Australian Government

Office of the Australian Information Commissioner

EXPOSURE DRAFT EXPLANATORY STATEMENT

Privacy (Children's Online Privacy) Code 2026

Introduction

This draft Explanatory Statement accompanies the Exposure Draft of the Privacy (Children's Online Privacy) Code 2026 **(the Children's Online Privacy Code)**.

The Office of the Australian Information Commissioner (OAIC) invites interested parties to provide feedback on the Exposure Draft of the Children's Online Privacy Code (the Code) and this Explanatory Statement.

OAIC is seeking comments on the Exposure Draft, in particular on any unintended consequences of this legislative instrument or issues relating to the drafting.

Please note that the draft Explanatory Statement is still being developed and is intended only as a guide to assist with the interpretation of the draft Code. OAIC will undertake further editorial review post consultation once the final version of the Code is settled.

Background

In 2023, the Government released the Report of the Attorney-General's Department's *Privacy Act Review*, which amongst other things identified concerns regarding the adequacy of existing privacy protections for children in the online environment. The Review recognised that children are increasingly reliant on online platforms, social media, mobile applications and internet-connected devices, and that these online services routinely collect and use large volumes of personal information about children. The Review also noted growing community concern about the extent to which children are being 'datafied', including through collection of information relating to their activities, interests, location, wellbeing and relationships.

To address these concerns, the Review made a range of recommendations aimed at strengthening children's privacy protections online under the *Privacy Act 1988* (Cth) (the Act). This included the recommendation to mandate the development of a Children's Online Privacy Code, applying to online services likely to be accessed by children and aligned, to the extent possible, with comparable international frameworks such as the United Kingdom's Age appropriate design: a code of practice for online services (Age Appropriate Design Code).

In its response to the Review, the Government agreed that a Children's Online Privacy Code should be developed to provide clearer obligations for how online services are expected to protect the privacy of children.

The *Privacy and Other Legislation Amendment Act 2024* subsequently established a legislative requirement for the development of an APP Code, known as the Children's Online Privacy Code, about online privacy for children. That Act also conferred responsibility on the Information Commissioner (the Commissioner) to develop and register the Code.

APP codes operate in addition to the requirements of the Australian Privacy Principles (APPs). An APP code must set out how one or more of the APPs are to be applied or complied with. An APP

code may also deal with other relevant matters and may impose additional requirements to those imposed by the APPs, so long as the additional requirements are not contrary to, or inconsistent with, the APPs.

A breach of a registered APP code by the entity in relation to personal information about an individual will be an interference with the individual's privacy under section 13 of the Act and subject to investigation by the Commissioner under Part 5 of the Act.

Any APP code, other than a temporary APP code, that is registered will be a disallowable legislative instrument.

Purpose of the Code

The Children's Online Privacy Code requires APP entities bound by the Code to adopt best practice approaches to the handling of children's personal information. The effective implementation of the Code will enhance those entities' privacy protection capabilities, increase transparency in information handling practices, promote a culture that recognises and respects children's privacy and the value of their personal information, centre the best interests of the child as a primary principle to consider when handling personal information and provide children with greater control over their personal information.

The Code specifies the APP entities that are bound by the Code, sets out how those APP entities are to apply and comply with one or more of the APPs, sets out the period during which the Code is in force and imposes additional requirements to those imposed by one or more of the APPs that are not contrary to, or inconsistent with, those principles.

Consultation

In developing the Code, the OAIC has had more than 60 individual engagements with key stakeholders from across government, international regulators, industry, academia and the community. The Commissioner has consulted with children, relevant organisations or bodies concerned with children's welfare, industry organisations or bodies representing the interests of one or more entities that may potentially be bound by the Code, the eSafety Commissioner, and the National Children's Commissioner as well as a range of other stakeholders that the Commissioner considered appropriate in accordance with Subsection 26GC(8) of the Act.

Consistent with the objects of the Code to strengthen and protect children's privacy online, the OAIC placed particular importance on ensuring that the views and experiences of children informed the development of the Code. To support this, the OAIC developed worksheets to enable children and young people, and their parents and carers, to share their views on online privacy. Separate age-appropriate worksheets were developed for children in Years 3 to 6 and young people in Years 7 to 12, as well as a dedicated worksheet for parents and carers. A total of 337 children, young people, parents and carers were able to participate through online forms or by completing and submitting written worksheets.

Feedback received through this consultation highlighted that children, young people, parents and carers place a high value on online privacy, including a desire for greater transparency about how personal information is used, stronger protections against practices perceived as intrusive or unfair and clearer, more accessible and transparent information designed for children. Specifically, children and young people expressed a desire to have information communicated through age-appropriate means and for this information to be easily accessible. Children and young people expressed the view that they want to better understand how their personal information is handled and know how to seek help if there is a problem. Parents and carers expressed a similar view, namely, a desire for children to have greater control of their personal information including limiting direct marketing, nudge techniques and location tracking. These insights informed the OAIC's consideration of the content of the Code.

In parallel, the OAIC publicly released an issues paper that invited submissions from interested stakeholders. The OAIC received 61 written submissions from industry, civil society and academia stakeholders. These submissions contained diverse views pertaining to issues including age assurance, consent, transparency, the best interests of the child and children's right to permanently delete their personal information. During the same period, the OAIC also convened three industry roundtables with 32 attendees to support detailed discussion of key issues and practical considerations relevant to the operation of the Code. This included discussion about the alignment of the Code to other domestic and international codes and standards, clarity on the scope of services included in the Code and a balance between principles-based and prescriptive guidance.

The OAIC also heard from 70 academic and civil society representatives during a one-day workshop. These stakeholders discussed a range of issues including greater transparency of handling of children's personal information, limiting direct marketing to children, and increasing children's access to their personal information and ability to make corrections.

While views from industry, civil society organisations, academia and other interested stakeholders were diverse in nature, there was broad support for the Code and the goal of uplifting privacy protections for children and young people.

Explanation of sections

Details of the *Privacy (Children's Online Privacy) Code 2026*

Part 1—Preliminary

Section 1 Name

This section provides that the title of the instrument is the *Privacy (Children's Online Privacy) Code 2026.*

Section 2 Commencement

This section relates to the commencement of the Code. The commencement date of the Code will be determined and inserted in the final published version of the Code, the OAIC invites interested parties to provide feedback on what they consider to be an appropriate commencement date.

An APP code cannot come into force before it is included on the Codes Register (Paragraph 26C(2)(c) of the Act). Subsection 12(2) (retrospective application of legislative instruments) of the *Legislation Act 2003* does not apply to a registered APP code (Subsection 26B(3) of the Act).

Section 3 Authority

This section states that Subsection 26GC(1) of the *Privacy Act 1988* is the authority under which the instrument is made.

Section 4 Definitions

This section sets out the definitions relevant to the Code.

A number of expressions used in the Code are defined in Section 6 of the Act.

The term **the Act** means the *Privacy Act 1988*.

The term ***age appropriate*** relates to information that an entity gives under this Code, including information in a notice, explanation or any other form, and the manner in which that information is presented.

Information will be considered age appropriate:

- where the entity's service is targeted at a particular age range of children, the information is appropriate for a child of the youngest age in the range; or
- if the service is not targeted at a particular age range, the information is appropriate for a child aged between 10 and 12 years.

This approach is intended to enable entities to comply with the Code without needing to determine the age of its end-users.

When determining whether an entity's service is targeted at a particular age range of children, an entity is expected to consider factors such as whether any design features of the service are targeted at children of a certain age range. For example, an entity simply stating that the targeted age range of a service is 15-16 will not be sufficient, an entity will need to be able to prove that the service only targets children aged 15–16 years. The 10-12 age range has been included to provide a clear reference point for entities when designing information in circumstances where it genuinely isn't clear what age range their service may be targeted at. The age range reflects a developmental stage at which children generally have emerging capacity to understand structured explanations. This will also help reduce compliance uncertainty for entities.

