of the ED.

Subsections 11(5) and (6) of the ED should both be qualified as for the purposes of paragraph 4(c), and/or combined, for clarity. Subsections 11(5) and (6) and section 29 serve the same purpose in respect of 'opt out' mechanisms for direct marketing uses and disclosures of personal information and sensitive information respectively, ideally both obligations should appear in section 11 or in section 29 for clarity.

8. Reducing the privacy risks created by consent and consent processes: ED, s 13

While we appreciate the logic of permitting a child of at least 15 years of age to consent to the use or disclosure of personal information about the child, it will be vital for the OAIC guidance on the COPC to clarify situations in which that consent would be invalid, particularly having regard to the information and power asymmetries.

The requirement in paragraph 13(2)(b) that the entity must 'take reasonable steps to confirm that the person who gives consent is a person with parental responsibility for the child' potentially provides a

[17] Katharine Kemp, 'Australia's Forgotten Privacy Principle: Why Common 'Enrichment' of Customer Data for Profiling and Targeting is Unlawful' (Research Paper, 2022) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4224653 .

basis for APP entities to claim that they are required to collect further personal information about a child and the child's parent or guardian for this purpose. Ideally, the APP entity would be obliged to destroy such personal information as soon as this purpose is fulfilled and prohibited from using or disclosing that information for any other purpose.

Since the COPC must create rules 'about the online privacy of children' and can impose additional requirements 'in relation to the privacy of children',[18] it is arguable that it cannot impose obligations about how APP entities must treat the additional personal information collected about adults as a result of the COPC. People over the age of 18 will likely be left with the existing inadequate protections of the Act in respect of personal information collected as a result of the COPC. Accordingly, any COPC provisions that would create an obligation or incentive for APP entities to collect personal information about individuals over the age of 18 should be strictly minimised.

9. Voluntary consent: ED, s 14

We support the provisions in respect of the voluntary nature of consent, including that consent should not be obtained through a bundled consent request.

We note that it will be particularly important for the OAIC to provide guidance to suppliers of education-related services and schools covered by the Act, to avoid circumstances where school students believe that they are 'required' to consent to additional collection, use or disclosure of personal information about them. For instance, a 15-year-old school student may well believe they are 'required' to consent when presented with a 'consent form' for human research by a member of the teaching staff, or for personality, aptitude and careers profiling by an external provider, given the school context in which they are consistently required to comply with the directions of adults.

10. Informed consent: ED, s 15

The reference to paragraph (3)(b) in subsection 15(4) should be a reference to paragraph (3)(c).

11. Currency of consent and destruction of personal information: ED, s 16

We generally support the provisions in respect of the current nature of consent.

Subsection 6(2) of the ED states that consent will be current in certain circumstances. For the avoidance of doubt, we recommend that subsection 6(2) specifies that consent will 'only' be current in these circumstances and that the entity 'obtained' rather than 'sought' the original consent.

[18] *Privacy Act*, ss 26GC(3)-(4).

UNSW SYDNEY

According to subsection 6(2), consent is current if it has not been withdrawn and it is less than 12 months since the consent was obtained or the entity obtained further consent before the expiration of that period of 12 months. Presumably, if consent is withdrawn or expires, APP 11 applies unless a request for destruction is made under section 32 of the ED.

12. Assent of a child under 15 years: ED, s 20

Section 20 of the ED concerns children under 15 years of age who are end-users of a relevant service. The significance of, and process for, obtaining such a child's assent under section 20 of the ED remains unclear.

According to the Explanatory Statement, the object of this provision is to 'involv[e] the child in [the] process' of obtaining the consent of a person with parental responsibility if the child is under 15, giving the child 'the opportunity to be more involved in the consent process'. This is because children in consultations on the COPC 'expressed a desire to be more involved and aware of how their personal information is being handled'.

Several aspects of section 20 of the ED appear ambiguous or disproportionately reduce privacy protections:

(a) The meaning of the child 'enabling' the entity to collect sensitive information etc is unclear. It seems from the Explanatory Statement that this refers to the child seeking to enable a privacy or information sharing setting presented via the relevant app or website in this respect. However, as statutory language, the word 'enables' may not be apt, given that the child has no authority to consent to the relevant activities.

