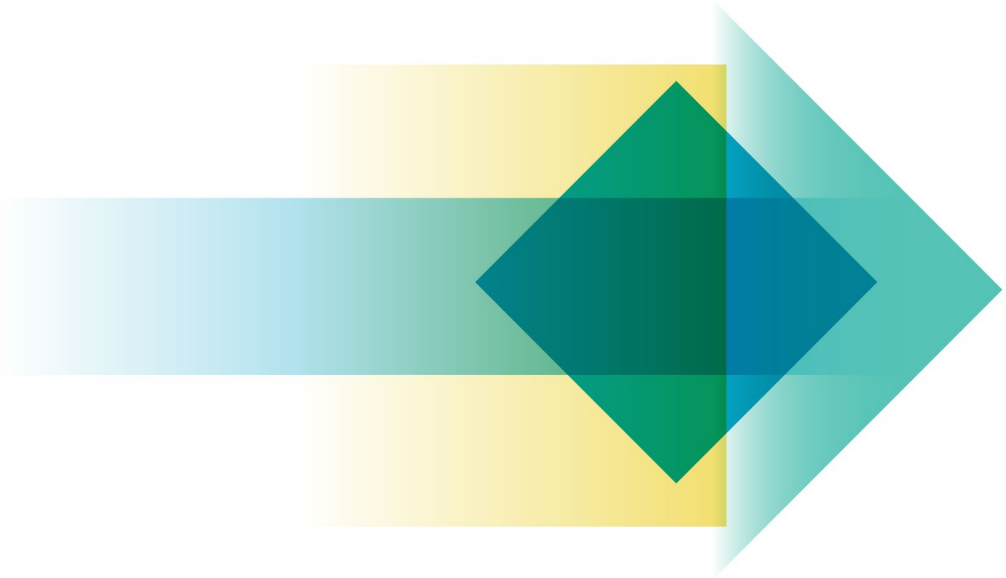
Australian Government

Office of the Australian Information Commissioner

OAIC Children's Online Privacy Code

Issues paper



12 June 2025

OAIC

Contents

Executive summary

This Issues Paper seeks feedback from relevant stakeholders into the Office of the Australian Information Commissioner's (OAIC) development of the Children's Online Privacy Code (the Code). The Code, mandated by the *Privacy and Other Legislation Amendment Act 2024* (the Act), will enhance privacy protections for children who engage in the digital world, where large amounts of personal information is collected from an early age. The aim of the Code is not to prevent children from engaging online, but to ensure their personal information is protected within that space.

The Code will apply to online services likely to be accessed by children, which includes social media services (SMS), relevant electronic services (RES) and designated internet services (DIS).[1] These categories cover a wide range of online services, such as social media, messaging apps, websites and cloud storage services. The Code will set out how one or more of the Australian Privacy Principles (APPs) will be applied or is to be complied with in relation to children's personal information. The Code may also include additional requirements if they are not contrary or inconsistent with the APPs.

This Issues Paper invites stakeholders to provide feedback on several matters that are being considered for the Code, including the scope of services covered, when and how the Code should apply to entities and whether protections should vary depending on the age and developmental stage of children. This consultation also seeks to address matters directly related to the relevant APPs including, how online services can ensure that privacy policies and collection notices are clearly communicated, that informed consent is meaningfully obtained and that children have greater control over their personal information, including the ability to access and correct it.

Initial consultations with children and young people, conducted by Reset.Tech Australia, highlighted significant concerns about privacy online. Many children expressed a desire for clearer, more accessible privacy policies, as well as greater control over their personal information, particularly in relation to areas such as targeted advertising and geolocation data. These consultations also revealed that current consent mechanisms are often perceived as insufficient, with many children feeling that they are not empowered to make informed decisions about their personal information. These findings underline the importance of the Code in ensuring that children can effectively protect their privacy while using online services.

While the primary objective of the Code is to improve privacy protections for children, it may also play an important role in uplifting privacy practices across entities more broadly, which may deliver wider benefits for all Australians.