Designated internet service has the same meaning as in the *Online Safety Act 2021*.

Person with parental responsibility, in relation a child, means a parent of the child, a guardian of the child or a person who is legally responsible for the child's day-to-day care, welfare and development.

Privacy impact assessment has the same meaning as in subsection 33(3) of the Act.

Relevant electronic service has the same meaning as in the *Online Safety Act 2021*.

Social media service has the same meaning as in the *Online Safety Act 2021*.

Part 2—Application of this Code

Section 5 Additional entities bound by this Code

The Code is binding on all entities covered by Paragraph 26GC(5)(a) of the Act. As per that Paragraph, the Code automatically applies to an APP entity if:

a. 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*),

b. the service is likely to be accessed by children, and

c. the entity is not providing a health service

For the purposes of paragraph 26GC(5)(b) of the Act, Section 5 sets out additional entities that are bound by the Code. The Code will apply to an APP entity if it meets all the conditions in Section 5, being:

a. 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*),

b. the service is primarily concerned with the activities of children, and

c. the entity is not providing a health service.

Binding these additional entities, and particularly the requirement under paragraph 5(b) of the Code, recognises that children's personal information may be handled by services that are not directly accessed by children but are nonetheless primarily concerned with children's activities and that such services may present comparable privacy risks. Examples of these kinds of services include applications that track early childhood development, family photo sharing applications, online school management systems that monitor student performance and internet-connected baby monitors.

Stakeholder consultation undertaken during the development of the Code indicated strong public interest in extending the application of the Code to the category of services set out in Section 5.

Section 6 Entities not bound by this Code

Section 6 is made under Subsection 26GC(7) of the Act and provides that an APP entity that is a carriage service provider within the meaning of the *Telecommunications Act 1997* is not bound by the Code. Carriage service providers are bodies such as internet service providers that supply telecommunications services to the public.

Section 7 Activities to which this Code applies

Section 7 is made under Paragraph 26C(4)(b) of the Act, which sets out that an APP code may apply to a specified activity, or a specified class of activities, of an entity. Section 7 provides that the Code applies to the activities of an entity to the extent that those activities consist of the provision of a social media service, relevant electronic service or designated internet service that is likely to be accessed by children or is primarily concerned with the activities of children. Effectively this means that the Code applies to specific services provided by an entity, rather than all the services of an entity as a whole.

For example, an entity may offer a singular service that is likely to be accessed by children (such as a pocket money app offered by a bank), while its other services are not (for example, that bank's

business banking and home loan apps). In that case, only the relevant service is captured, ensuring that other services which the entity provides that are not likely to be accessed by children or primarily concerned with the activities of children are not unintentionally brought within scope.

Part 3 The Australian Privacy Principles and the privacy of children

Division 1 General requirements

Section 8 Ascertaining the age of end-users of an entity's service

Section 8(1) provides that entities will need to take steps that are reasonable in the circumstances to establish the age of the end-user. Under Subsection 8(2), what steps are reasonable in the circumstances depend on the risk of harm that may arise from any collection, use or disclosure of the end-user's personal information. For example, an entity may take reasonable steps to ascertain an end-user's age by implementing age assurance. An entity does not need to undertake those steps if the entity applies the privacy protections afforded to children in the Code to all end-users. This establishes a standard that is intended to align with the UK Age Appropriate Design Code (Standard 3).

Age assurance is an umbrella term to describe a range of methods used to establish an individual's age or age range. Examples include age inference, age estimation, age verification, self-declaration, and parental attestation. The OAIC will maintain guidance on age assurance technologies to ensure entities comply with privacy obligations.

Subsection 8(1) will not apply retrospectively. Entities which have collected personal information before the commencement of the Code are expected to take steps that are reasonable in the circumstances to ascertain the age of the end-user before any further information is collected post-commencement.

The intention of Subsection 8(2) is to adopt a risk-based approach to age assurance. For example, it may be appropriate for lower risk services to accept a higher degree of uncertainty as to an end-user's age, whereas higher risk services would require a higher degree of certainty.

In having regard to the risk of harm from any collection, use or disclosure of a child's personal information, the intention is that entities consider factors such as the types of personal information collected, the volume of personal information and whether the personal information is being shared with third parties. Entities are expected to proactively assess the risk of harm from any collection, use or disclosure based on the personal information handling practices that occur in relation to the normal provision of their service or activities.

In determining what additional steps are reasonable to establish an individual's age, entities should also have regard to the suite of age assurance methods available, their relative efficacy, costs associated with their implementation, and data and privacy implications on end-users, amongst other things.

Subsection 8(3) provides that an entity may collect personal information about an individual before having ascertained the individual's age, only if that information is necessary for the entity to comply with Subsection 8(1). This recognises that personal information may need to be collected in order to comply with that Subsection.

Subsection 8(4) requires that an entity must as soon as practicable after complying with Subsection 8(1) destroy any sensitive information that was collected for the purposes of complying with Subsection 8(1), subject to specific exceptions. The exceptions relate to where the information is not contained in a Commonwealth record and the entity is not required by or under an Australian law, or a court/tribunal order, to retain the information. The intention of Section 8(4) is to reduce risks that may be associated with the collection of sensitive information that may arise from ascertaining the age of individuals. It is also intended to provide stronger privacy protection requirements than APP 11.2 by

requiring that an entity destroys information once the entity no longer needs the information for its original purpose, mitigating risks of re-identification.

Subsection 8(5) provides that Section 8 does not apply if the entity applies the protections afforded to children in the Code, other than Section 8, to the entity's service regardless of the age of the end-users.

Where an entity has already taken steps that are reasonable in the circumstances to ascertain the age of the end-user (for example, for the purposes of complying with Part 4A of the *Online Safety Act 2021* or otherwise), the entity may reuse that data-minimised age result for the purposes of complying with the requirements set out in this section, provided compliance with the Code was a stated purpose of collection and the entity has taken reasonable steps to ensure the information is accurate, up-to-date, complete and relevant.

Subsection 8(6) provides that nothing in this section affects the operation of another law of the Commonwealth, For example, if another law were to impose a lower threshold for steps required from an entity to establish the age of the end-user, or require that an entity need not take any steps at all, that law would override this section of the Code.

Section 9 Entities may collect etc. personal information about a child by default only if strictly necessary

Section 9 will introduce a requirement for entities to establish privacy protections by default in the design of their online services.

Subsection 9(1) requires entities to implement technical and organisational measures that, by default, ensure that the entity only collects, uses or discloses personal information about a child that is strictly necessary to provide the entity's service.

A 'default', as commonly defined in computer science, refers to the pre-existing or preselected value of a configurable setting that is assigned to a software application, computer program or device. Such settings are also called 'presets' or 'factory presets', especially for electronic devices. A 'default' also has the role of designating the settings that are automatically applied if the user does not choose or specify an alternative setting when presented with multiple options.

The term 'by default', when handling personal information, refers to making choices regarding configuration values or options that are set or prescribed in a system (such as a software application, service or device) or a manual procedure that affect the amount of personal information collected, the extent of the use or disclosure of the information, the storage period and accessibility. Those choices must ensure that, by default, only personal information about a child that is strictly necessary to provide the relevant service is collected, used or disclosed.

The term 'technical and organisational measures' has been used to provide a technology-neutral obligation intended to ensure this provision remains flexible and relevant in the case of technological change.

Examples of technical measures include physical, software and hardware measures, for example, implementing privacy settings set to 'high privacy by default' to allow children to opt in and out of optional handling of their personal information and configuring systems to collect only the minimal personal information required to provide the core service.

Examples of organisational measures include steps, processes and actions an entity should put in place, for example, training employees on integrating 'by default' obligations into the design of systems and developing standard operating procedures and policies to identify what personal information is strictly necessary to provide the core service.