(b) The required sequencing of child's assent and parental consent is not clear from the wording of the ED. The Explanatory Statement indicates that 'an entity will need to first obtain assent from the child for the handling of the information for that purpose and for contacting a person with parental responsibility to obtain consent'. However, neither section 20 nor section 13 specify that the entity must obtain the assent of the child before it seeks or obtains the consent of the person with parental responsibility.

(c) Subsection 20(2) requires the entity to seek the assent of the child 'for the entity to contact a person with parental responsibility for the child for the purposes of obtaining consent to that collection, use or disclosure' (presumably to 'seek' rather than 'obtain' that consent), but there is no substantive obligation on the entity to in fact contact the person with parental responsibility for this purpose.

(d) Most importantly, section 20 also potentially introduces privacy risks for families. While the meaning of the relevant obligations requires clarification, it seems the intention is that a child end-user under 15 years of age would, for instance, signal their intention to use a feature of the service that requires collection of sensitive information or use or disclosure of personal information for an unnecessary purpose, and the entity would then be required to provide that child with certain information and ask for their consent for the entity to contact their parent. Since this only applies where the child is the end-user, this would likely require the entity to collect personal information from a child about their parent, such as their name, mobile number and/or email address.

In our view, it is not appropriate for organisations interacting with young children to ask those young children for personal information about adults in their family, adults who may have made conscious choices not to disclose their personal information to the same organisations and whose privacy is not protected under the COPC, but left to the protections of the Act which are widely recognised as deficient.

If a child's assent is required, that should not be the child's assent for the entity to contact the child's parent if the parent is not an end-user of the service. Rather, the entity should give the child notice that it will be necessary for the child's parent to provide consent in addition to the child's relevant 'assent'. Any contact and further collection of personal information should be initiated by the person with parental responsibility.

13. Consent to cross-border disclosures: ED, s 26

We appreciate the intention to provide children with age-appropriate information regarding cross-border disclosure of personal information about the child for the purposes of obtaining the child's consent to cross-border disclosure under APP 8.

While this may reflect the limitations of statute itself, we note the likely farcical nature of a process in which an organisation opts not to take reasonable steps to ensure that an overseas recipient does not breach the APPs in relation to the personal information about a child, and instead justifies cross-border disclosure of that personal information on the basis of the 'informed' consent of a child under the age of 15.

14. Accessing personal information about a child: ED, s 27

Section 27 of the ED in part permits a person with parental responsibility seeking access to personal information about a child. This is arguably consistent with the power to 'impose additional requirements to those imposed by one or more of the Australian Privacy Principles, so long as the additional requirements are not contrary to, or inconsistent with, those principles.'

However, on the current wording of section 27 of the ED, a request for access to personal information about a child under APP 12.1 can be made 'on behalf of a child'. It is not clear who can make such a request and how this provision interacts with other laws that, for example, limit parent's access to the health records of their children after the age of 14.

15. Right to request information about handling of personal information: ED, s 28

We support the obligations under section 28 of the ED in respect of access to information about the entity's handling of personal information about a child, necessary for a child to have any hope of making an effective complaint about the handling of their personal information.

16. Requests to destroy personal information about a child: ED, s 32

We support the obligations in respect of requests for destruction of the personal information of a child under section 32 of the ED.

17. Notification of mechanisms that control or monitor or geolocation monitoring: ED, s 33

We support the obligation of APP entities to provide notification of geolocation monitoring by persons with parental responsibility and other end-users under section 33 of the ED.

We support the obligation of APP entities to provide notification of control or monitor services used by persons with parental responsibility under subsection 33(1). However, this notification should also be required in respect of other end-users of the service under subsection 33(2). Such control / monitor services are not exclusively supplied to persons with parental responsibility for the other user.[19]

We are available to clarify any points within this submission or to discuss further.

[redacted]

[19] eSafety Commissioner, 'Track, Harass, Repeat: Attitudes that Normalise Tech-Based Coercive Control' . <https://www.esafety.gov.au/sites/default/files/2025-04/Track-harass-repeat-attitudes-around-tech-based-coercive-control.pdf?v=1780552867715>