The feedback on this consultation will help inform the OAIC how the Code can better protect the privacy of children within Australia’s digital environment and legal system. A draft version of the Code

[1] Social media service, relevant electronic service and designated internet service are all within the meaning of the *Online Safety Act 2021*

will be released for public consultation in early 2026, where further feedback will be considered before the Code is registered on 10 December 2026.

Acknowledgement of Country

The Office of the Australian Information Commissioner acknowledges Traditional Custodians of Country across Australia and recognises their continuing connection to lands, waters and communities. We pay our respect to Aboriginal and Torres Strait Islander cultures, and to Elders past and present.

About the OAIC

The Office of the Australian Information Commissioner (OAIC) is an independent statutory agency in the Attorney-General's portfolio, established under the Australian Information Commissioner Act 2010 (AIC Act).

Our purpose is to promote and uphold privacy and information access rights. We do this by:

- ensuring proper handling of personal information under the Privacy Act 1988 and other legislation
- protecting the public's right of access to documents under the Freedom of Information Act 1982 (FOI Act)
- carrying out strategic information management functions within the Australian Government under the AIC Act.

Our regulatory activities include:

- conducting investigations
- handling complaints
- reviewing decisions made under the FOI Act
- monitoring agency administration
- providing advice to the public, organisations and Australian Government agencies.

Our vision is to increase public trust and confidence in the protection of personal information and access to government-held information.

Consultation process

Request for feedback and comments

This paper seeks information and views to inform the OAIC's development of the Children's Online Privacy Code.

Questions are included throughout the paper to guide comments. You are invited to answer some or all questions, or to comment on issues more broadly.

Please ensure your submission includes the corresponding question numbers and submit via email to copc@oaic.gov.au.

Please note, this consultation is not a statutory requirement. The OAIC has chosen to seek views to help inform the development of the Code by identifying key issues, perspectives or gaps, but inclusion of specific feedback remains at the OAIC's discretion.

The OAIC is required to conduct a public consultation on the draft Code. This will occur in 2026. It will be open for a minimum of 60 days, and the OAIC will give consideration to any submissions made within the consultation period.

Publication of submissions and confidentiality

Submissions may be made available to the public on the OAIC's website. Please refrain from including any personal information in your submission. Any personal information that is included in the submissions will be redacted for publication purposes.

Closing date for submissions: 31 July 2025.

What is the Children's Online Privacy Code and why do we need it?

While digital technologies offer significant benefits, they also increase privacy risks, particularly for children who are more vulnerable to online harms. As the Attorney-General noted in the second reading speech for the *Privacy and Other Legislation Amendment Bill 2024* (Cth), many children have grown up entirely in the digital word, where large amounts of their personal information is collected from an early age. It is estimated that by the time a child turns 13, it is estimated that up to 72 million data points may have been gathered about them.[2]

Children are particularly vulnerable to the misuse of their data and may not fully understand the privacy implications of their online activity. This high volume of data collection has created serious risks that can turn into real and serious harms, an example is a major data breach occurring and revealing the sensitive information of millions of Australians, exposing them to risks such as identity fraud and scams.

Existing privacy laws have not kept pace with these changes in digital engagement or the scale of data collection. In response, the Act introduced a mandate for the OAIC to develop a Children's Online Privacy Code (the Code), which will put children at the centre of privacy protections in Australia.

As code developer, our ultimate objective is not to prevent children from engaging in the digital world, but rather to protect them within it through strengthened privacy protections for the handling of their personal information. The Code also presents a significant opportunity to elevate the privacy practices of entities, that will benefit Australians more broadly, particularly for individuals within the wider community who are at higher risk of harm due to vulnerability factors, such as possessing low levels of literacy or education, or living with impaired cognitive functions.

The Code will apply to social media services and a wide range of other internet services likely to be accessed by children, including apps, websites and messaging platforms. It will specify how these services must comply with the Australian Privacy Principles (APPs). The code may impose additional requirements provided they are not inconsistent with the existing privacy principles.