The ‘strictly necessary’ requirement means that the collection, use or disclosure of that information should be essential to provide the service to which the Code applies, rather than reasonably necessary. In other words, an entity needs to collect, use and disclose personal information in that way in order to actually deliver the elements of the service the child has signed up for. For example, this does not include the collection, use or disclosure of personal information for broader business purposes (e.g. for marketing, service improvement or as part of an indirect funding model).

The ‘strictly necessary’ test establishes a narrower and more protective threshold than ‘reasonably necessary’.

Subsection 9(2) provides that such technical and organisation measures, as required in Subsection 9(1), must enable an end-user of the entity’s service, who is a child, to control whether the personal information is collected, used or disclosed, if that information is not strictly necessary to provide the entity’s core service, and that such measures must be easily accessible and clear. When assessing whether measures are accessible and clear, entities are expected to consider whether such measures are appropriate for children, including whether they can be easily understood, located and used.

This obligation means that children should be able to control when and how their personal information is collected, used or disclosed, for example, by choosing whether their personal information is collected, used or disclosed for a particular purpose. In other words, rather than managing and implementing lengthy and complex privacy settings, children should be able to turn additional elements of the entity’s service ‘on’ or ‘off’ that rely on the collection, use or disclosure of their personal information which is not strictly necessary to provide the service (i.e. additional features which aren’t necessary to provide the core service). For example, a child should be able to turn on or off additional elements such as personalised content, targeted advertising or recommendations that rely on the handling of a child’s personal information. When an additional element is turned off, the service must not collect, use or disclose the child’s information for that purpose.

This section is closely tied with APP 11 requirements. If a child turns ‘off’ an additional element of the entities service, such as personalised content, and a range of personal information has been collected solely for that purpose, the entity will no longer need the information for that purpose for which the information may have been used or disclosed by the entity. The entity will need to comply with the requirements under APP 11 and take such steps as are reasonable in the circumstances to destroy the information or to ensure that the information is de-identified, so long as an APP 11 exception does not apply.

This section also does not narrow or restrict the operation of APP 3.1 or 3.2. An entity may still collect children’s personal information where it is reasonably necessary for one of their functions or activities (and, for agencies, where it is reasonably necessary, or directly related to, one of their functions or activities). Rather, the requirement is directed to the default design of services. It requires that additional collection, use or disclosure that is not strictly necessary for the provision of the service is not enabled by default and is subject to appropriate transparency and choice. This reflects a privacy-by-default approach, under which only the personal information necessary to provide the core service is handled automatically, while other optional elements of the service that rely on personal information handling must be actively enabled.

For example, where a child signs up for an online messaging service, it may be strictly necessary for the entity to collect limited personal information in order to create an account and enable messages to be sent and received. However, the collection or use of the child’s personal information to provide personalised recommendations, targeted advertising or make service improvements would not generally be strictly necessary to deliver the core messaging service. These additional elements of the service may still be offered if they are reasonably necessary for the entities functions or activities, but they should not involve the collection, use or disclosure of the child’s personal information by default and should instead be subject to clear and meaningful choice (for example through privacy settings which are set to ‘off’ by default).

The obligations in this section also do not introduce new consent requirements for the purposes of APP 3.1 and 3.2. The provision concerns how an entity should configure the default settings of their service – it does not require additional consent when a child actively chooses to depart from those default settings.

For example, where the collection of personal information is reasonably necessary for the entity's functions or activities, but not strictly necessary for the provision of the entity's service, a child actively enabling a setting to allow for the collection of personal information that is reasonably necessary for the entity's functions or activities would permit the collection of the child's personal information for that purpose. In this example, proposed Section 9 does not, in departing from the default settings of the service, require the child's consent. To provide another example, a child enabling a privacy setting that allows for the collection, use or disclosure of certain sensitive information may still require consent due to the operation of APP 3.3(a), as opposed to Section 9.

This section will apply to both existing and new user accounts, upon the commencement of the Code. That is, upon the commencement of the Code, every service account of a child that is captured by the Code must be set to 'high privacy by default' such that the entity only collects, uses or discloses personal information about those children that is strictly necessary to provide the entity's service.

Section 9 establishes an obligation that is intended to align with the UK Information Commissioner's Age Appropriate Design Code (Standard 7). The 'high privacy by default' obligation is an important safeguard as many children will just accept the default settings they are provided upon their first use of a service and never change them. Section 9 ensures that a child must take an active step to opt in to collection, use or disclosure of their personal information. The intention of this obligation is to provide children with greater control over their personal information, increase transparency and minimise the amount of personal information in circulation online. Minimising the collection and retention of personal information also reduces the risk and impact of data breaches, improves the quality and accuracy of personal information and lowers the cost of storing and managing personal information.

Section 10 Collection of personal information about a child must be reasonably consistent with best interests of the child

Section 10 introduces additional requirements for entities to collect children's personal information in ways that are consistent with the best interests of the child.

The term 'best interests of the child' refers to the fundamental principle in international law concerning children that all decisions made, and actions taken, should be in their 'best interests' as per Article 3 of the United Nations Convention on the Rights of the Child (UNCRC).

When assessing whether any collection, use or disclosure of personal information is consistent with the best interests of the child, an entity should consider factors such as:

(a) the nature and extent of child exploitation risks (child exploitation is any situation where a child is abused, harmed or used by another person for economic, sexual or personal gain)

(b) the likely mental or physical impacts on the child

(c) the likely impact on the physical, psychological, emotional, social and cognitive development of the child

(d) the extent to which the child's ability to develop and express their views and identities may be affected

(e) the extent to which the child's freedom of association, play, leisure or participation in social, cultural or educational activities may be affected

(f) whether particular groups of children may experience disproportionate or adverse impacts (including children with disabilities, Aboriginal and Torres Strait Islander children, children from culturally and linguistically diverse backgrounds)

(g) the evolving capacities of children, including differences in age, maturity and developmental stage across childhood

Collecting, using or disclosing personal information in ways that are consistent with the best interests of the child does not mean that an entity cannot pursue its own commercial or other interests. An entity's commercial interests may not be incompatible with the best interests of the child.

In certain instances, an entity will need to act consistently with the best interests of a particular individual child. For example, if a child reports issues with how their personal information is being used, this may inform whether the collection, use or disclosure of the child's personal information is in the child's best interests. In other circumstances, it is the best interests of an identified group of children or children in general, that is relevant. This is the case when decisions are made about issues that do not relate to one specific child, but for instance, to the group of children users of a specific service. Vulnerabilities of certain groups of children may need to be considered (such as children with disabilities, Aboriginal and Torres Strait Islander children, children from culturally and linguistically diverse backgrounds) depending on the nature of the service being provided.

Subsection 10(1) provides that, in complying with APP 3.2, an organisation must not collect personal information (other than sensitive information) about a child unless it is consistent with the best interests of the child to comply with APP 3.2. This obligation applies in addition to APP 3.2. This means that an organisation must not collect personal information (other than sensitive information) about a child unless the information is reasonably necessary for one or more of the organisation's functions or activities and it is consistent with the best interests of the child.

Subsection 10(2) provides that in complying with APP 3.3(a) an entity may collect sensitive information about a child only if the collection is consistent with the best interests of the child. This obligation applies in addition to APP 3.3(a).

Subsection 10(3) sets out how APP 3.5 applies in relation to collecting personal information by lawful and fair means. This obligation provides that the means of collection must be consistent with the best interests of the child for it to be considered lawful and fair means of collection. This obligation does not limit APP 3.5 and the circumstances in which an entity collects, or does not collect, personal information through lawful and fair means.

Subsection 10(5) provides that an entity may collect personal information about a child under APP 3.6(b) only if the collection is consistent with the best interests of the child. Under APP 3.6(b), an entity must collect personal information about an individual only from the individual unless it is unreasonable or impracticable to do so. This means that indirect collection can only happen if it is 'unreasonable or impractical' and it consistent with the best interests of the child.

Subsection 10(6) sets out the circumstances in which this section does not apply. These exceptions are necessary to achieve consistency between the Code and the Act and recognises that collection may still be necessary in limited circumstances, for example if the information is required or authorised by or under an Australian law or a court/tribunal order.

Section 11 Use or disclosure of personal information about a child must be reasonably consistent with best interests of the child

Subsection 11(1) provides that in complying with APP 6.1 an entity must not use or disclose personal information about a child unless consent has been obtained and the use or disclosure is consistent with the best interests of the child. The introduction of this requirement will mean that entities will not be able to rely on APP 6.1(b) as a basis for the use and disclosure of a child's personal information.

Subsection 11(2) provides that Subsection (1) does not apply to the use or disclosure of personal information to which APP 6.2(b), (c), (d), (e), 6.3 or 6.7 applies. These exceptions are necessary to achieve consistency between the Code and the Act, and recognise that use and disclosure may still be necessary in limited circumstances, for example to promote justice, or in response to a serious threat to individual or public health or safety.

Subsection 11(3) sets out that in complying with APP 7, an organisation may use or disclose personal information (other than sensitive information) about a child for the purpose of direct marketing only if APP 7.2 applies, consent is obtained and if it is consistent with the best interests of the child. The effect of Subsection 11(3) is that it removes the ability for an organisation to rely on APP 7.3 as a basis for the use or disclosure of a child's personal information (other than sensitive information) for direct marketing. Effectively this means that entities that are organisations will only be able to use or disclose personal information (other than sensitive information) about a child for the purpose of direct marketing if the information is collected directly from the child, consent is obtained, the child would reasonably expect to use or disclose the information for the purpose of direct marketing, a simple means to opt out of direct marketing communications is provided and the direct marketing is in the child's best interests. This obligation precludes an entity from using personal information collected from a third party to undertake direct marketing.

Subsection 11(4) sets out additional requirements to APP 7.4, providing that an organisation may use or disclose sensitive information for the purposes of direct marketing if the information was collected from the child, the organisation provides a simple means for the child to opt out and the use or disclosure if consistent with the best interests of the child. This obligation applies in addition to the requirements in APP 7.4, which provides that consent must be obtained to use or disclose sensitive information for the purposes of direct marketing.

Subparagraphs 11(5) and (6) provide that the simple means to opt out for children must not, in alignment with Section 29, incorporate processes or features that make it difficult to make the request. Information about the means must be located in a prominent position, in a font size and type that is easy to read and written in plain language, is clear and age appropriate. This requirement is intended to preclude entities from using design practices that make it hard for a child to opt out of direct marketing.

The purpose of this section is to establish a framework within the Code to help entities understand the needs of children and the rights that they must take into account when collecting, using and disclosing children's personal information. These obligations are important because children merit specific protection with regard to their personal information as they may be less aware of the risks, consequences and their rights in relation to the collection, use and disclosure of their personal information.

Division 2 Consent

Section 12 Purpose of this division

Section 12 provides that Division 2 sets out the application of the Code in relation to consent.

Division 2 provides how APPs 3, 6, 7 and 8, as well as various provisions of the Code, are to be complied with in relation to consent to the collection, use and disclosure of personal information about a child.

Amongst other requirements, this division sets out an age of consent and provides that consent must be voluntary, informed, current, specific and unambiguous (aligning with existing consent requirements under the Social Media Minimum Age scheme in Part 4A of the *Online Safety Act 2021*).

The requirements for consent apply to both consent provided by a child, and consent provided by a person with parental responsibility for a child.

Section 13 Consent given by child or person with parental responsibility

Section 13 provides that consent can only be given by a child if they are at least 15 years of age. The age of 15 has been included to align with the OAIC's current guidance on children's presumed age of consent for the handling of their personal information.[1] The existing OAIC guidance about presumed age of consent was recommended by the ALRC in Report 108 (2008), For Your Information: Australian Privacy Law and Practice. The age of 15 was selected following consideration of the research on child brain development and adolescent decision-making, as well as the types of decisions made under the Act and likely consequences of those decisions.

If a child is under 15 years of age the Code will require that consent be obtained by a person with parental responsibility for the child.

Subsection 13(2) sets out that the entity will need to take reasonable steps to confirm that consent is given by a person with parental responsibility for the child. This is an essential obligation to ensure that consent is obtained from a parent, guardian or another person with legal responsibility for the child's day-to-day care, welfare and development.

When assessing what steps are reasonable for verifying parental consent, an entity is expected to choose a verification method reasonably designed in light of available technology to ensure that the person giving the consent is a person with parental responsibility for the child.

For example, this could be achieved through:

- email communication where a person with parental responsibility has set up an account or profile for the child,
- vouching via a token provided by a bank, school or telecommunications provider,
- connecting the person with parental responsibility with a customer service agent via a video conference, or
- providing a form of government digital ID.

Subsection 13(3) requires an entity to provide an age appropriate notice to a child when a person with parental responsibility provides their consent to the collection, use or disclosure of a child's personal information. The notice must clearly state details regarding the purpose, period, and consequences of consent as well as withdrawal rights, use descriptors and any recipients associated with personal information that may be collected, used or disclosed. This requirement responds to feedback received from children during OAIC consultations that children want greater transparency over how their personal information is being handled and they want to be more involved in the consent process to improve their digital literacy and privacy education.

Subsection 13(4) provides exceptions to obtaining consent from a person with parental responsibility for the handling of a child's personal information, under 15 years of age. A child under 15 years of age may give consent to the collection, use or disclosure of their personal information if the child is seeking legal or health-related information or support in connection with a person with parental responsibility for the child. The purpose of this exception is to account for circumstances where it may be problematic to involve a person with parental responsibility, for example, if a child is seeking legal advice in connection with an issue that the person with parental responsibility caused. A child under 15 years of age may also give consent to the collection, use or disclosure of their personal information where a different age is otherwise specified by law in relation to that collection, use or disclosure

[1] The Australian Privacy Principles (APP) guidelines 2025, Chapter B: Key concepts

Section 14 Consent must be voluntary

Section 14 provides that consent to the collection, use or disclosure of personal information about a child must be voluntary. The section sets out the factors that an entity must consider when determining whether consent is voluntary and the circumstances in which consent is not voluntary.

Subsection 14(2) provides that, when determining whether consent is voluntary, an entity must consider the alternatives open to the individual if the individual does not consent to the collection, use or disclosure of their personal information. For example, an entity must consider whether an individual can still access a basic version of the entity's service if they don't consent to their personal information being used for a particular purpose, such as targeted advertising. An entity will also need to consider the seriousness of any consequences for the individual, their family members or associates if they do not consent.

Paragraph 14(3)(a) provides that consent is not voluntary if it is obtained by manipulative, deceptive or misleading practices. This requirement will preclude entities from seeking consent through design practices such as nudge techniques that are designed to compel an individual to consent to more handling of personal information than they would otherwise agree to.

An example of nudge techniques is persistently prompting a child to consent to the use of their personal information for a particular activity, such as subscribing to a direct marketing newsletter. Pop-ups that reappear after being closed or prompts that interfere with the user's intended task can frustrate users and impede their experience, incentivising them to eventually just agree to such handling.

Paragraph 14(3)(b) provides that consent is not voluntary if it is obtained using a bundled consent request. Subsection 14(4) provides that a bundled consent request means a request to the individual that seeks their consent to multiple collections, uses or disclosures of their personal information and does not allow the individual to consent, or not consent, to each individual collection, use or disclosure.

Each collection, use or disclosure of personal information necessarily occurs for one or more distinct purposes. In the context of bundled consent requests, voluntary consent is closely tied to specific consent as an entity will need to obtain consent in relation to each distinct purpose for which the personal information is handled, but this will generally not be considered voluntary if an entity seeks consent through a bundled consent request. This ensures that entities generally do not combine multiple purposes into a single consent request, which would limit an individual's ability to make a genuine and informed choice.