For example, under the APPs, APP entities (any organisation or agency that is subject to the *Privacy Act 1988*) have obligations to have a privacy policy that is accessible to individuals and to provide individuals with collection notices, where appropriate. The Code might set out how organisations should tailor their privacy policies and collection notices for a child specific audience, so that they are clear, easy to understand and more digestible for children. For example, by using graphics, video and audio content, rather than relying solely on words.

---

[2] Mark Dreyfus, "Second Reading Speech" (House of Representatives, 12 September 2024) Parlinfo - BILLS : Privacy and Other Legislation Amendment Bill 2024 : Second Reading

What we've learnt from children and young people so far

Initial consultations and engagement with children, coordinated by Reset.Tech Australia, have provided valuable insights that have helped shape the framing of issues in this paper.

Concerns about privacy and a call for stronger protections

Findings from these activities highlight that generally children have concerns about how their personal information and data is being collected, used and disclosed, and want greater protections in place. Children want to be involved in, and empowered by, discussions about the protection of their personal information.

"As a young person I am aware that you have the rare opportunity to reshape digital culture for young Australians. Not by shielding us, but by trusting us. Not by speaking for us, but by including us. If you build with that in mind, this Code will be transformative for all Australians."[3]

Transparency and age-appropriate communication

Participants in the consultations, held by Reset.Tech Australia, consistently called for greater transparency about how their personal information is collected, used, and with whom it's shared.[4] Many highlighted that terms of use outlined in privacy policies, and information about how to manage privacy settings, are often inaccessible due to various barriers, including complicated jargon and lengthiness.[5] Additionally, some felt that reading the policy would not help them to understand or gain control over their privacy, regardless.[6]

The desire for greater transparency was particularly apparent in relation to targeted advertising, with some children reporting unease with its accuracy.[7] While many did not want to be targeted with

[3] Reset.Tech Australia, Consultation with young people about the Children's Online Privacy Code and consent and agency, page 7.

[4] Reset.Tech Australia, Results from a survey with young people about the Children's Online Privacy Code, page 1.

[5] Reset.Tech Australia, Consultation with young people about the Children's Online Privacy Code; especially Transparency, Geolocation, Advertising & EdTech, page 3.

[6] Ibid.

[7] Reset.Tech Australia, Consultation with young people about the Children's Online Privacy Code; especially Transparency, Geolocation, Advertising & EdTech, page 10.

direct advertising at all,[8] others wanted greater insight and discretion over the methods of data collection used, highlighting a need for informed consent.[9]

Informed consent and digital literacy

Children expressed that meaningful consent is often lacking in their online experience. To be able to provide informed consent, children reported the need for greater education to improve digital literacy in relation to data and privacy risks, and their available privacy rights.[10]

Some children did not feel that the consent that they currently provide to online platforms is meaningful or transparent, with one young person suggesting that *"the process feels performative, like coercion."*[11]

Many acknowledged that consent may need to be provided or supported by a parent for children under a certain age, although responses as to which age this should be varied.[12] Some children also raised that consent provided by a child's school on behalf of them should be critically analysed and should not override the child's consent.[13]

Control over personal data and privacy

A recurring theme throughout the consultations was the desire for children to have more control over their privacy and personal information, with one participant reporting, *"I feel as though my privacy should be determined by what I want and how I want that to be displayed."*[14]

Many children want the ability to delete their data, and the need to gain explicit consent before data is collected, shared or used.[15] Notably, children want to be able to change their mind and have any

---

[8] Reset.Tech Australia, Results from a survey with young people about the Children's Online Privacy Code, page 4; *"I would like to be protected online by not being targeted with advertising. I'm still a young child."*

[9] Reset.Tech Australia, Consultation with young people about the Children's Online Privacy Code; especially Transparency, Geolocation, Advertising & EdTech, page 11.

[10] Reset.Tech Australia, Consultation with young people about the Children's Online Privacy Code; especially Transparency, Geolocation, Advertising & EdTech, page 16.