Paragraph 14(3)(c) provides that unless the personal information is strictly necessary to provide the service, consent is not voluntary if the individual is unable to access the entity's service if they refuse to consent to the collection, use or disclosure of that information. This means that consent is not voluntary if the individual is not given a genuine choice to refuse personal information handling that is not strictly necessary for the service. This obligation is tied closely with Paragraph 14(2)(a) and what alternatives are open to the individual if they do not consent to such handling.

Section 15 Consent must be informed

Section 15 provides that consent to the collection, use or disclosure of personal information about a child must be informed and the conditions for meeting informed consent.

Subsection 15(2) sets out that consent is informed if the entity gives an individual written notice containing the information required under Subsection 15(3).

Subsection 15(4) is consistent with the APP Guidelines published by the OAIC. Relevantly, these guidelines provide that consent given at a particular time in particular circumstances cannot be assumed to endure indefinitely. Consistent with these guidelines, this obligation provides for express consent to expire within a specified period of time, which must be reasonably appropriate to the

nature of the information being handled but must not be more than 12 months after the consent was initially given. This obligation is closely tied to Section 16 (consent must be current), if the specified period of time mentioned in the notice required under Subparagraph 15(3)(c) has expired, consent will not be considered 'current'.

Subsection 15(5) sets out that if the notice, required under Subsection 15(2), is provided to a child, the notice must be provided in terms and in a format that is simple, easy to understand and age appropriate. Providing information to children in an age appropriate manner prior to obtaining their consent is essential in order to enable them to make informed decisions, understand what they are agreeing to and, for example, exercise their right to withdraw their consent.

Section 16 Consent must be current

Subsection 16(1) provides that consent to the collection, use or disclosure of personal information about a child must be current.

Subsection 16(2) provides that consent is current if it is sought at the time the information was collected, used or disclosed, the consent has not been withdrawn and the period mentioned in the notice required under Subparagraph 15(3)(c) has not expired or if the entity obtained further consent to the collection, use or disclosure before that period expired.

Section 17 Consent can be withdrawn

Section 17 provides that consent to the collection, use or disclosure of personal information about a child can be withdrawn at any time and that an entity must provide a clear, simple and easily accessible means for individuals to withdraw consent. When assessing whether the means for an individual to withdraw consent are clear, simple and accessible, entities are expected to consider whether such means can be easily understood, located and used by both a child and a person with parental responsibility.

Section 18 Consent must be specific

Section 18 provides that consent to the collection, use or disclosure of personal information about a child must be specific. The intention of including a requirement for specific consent is to ensure a safeguard against the gradual widening or blurring of purposes for which personal information is handled, after an individual has agreed to the initial collection of their personal information. The requirement that consent must be 'specific' aims to provide children with greater control over their personal information by increasing transparency around each specific purpose for which the information is collected, used or disclosed.

Subsection 18(2) sets out that consent is specific if it is for a distinct purpose and is not broader than is necessary for that distinct purpose. If an entity is handling personal information based on consent and wishes to handle the information for another purpose, the entity will need to seek additional consent for this other purpose. For example, seeking consent for the collection of personal information for all purposes as determined by the entity, or within the entity's interests, would not be a distinct purpose.

Subsection 18(2) sets out than an entity must express the purpose for which the information is collected, used or disclosed with a level of specificity that is reasonably appropriate to the circumstances, including whether the information is sensitive information. Sensitive information has the same meaning as per the Act.

Specific consent is closely tied to informed consent, in that specific consent can only be obtained when an individual is specifically informed about the intended purposes of the collection, use or disclosure of the personal information.

Section 19 Consent must be unambiguous

Section 19 provides that consent must be unambiguous and that consent is not unambiguous if it arises from an omission by the individual. This requirement precludes entities from seeking consent through, for example, silence, preselected settings or opt-outs.

The purpose of including an unambiguous consent requirement is to require a clear affirmative indication by an individual that indicates that the individual has agreed to the collection, use or disclosure of personal information for a particular purpose. Because unambiguous consent cannot be given by omission, it must be given through a positive act or statement that clearly indicates agreement.

Unambiguous consent will ordinarily be express. However, consent may in limited circumstances be implied from a clear affirmative action, but only to the extent that the purpose of the consent is obvious from the context. For example, where an individual takes a deliberate action that clearly indicates agreement to the handling of their personal information for a specific purpose, consent may be inferred for that purpose only. An individual who voluntarily provides their contact details for the purpose of participating in a prize draw may be taken to have consented to the use of that information for administering the prize draw but not for unrelated purposes such as marketing.

Section 20 Assent of child under 15 years must be obtained in certain circumstances

Section 20 requires that, when a child under the age of 15 enables an entity to collect, use or disclose certain personal information, the entity must seek the child's assent to that collection, use or disclosure, as well as for the entity to contact a person with parental responsibility for the child for the purposes of obtaining their consent to that collection, use or disclosure.

The assent requirement maintains consent from a person with parental responsibility as the legal authorisation for the collection of sensitive information, the secondary use and disclosure of children's personal information and the use or disclosure of personal information for the purpose of direct marketing, whilst still involving the child in this process. This increases transparency, digital literacy and a level of autonomy for the child over the handling of their personal information.

The assent requirement only applies where a child below the age of 15 enables an entity to collect sensitive information, use or disclose their personal information for a secondary purpose, or use or disclose personal information for the purpose of direct marketing.

The child's assent is not required in circumstances where a person with parental responsibility has already provided their consent to the handling of the child's personal information for a specific purpose.

For example, circumstances where assent would not be required could include where a person with parental responsibility has:

(a) set up an account on behalf of their child and provided their consent to the collection of the child's sensitive information for a specific purpose, or
(b) consented to the use of their child's personal information for a secondary purpose through parental controls applied on the child's account.

The child's assent must be specific, meaning that it is for a distinct purpose and is not unnecessarily broad.

Entities seeking a child's assent must provide a child with an age appropriate notice regarding, among other things, the purpose, period, and consequences of assent as well as consent withdrawal rights, use descriptors, and information about recipients associated with assent being granted for the collection, use or disclosure of the child's personal information. Under Section 9 of the Code, an entity will need to provide technical measures such as privacy settings that are set to high privacy by default for any personal information handling that is not strictly necessary to provide the service, including the handling of personal information that requires consent. Where a child under the age of 15 enables a

setting involving the collection, use or disclosure of personal information requiring consent, 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.

For example, consider an entity that provides a privacy setting for personalised content, and wants to collect sensitive information for this purpose. When a child (as opposed to a person with parental responsibility) enables this setting, a child-friendly notice must be provided to the child which sets out the information under Paragraph 20(5)(b). The child must then first assent to:

(a) the collection of that information for that specific purpose, and
(b) the child's parent (a person with parental responsibility) being contacted to provide their parental consent to the collection of that information for that purpose.

If the child does not agree to (a) and/or (b) then the entity must not proceed with the collection of that information for that purpose. If the child agrees to both (a) and (b), the entity can then proceed to obtain consent from a person with parental responsibility on behalf of the child.

Assent can only be relied upon to the extent that it is appropriate for the information being handled and is valid for a maximum of 12 months.

Children, in consultations on the Code, expressed a desire to be more involved and aware of how their personal information is being handled, this section directly responds to this feedback. Providing children with the opportunity to be more involved in the consent process supports the development of privacy literacy from a younger age and creates opportunities for children and their parents to determine appropriate privacy safeguards together. It also allows children to stop, think and determine whether they actually do want to turn on a feature in exchange for the handling of their personal information and whether they want to proceed to obtain parental consent.

Section 21 Consent must not be obtained by coercion etc.

Subsection 21(1) 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 seeks consent to the collection of the information in a way that coerces or manipulates the individual from whom the information will be collected to consent, or substantially impedes the ability of the individual to decide whether to consent to the collection. This obligation does not limit APP 3.5 and the circumstances in which an entity collects, or does not collect, sensitive information through lawful and fair means.

Subsection 21(3) sets out that an entity must not seek consent to the use and disclosure in a way that coerces or manipulates the individual to consent or substantially impedes the ability of the individual to decide whether to consent to the use or disclosure of the information.

This section is closely tied to voluntary consent, these obligations will preclude entities from seeking consent through design practices such as nudge techniques that are designed to compel an individual to consent to more handling of personal information than they would otherwise agree to.

For example, 'confirmshaming', is a design practice that uses guilt-inducing language to manipulate users into opting into something, such as the handling of their personal information for a specific purpose. 'Confirmingshaming' might look like decline options attached to consent notices which are phrased negatively, such as "No thanks, I prefer to play a boring version of the game.", making users feel bad for saying no to the handling of their personal information for that purpose.

Division 3 Transparency

Section 22 Purpose of this Division

Section 22 provides that Division 3 sets out how entities are to comply with APPs 1, 2, 5, 7, 8 and 12 to ensure transparency when those entities are dealing with children and their personal information.

Section 23 APP privacy policy–requirements

Section 23 sets out how APP 1.3 and 1.4 are to be complied with. Subsection 23(2) provides that an entity, whose service is likely to be accessed by children, must have a version of their privacy policy that is directed specifically at children. The application of this section is not intended to extend to an entity whose service is primarily concerned with the activities of children but is not likely to be accessed by children. The qualifier has been included as the Code also applies to services that are primarily concerned with the activities of children but are not likely to be accessed by children themselves. In these circumstances, it will not be appropriate for measures such as developing child-specific privacy policies to be applied to such services.

An entity may meet this obligation by providing a separate version of their main privacy policy where necessary. An entity may also meet this obligation by only providing a singular privacy policy that is written in clear, simple and accessible language so it can be understood by both children and adults.

Section 23 operates in addition to APP 1.3 and APP 1.4, specifying additional matters relevant to the presentation of APP privacy policies for children as well as additional matters they must contain. It is intended that the privacy policy will include the information required by APP 1.4 and Subsection 23(5), while presenting that information in the manner prescribed by Subsections 23(3), (4) and (5).

Subsection 23(3) prescribes how the information in the entity's child-friendly privacy policy must be presented.

For the purposes of Subparagraph 23(3)(c), an APP privacy policy must, where appropriate, incorporate non-text material to engage children effectively. This may include visual or audio content, such as icons, images, diagrams, animations or short videos, where this would assist children to understand the entity's child-friendly privacy policy.

Subsection 23(4) provides that an APP privacy policy must be located in a prominent position, be presented in a font size and type that is easy to read. Subsection (5) provides that an APP privacy policy must not include complex or technical language or legal jargon.

Subsection 23(6) also sets out matters that must be included in the entity's child-friendly APP privacy policy, which are in addition to the matters set out in APP 1.4. These are intended to support an individual's right, under APP 2, to have the option of not identifying themselves, or of using a pseudonym, when dealing with an entity.

Section 24 Notification of the collection of personal information

Section 24 sets out how APP 5 is to be complied with in relation to notifying children about the collection of personal information.

Subsection 24(1) provides that the section applies to an entity only if the entity's service is likely to be accessed by children. As such, the application of this section is not intended to extend to an entity whose service is primarily concerned with the activities of children but is not likely to be accessed by children. As per Section 24 this qualifier has been included as the Code also applies to services that are primarily concerned with the activities of children but are not likely to be accessed by children themselves. In these circumstances, it will not be appropriate for measures such as developing age appropriate notifications to be applied to such services.

Subsection 24(2) provides the manner in which the information, required by APP 5, must be presented. Notifications must be clear, concise, transparent, easily accessible, and age appropriate to ensure that children can meaningfully understand the notification of the collection of personal information, which increases transparency. Information must not be expressed in a way that obscures or misrepresents the nature or consequences of the handling, as a measure intended to both prohibit entities from deceptively framing their handling practices, and give children the ability to assess the lawfulness of such handling.

For example, if an entity tells a child that they have collected their personal information to show them videos that they might like, without explaining that this involves the entity tracking their activity across

the service to build a behavioural profile, this may misrepresent the consequences of the handling by failing to explain how the child's personal information will actually be used.

Section 25 Review of privacy practices etc.

Section 25 requires an entity, in complying with APP 1.2, to review and update its privacy practices, procedures and systems at least annually. An entity will also be required to keep records of the reviews and updates undertaken and provide a copy of those records to the Commissioner if requested to do so. Commissioner refers to the Information Commissioner and has the same meaning as in the *Australian Information Commissioner Act 2010*.

For example, policies and practices under APP 1.2 could include:

- training and educating staff on the entity's obligations in relation to the handling of personal information about children and the entity's practices, procedures and systems relating to handling personal information about children (as per Section 40 of the Code), or
- establishing procedures to deal with complaints and inquiries in relation to the handling of personal information about children within 30 days (as per Section 36 of the Code)

Section 26 Consent to cross-border disclosures

APP 8.1 requires an entity to take reasonable steps to ensure privacy protections are maintained when disclosing personal information to an overseas recipient. APP 8.2(b) exempts an entity from the requirements of APP 8.1 if the entity expressly informs the individual that if they consent to the disclosure of the information, Subclause 8.1 will not apply to the disclosure and, after being informed, the individual consents. Section 26 sets out requirements that must be met when expressly informing a child of such matters.

Subsection 26(2) requires that the presentation of such information must meet a range of criteria so that children can understand it meaningfully. Subsection 26(3)(3) provides that this information must be located in a prominent position on the service, be presented in a font size and type that is easy to read. Subsection 26(5) requires that the information must not include complex or technical language or legal jargon.

The purpose of this section is to ensure an entity adequately meets its obligations under APP 8.2 in relation to expressly informing children.

Section 27 Accessing personal information

Section 27 creates an additional requirement for entities in relation to compliance with APP 12. Section 27 provides that if an entity gives a child access to personal information in response to an access request, the entity must give access in a manner which is simple, easy to read and age appropriate. The manner in which the information is provided should enable the child to meaningfully understand what personal information is held about them.

For example, an entity could provide the child with access to the personal information requested in a child-friendly format that can be viewed directly within the service, without requiring the child to download a file or use another application to view the information. This could be displayed on a clear summary page within the service, using simple language and headings so the information is easy to read and understand.

This is intended to support an individual's right to request the correction (APP 13) or destruction (Section 32) of their personal information. It is important that a child is able to meaningfully understand what information is held about them so that they are able to exercise their right to request the correction or destruction of their personal information.

Section 28 Right to request access to information about handling of personal information

Subsection 28(1) sets out that if a child, or a person with parental responsibility on behalf of a child, requests access to personal information under APP 12.1, the child or person may also request access to information about the entity's handling of the child's personal information, to the extent the entity holds that information.

Subsection 28(2) provides the type of information that may be requested may include. However, this does not limit the types of requests in relation to the entity's handling of a child's personal information that an individual can make.

For example, an individual may request information about the existence of any automated decision-making, including profiling, relating to the child's personal information. An entity is expected to provide the individual with information on the existence of any automated decision-making relating to the child's personal information and whether profiling has been used as a decision-making basis. If so, the entity will need to provide the individual with simple, easy to understand and age appropriate information about the context of such decisions, including the logic involved and the consequences of making them.

In relation to providing the individual with information about the logic involved, an entity is not expected to provide all details about the technologies used for automated decision-making or profiling. It is expected that the information about the logic must be meaningful to an individual, without requiring them to have any technical knowledge.

Subsection 28(3) and (4) deal with timeframes for responding to destruction requests. A response to such a request must be provided within a reasonable period after the request is made. Where a reasonable period is less than 30 days, the entity must respond within that shorter period; otherwise, the response must be within 30 days. This obligation recognises that the processing of more complicated requests should not usually exceed 30 days. However, the compliance burden entailed by Section 28 will be eased by Paragraph 28(3)(b) and Subsection 28(4), which, read together, provide that the entity can respond to the request within 60 days of the original request if the entity reasonably considers it is necessary to do so having regard to the complexity and number of requests that the entity is dealing with.