[11] Reset.Tech Australia, Consultation with young people about the Children's Online Privacy Code and consent and agency, page 4.

[12] Reset.Tech Australia, Results from a survey with young people about the Children's Online Privacy Code, page 3.

[13] Reset.Tech Australia, Consultation with young people about the Children's Online Privacy Code and consent and agency, page 5.

[14] Reset.Tech Australia, Results from a survey with young people about the Children's Online Privacy Code, page 12

[15] Reset.Tech Australia, Results from a survey with young people about the Children's Online Privacy Code, page 7; *"I would like companies like Roblox, YouTube and Microsoft to have an option for Australian users to easily delete accounts and other stored data."*

stored data deleted if consent was previously given.[16] Additionally, a reasonable number of children want their data to be deleted by online platforms after a certain period of inactivity, as well as the option to delete some or all of their data when they turn 18 years old.[17]

Data minimisation, privacy settings and geolocation data

A call for data minimisation was apparent, with one respondent reporting, *"I would like them* [online platforms] *to collect less data in the first place."*[18] Over eight-in-ten (88%) Australian children want default privacy settings on online platforms to be automatically set to high, and default geolocation settings to be automatically turned off.[19] While children highlighted fewer concerns about the use of geolocation data where the purpose of that usage was apparent (i.e. SnapMaps, Google Maps or Life360), they tended to raise concerns about misuse and necessity for collection where such information was requested without an evident purpose. Due to concerns around safety, data security was raised as particularly important in relation to geolocation data.[20]

Data security and protection from harm

Children are also acutely aware of the need to protect data from bad actors such as hackers and scam actors and raised the need to ensure greater data security through two-factor authentication and encryption.[21]

The findings from these consultations highlight a general awareness of the risks around data security, but low levels of empowerment among children in Australia when it comes to privacy protection.[22] These insights have helped shape the framing of issues raised in this paper, ensuring that the development of the Code is grounded in the real experience and expectations of children and young people.

---

[16] Reset.Tech Australia, Consultation with young people about the Children's Online Privacy Code; especially Transparency, Geolocation, Advertising & EdTech, page 8; *"We should be able to delete our online footprint at any time"*

[17] Reset.Tech Australia, Results from a survey with young people about the Children's Online Privacy Code, page 5.

[18] Reset.Tech Australia, Results from a survey with young people about the Children's Online Privacy Code, page 14

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

[20] Reset.Tech Australia, Consultation with young people about the Children's Online Privacy Code; especially Transparency, Geolocation, Advertising & EdTech, pages 6-7; *"I don't appreciate how companies track my viewing or activity its quite creepy."*

[21] Reset.Tech Australia, Results from a survey with young people about the Children's Online Privacy Code, page 7.

[22] Reset.Tech Australia, Consultation with young people about the Children's Online Privacy Code and consent and agency, page 2.

Your views and evidence

Please provide us with your views and evidence in the following areas:

1. Scope of services covered by the Code

The Act sets out that the Code will apply to APP entities[23] if they provide a:

- Social media service: online services where users connect, share content and interact (e.g. social networks, media-sharing sites, forums, review platforms)
- Relevant electronic service: online services that facilitate communication (e.g. messaging apps, email, video calling platforms, online games with chat)
- Designated internet service: online services that allow users to access or receive material over the internet. (e.g. cloud storage, websites that let users receive/access content, streaming platforms, consumer IoT devices).[24]

In each case, the service must be likely to be accessed by children and must not be a health service provider[25]. However, the OAIC may specify in the Code additional APP entities, or a class of entities to which the Code applies or does not apply. For example, the Code may specify that:

- A provider of a designated internet service may be excluded
- A health service provider may be included
- An APP entity that doesn't fall under the three service types listed above may still be included.

Questions:

1.1 Are there additional APP entities, or a class of entities, that should be covered by the Code? Please provide reasons or evidence to support your view.
1.2 Are there any APP entities, or a class of entities, that should be excluded from the Code's application? If so, on what basis?
1.3 Is there criteria that should be used to determine whether a particular APP entity, or class of entities, is appropriately included or excluded from the scope of the Code?

2. When and how the Code should apply to APP entities

The Act states that the OAIC may issue written guidelines to assist APP entities in determining whether a service is likely to be accessed by children.

Questions:

[23] See Chapter B: Key concepts | OAIC for a definition of APP entities.

[24] Social media service, relevant electronic service and designated internet service are all within the meaning of the *Online Safety Act 2021*

[25] What is a health service provider? | OAIC

2.1 What threshold should determine when a service is considered 'likely to be accessed by children'?
2.2 'Likely to be accessed by children' is the same standard as the Age Appropriate Design Code. Is there any evidence as to the practical effectiveness of the threshold in that context?
2.3 What steps should APP entities reasonably be expected to take to assess whether children are likely to access their services?
2.4 What role, if any, should age gating or other access control mechanisms play in meeting obligations under the Code?
2.5 Are there alternative approaches APP entities could take to meet their obligations under the Code, beyond age gating or age verification methods? If so, is there any evidence on the impact of such approaches on children's access to services or privacy outcomes?

The Act states that the Code may provide differently for different classes of entities, personal information and activities of entities.

Questions:

2.6 Are there classes of APP entities, personal information, or activities of entities, for which different requirements under the Code may be appropriate? If so, what considerations should inform that approach?
2.7 How should the Code accommodate for the varying roles, functions and risk profiles of different kinds of services, activities or personal information?

3. Age range-specific guidance

The OAIC may provide age range-specific guidance, aligning with the UK Information Commissioner's Office's Age Appropriate Design Code, to ensure the development needs of children at different ages are taken into account when drafting the Code.

It is noted that any age-based guidance will not be a 'one size fits all' approach, given the variance of development needs among children, not just due to age but due to other factors, including neurodiversity or learning differences.

The proposed age ranges are as follows:

- 0-5: pre-literate and early literacy
- 6-9: core primary school years
- 10-12: transitional years
- 13-15: early teens
- 16-17: approaching adulthood

Questions:

3.1 Would age-based guidance be appropriate and assist APP entities in tailoring protections and interfaces appropriately and effectively?

3.2 In terms of providing guidance for the processing of children's personal information by APP entities covered by the Code, how appropriate do you consider the above age ranges would be?
3.3 Please provide any views or evidence you have on children's development needs, in an online context in each or any of the above age ranges.

APP specific questions

4. APP 1 – open and transparent management of personal information

APP 1 requires APP entities to manage personal information in an open and transparent way. This includes having a clearly expressed and up-to-date privacy policy that outlines how personal information is collected, held, used and disclosed. Under APP 1, APP entities must take reasonable steps in the circumstances to implement practices, procedures and systems to ensure compliance with the APPs and a registered APP code, and to deal with inquiries or complaints from individuals about their compliance with the APPs or such a code.

The requirement to implement practices, procedures and systems is qualified by a 'reasonable steps' test. The reasonable steps that an APP entity is required to take will depend upon circumstances, such as the sensitivity of the personal information; potential adverse consequences for individuals, such as the risk of harm; the nature of the entity; and the practicability of taking such steps.[26]

Questions:

4.1 What communication methods should APP entities use to ensure privacy policies are meaningfully understood by children of different ages, abilities and backgrounds?
4.2 How should APP entities ensure APP1 obligations are met when their services are used by both adults and children, particularly when children are not the intended primary users?
4.3 What should be considered under the 'reasonable steps' test when implementing internal practices, procedures and systems for managing children's personal information?
4.4 What steps should APP entities take to ensure children, and their parents, can easily make privacy-related inquiries or complaints, and how should APP entities respond in a child-appropriate way?
4.5 Do you have any specific views on how APP 1 should be applied or complied with in relation to the privacy of children?