Subsection 28(5)(a) sets out that an entity's response must be direct and informative to the request. An entity is expected to comply with this requirement by expressing the response to the request in a way that does not obscure or misrepresent the nature of how a child's personal information is being handled. This is to ensure that meaningful responses to requests are provided to children.

Paragraph 28(5)(b) provides that if the child's personal information has been disclosed to an overseas recipient, the entity's response must include an explanation of the steps taken to comply with APP 8.1. This obligation is intended to apply to requests that are made in relation to any cross-border disclosure of personal information, including, but not limited to, when a child requests information about the recipients, or categories of recipients, of the personal information under Paragraph 28(2)(d).

Subsection 28(6) aligns with Section 27, requiring that an entity's response to a request made by a child must be provided in terms and a format that is simple, easy to read and age appropriate. This is to ensure that a child can meaningfully understand the response to their request.

Subsection 28(7) provides that APP 12.2 to 12.10 apply in relation to a request for information under this section in the same way they apply to a request for access under APP 12.1.

The purpose of introducing a right to request access to information about the handling of personal information is to enhance transparency and empower children to make informed choices about their personal information by creating an enforceable right to obtain clear explanations of what personal information is held about them and how it is being processed. It is also intended to support their ability to verify the lawfulness of such handling.

Section 29 Opting out of direct marketing

Section 29 sets out how APP 7.2(c) must be complied with for the purposes of this Code. It provides that an entity must provide a simple and easy means by which the child may request not to receive direct marketing communications. The means must not incorporate processes or features that make it difficult to make the request. Information about the means must be located in a prominent position and displayed in a font size and type that is easy to read, as well as age appropriate.

This requirement will preclude entities from using design practices that make it hard for a child to opt out of direct marketing, for example, requiring a child to navigate through multiple screens, with misleading buttons that try to trick them into cancelling their request to opt out of the direct marketing.

Division 4 Access to, and correction of, personal information about children

Section 30 Dealing with requests for access to personal information about children

Section 30 requires an entity, that is an organisation, to respond within a certain timeframe to requests for access to a child's personal information made under APP 12. This response must be provided within a reasonable period after the request is made, otherwise, within 30 days after the request is made. Where a reasonable period is less than 30 days, the entity must respond within that shorter period.

Section 30 recognises, in limited circumstances, additional time may be required to process requests. While the processing of more complicated requests should not usually exceed 30 days, an entity may reasonably consider that more than 30 days is needed where the request is significantly complex and the entity is dealing with a large number of requests. In such circumstances, an entity must respond within a maximum period of 60 days after the request was made, provided it notifies the individual within 30 days of receiving the request that it will rely on the extended timeframe, including an explanation of why the response cannot be provided within 30 days. The 30 day extension for dealing with access requests will ease the compliance burden on organisations.

Section 31 Dealing with requests to correct personal information about children

Section 31 requires an entity, that is an organisation, to respond within a certain timeframe for requests to correct a child's personal information made under APP 13.1 or 13.4. This response must be provided within a reasonable period after the request is made, otherwise, within 30 days after the request is made. Where a reasonable period is less than 30 days, the entity must respond within that shorter period.

Section 31 recognises, in limited circumstances, additional time may be required to process requests. While the processing of more complicated requests should not usually exceed 30 days, an entity may reasonably consider that more than 30 days is needed where the request is significantly complex and the entity is dealing with a large number of requests. In such circumstances, an entity must respond within a maximum period of 60 days after the request was made provided it notifies the individual within 30 days of receiving the request that it will rely on the extended timeframe, including an explanation of why the response cannot be provided within 30 days. The 30 day extension for dealing with correction requests will ease the compliance burden on organisations.

Division 5 Destruction of personal information about children

Section 32 Request to destroy personal information about a child

Section 32 provides that entities must destroy specified personal information about a child upon request by the child or a person with parental responsibility for the child, subject to specific exceptions.

The exceptions relate to where:

- the entity reasonably believes that destroying the information would pose a serious threat to the life, health or safety of any individual, or to public health or public safety,
- the information relates to existing or anticipated legal proceedings relating to the entity and the child,
- destruction would be unlawful,
- retaining the information is required by or under an Australian law, or a court/tribunal order,
- the information is contained in a Commonwealth record,
- a permitted general situation (other than the situation referred to in item 1 of the table in subsection 16A(1)) exists in relation to the use or disclosure of the information by the entity,
- the entity is an organisation, and a permitted health situation exists in relation to the use or disclosure of the information by the entity, or
- the entity reasonably believes that the use or disclosure of the information is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body.

The reference in Subsection 32(3) to information 'contained in a Commonwealth record' ensures that the requirements on agencies to retain such information under the Archives Act will override the Section 32 destruction requirements. Commonwealth record has the same meaning as in the *Archives Act 1983*.

This obligation is intended to provide stronger privacy protection requirements than APP 11.2 by generally requiring that an entity destroy personal information upon request. De-identification of personal information will not be sufficient to comply with this obligation. The intention of this is to mitigate the risks of data re-identification. With an increasing volume of publicly available, de-identified data, the risks of re-identification are enhanced, as disparate datasets can be cross-referenced to uncover personal identities. Several issues with de-identification practices have also been observed, including de-identification processes being done incorrectly and entities inadequately assessing the risks of re-identification.

Subsection 32(4) requires an entity to provide the child or person with parental responsibility a written notice that the personal information has been destroyed. This is to increase transparency over the destruction process after such a request has been made.

If an entity refuses to destroy the personal information due to one of the exceptions, Subsection 32(4) will also require the entity to give written notice for the refusal. The notice must include the reasons for why the information was not destroyed, except to the extent that it would be unreasonable to do so, having regard to the grounds for the refusal. This is intended to operate the same way as APP 12.9(a). If the request is made by a child, the written notice must be age appropriate.

Subsections 32(7) and (8) deal with timeframes for responding to destruction requests. A response to such a request must be provided within a reasonable period after the request is made. Where a reasonable period is less than 30 days, the entity must respond within that shorter period, otherwise, the response must be within 30 days. This provision recognises that more complicated requests should not usually exceed 30 days. However, the compliance burden entailed by Subsection 32(7) will be eased by Subparagraph 32(7)(b)(ii) and Subsection 32(8), which, read together, provide that the entity can respond to the request within 60 days of the original request if the entity reasonably considers it is necessary to do so having regard to the complexity and number of requests that the entity is dealing with.

As children are a more vulnerable group and at a higher risk of possible adverse consequences if the quality of their personal information is not ensured, they should be afforded a greater level of protection and control over their personal information that is held by entities.

Consultations on the Code found that both children and parents support introducing a right to request the destruction of children's personal information. In a poll of 1,624 13–17-year-old Australians regarding the Code, organised by Reset.Tech Australia and conducted by YouGov in July 2025, 92% indicated that they support the Code creating a right to erasure.[2]

The objective of this obligation is to increase transparency and give children stronger control over their personal information by creating an enforceable right to request its destruction. This obligation ensures children's personal information is generally not retained indefinitely, reducing privacy risks associated with unnecessary storage and upholds the right of the child under Article 16 of the UNCRC to protection from arbitrary or unlawful interference with their privacy.

Division 6 Notification requirements for control or monitoring mechanisms

Section 33 Notification of mechanisms that monitor or control service use or monitor geolocation

Subsection 33(1) applies where an entity provides a mechanism that enables a person with parental responsibility for a child to control or monitor the child's use of the service or monitor the geolocation data of the child. Subsection 33(1) requires the entity to notify the child that such a mechanism is in place. This is intended to ensure that children know when their use of a service is being restricted or monitored, including where their online activity or location may be observed, to increase transparency and promote the privacy of children.

For example, this section may apply to control or monitoring mechanisms such as parental controls applied on making in-app purchases (such as preventing them altogether) or communication permissions applied to the collection of voice data in a gaming app.

Subsection 33(2) applies where an entity provides a mechanism that enables an end-user of the service to monitor the geolocation data of another end-user of the service who is a child. An entity must notify a child when their geolocation data is being shared with another end-user. This notification must occur throughout the period during which the monitoring is occurring. For example, if an entity provides a service that has an interactive feature that allows end-users to share their real-time location with friends, if a child end-user of the service enables this feature, the entity will need to notify the child that their geolocation is being shared with other end-users while the sharing is occurring. That notification could take the form of an illuminated icon, for example.

Subsection 33(3) provides that the notification must be age appropriate; it must also be given as soon as practicable after the mechanism starts to be used and in a way that reasonably ensures the child is aware of the use of the mechanism.

Subsection 33(4) provides that the entity must also ensure the notification is easily accessible to the child.

These requirements ensure that the design of the notification is flexible enough to be tailored to the needs of individual services but provides important parameters for designing the notifications so that children can meaningfully understand them to improve transparency and promote the privacy of children.

Parental controls are important because they can be used to support parents in protecting and promoting the best interests of their child, a role recognised by the UNCRC. Location sharing also has a range of benefits, including enhanced personal safety, convenience and social connection.

Section 33 recognises that parental controls also impact on the child's right to privacy as recognised by Article 16 of the UNCRC and the child's rights to association, play, access to information and

[2] Results from a survey with young people about the Children's Online Privacy Code, Reset.Tech Australia, March 2025

freedom of expression. Children who are subject to persistent parental monitoring or location tracking may have a diminished sense of their own private space which may affect the development of their sense of their own identity. This is particularly the case as the child matures and their expectation of privacy increases.

Division 7 Making inquiries and complaints

Section 34 Application of this Code in relation to inquiries and complaints

Section 34 provides that Division 8 sets out how entities are to comply with APP 1 in relation to enabling inquiries and complaints about an entity's handling of personal information about a child.

Section 35 Information about children's privacy rights

Section 35 requires that an entity must provide children with clear, concise, transparent and age appropriate information about the kinds of information the entity may collect, use and disclose, what kinds of inquiries and complaints can be made about the collection, use and disclosure of their personal information, and the potential outcomes of an inquiry or complaint. This section does not prescribe where or how this information must be set out to allow for flexibility for an entity to embed this information into its service in a way that is suitable for both a child and the service.

For example, an entity may incorporate age appropriate information into their existing privacy policy or create specific webpages with frequently asked questions (FAQs) that detail the kinds of personal information handled by the entity.

Section 36 Child-friendly inquiry and complaints processes

Subsections 36(1) and (2) provide that an entity must take reasonable steps to embed a process into its service that enables an end-user and, when that end-user is a child, a person with parental responsibility for the child, to make certain inquiries, requests and complaints.

This includes making a general inquiry about the handling of children's personal information and obtaining from the entity a clear explanation of how children's personal information is being handled. If the person is a child or has parental responsibility for a child under 15 years of age, the entity is also required to embed a process that supports access, correction or destruction requests as per APP 12 and 13 and Section 32 of the Code. An entity is also required to embed a process that enables an end-user to make a complaint about an entity's handling of children's personal information.

Subsection 36(3) requires that such processes must be clear, simple and easily accessible, expressed in clear and concise language and, if the end-user of the service is a child, expressed in age appropriate language and presented simply and in a way children can understand. This prohibits entities from embedding design elements into their service that purposefully make it difficult for end-users to locate and understand how to make an inquiry or complaint in relation to the entity's handling of children's personal information.

For example, an entity may develop a dedicated online webform for children to lodge privacy complaints which includes information explaining how a child's complaint will be handled in accordance with the Code.

Subsection 36(4) requires that the process must allow for complaints and inquiries that are general in nature to be made anonymously or by pseudonym and ensure that the option to do so can be easily located. This provision supports the application of APP 2, which provides for an individual's right to anonymity and pseudonymity. The entity must also make it clear how information regarding the inquiry or complaint will be dealt with and the available review processes, including making a complaint to the Commissioner.

Subsection 36(5) provides exceptions to Paragraph 36(4)(a). This recognises that in some circumstances it will be impracticable for an entity to deal with individuals who have not identified themselves. It further recognises that in some circumstances an entity will be required or authorised by or under an Australian law, or a court/tribunal order, to deal with individuals who have identified themselves.

Subsection 36(7) requires that an entity must take reasonable steps to deal with an inquiry or complaint within 30 days after it is made.

Division 8 Privacy impact assessments and privacy education and training

Section 37 Application of this Code in relation to privacy impact assessments and privacy education and training

In recognition of the risks associated with different online services, Section 37 provides that Division 8 sets out how entities are to comply with APP 1 in relation to assisting persons employed or otherwise engaged by such entities to understand their obligations in relation to the handling of children's personal information.

Section 38 Privacy impact assessments

Section 38 provides that an entity must conduct a privacy impact assessment (PIA) when proposing to provide any new service or activity that is likely to be accessed by children or will be primarily concerned with the activities of children.

An entity must also conduct a PIA if the entity plans to make any new or changed way of handling personal information, in relation to an existing service or activity, that is likely to have a significant impact on the privacy of children. Section 38 does not define what constitutes as a 'significant impact' in relation to the privacy of children. The ordinary meaning of these words will apply.

Subsection 38(2) provides that the PIA must include:

- a description of the nature, scope, context, flow and purposes of the handling of children's personal information,
- an explanation as to why the collection of children's personal information is strictly necessary to provide the service or activity,
- an explanation as to how the collection of children's personal information is done by lawful and fair means,
- an assessment of whether the handling of children's personal information is consistent with the best interests of the child and record this assessment, including the reasoning on which the assessment is based,
- specific information about how the entity complies with this Code and the Act, and
- an assessment of the risk of harm to, and the potential impact on, children resulting from the handling of their personal information.
    - Harms and impacts may include those of a physical, emotional, developmental or material nature.

This effectively establishes that the PIA must cover three core components – an information flows mapping exercise, a compliance check against the requirements set out in the Code and Privacy Act and a risk assessment. An information flows mapping exercise involves describing how the project deals with personal information. For example, an entity might use diagrams to depict the flow of information, or tables setting out the key information for different types of personal information to be used in the project.

Subsection 38(3) requires that the PIA be conducted before the new service is made available to end-users, or the new or changed way is implemented. When developing a new service or activity, an

entity is expected to begin a PIA early in the design of the service or activity, before the entity handles any personal information.

Section 38 establishes an obligation that is intended to align with the UK Information Commissioner's Age Appropriate Design Code (Standard 2) .

Section 39 Register of privacy impact assessments

Section 39 requires that an entity maintain a register of the PIAs it conducts and publish the register online. An entity must also provide a copy of the register and any PIAs that are listed on the register to the Commissioner, if requested to do so. This provision is designed to enhance transparency, accountability and improve record keeping in relation to an entity's obligations under Section 38.

Section 40 Privacy education and training

Section 40 requires entities to ensure that all individuals they employ or otherwise engage, who have regular or frequent access to children's personal information in the course of performing their duties, must participate in education and training about the protection of children's personal information.

Subsection 40(2) provides that the education and training must address the entity's obligations in relation to handling personal information about children, set out in the Code and the Act, and explain the entity's practices, procedures and systems relating to handling personal information about children. This relates to the practices, procedures and systems referred to in APP 1 and Section 25 of the Code. The education and training must be provided to each person employed or otherwise engaged by the entity as soon as practicable after the person is employed or engaged by the entity and at least annually after.

Subsection 40(3) provides that an entity must also keep records of the education and training provided and, if requested to do so by the Commissioner, provide a copy of those records. This provision is designed to enhance accountability and improve record keeping in relation to the entity's obligations under this section.