[26]APP Guidelines, Chapter 1: APP 1 Open and transparent management of personal information | OAIC, paragraph 1.6

5. APP 2 – anonymity and pseudonymity

APP 2 requires APP entities to provide individuals with the option of not identifying themselves or of using a pseudonym when dealing with the entity, unless it is impracticable to do so, or if the entity is legally required or authorised to deal with identified individuals.[27]

Questions:

5.1 How can APP entities provide children with meaningful options to use services anonymously or under pseudonyms, considering their developmental stages at different ages?
5.2 In what scenarios would it be justifiable to require children to identify themselves in order to access an APP entity's service? How can these instances be minimised to protect their privacy?
5.3 Are there instances where age assurance technologies conflict with an individual's right to remain anonymous or pseudonymous, and what evidence supports this, or suggests otherwise?
5.4 Do you have any specific views on how APP 2 should be applied or complied with in relation to the privacy of children?

6. APP 3 - collection of solicited personal information

APP 3 stipulates that APP entities must only collect personal information that is reasonably necessary for or directly related to their functions or activities. Sensitive information, such as health or biometric information, must only be collected with an individual's consent, unless an exception applies. Collection must only be by lawful and fair means and must be collected directly from the individual unless an exception applies.[28]

Questions:

6.1 What criteria should define what is 'reasonably necessary' for an APP entity's functions or activities when collecting children's personal information, and how can APP entities ensure they adhere to this?
6.2 What does 'lawful 'and 'fair' mean in the context of children's personal information? How should these terms be applied specifically for children, given their evolving developmental and digital engagement stages?
6.3 Are there cases in which the collection of children's personal information would not be considered fair in any circumstances?
6.4 How can APP entities obtain genuine consent from children, or their parents or guardians, for the collection of sensitive information?
6.5 Do you have any specific views on how APP 3 should be applied, or complied with, in relation to the privacy of children?

---

[27] Chapter 2: APP 2 Anonymity and pseudonymity | OAIC

[28] Chapter 3: APP 3 Collection of solicited personal information | OAIC

7. APP 4 – dealing with unsolicited personal information

APP 4 outlines how APP entities must handle unsolicited personal information. If an APP entity receives personal information, it did not solicit, it must, within a reasonable period after receiving the information, determine whether it could have collected the information under APP 3. If not, the entity must destroy or de-identity the information as soon as practicable, provided it is lawful and reasonable to do so.[29]

Questions:

7.1 What processes should APP entities implement to identify and appropriately handle unsolicited personal information related to children?

7.2 Do you have any specific views on how APP 4 should be applied, or complied with, in relation to the privacy of children?

8. APP 5 – notification of the collection of personal information

APP 5 requires an APP entity that collects personal information about an individual to take reasonable steps either to notify the individual of certain matters or to ensure the individual is aware of those matters, at or before the time of collection or as soon as practicable after. These matters include, the APP entity's identity and contact details; the facts and circumstances of collection; if the collection is required or authorised by law; the purposes of collection; the consequences for the individual if personal information is not collected; other APP entities, bodies or persons to which the personal information is usually disclosed; information about access and correction in the APP entity's APP Privacy Policy and likely cross-border disclosures of the personal information.[30]

Questions:

8.1 What methods can be employed by APP entities to effectively notify or ensure children are aware of data collection practices in a manner that is age-appropriate and can be easily understood by children?

8.2 How can APP entities ensure that notifications are accessible to children with diverse needs, including those from culturally and linguistically diverse backgrounds, or living with disability?

---

[29] Chapter 4: APP 4 Dealing with unsolicited personal information | OAIC

[30] Chapter 5: APP 5 Notification of the collection of personal information | OAIC

8.3 Are there circumstances in which an APP entity would be justified in taking no steps to notify or ensure children are aware about data collection practices? How can we minimise these instances to ensure that APP entities are adopting a best practice approach when it comes to notification and awareness?

8.4 Do you have any specific views on how APP 5 should be applied or complied with in relation to the privacy of children?

9. APP 6 – use or disclosure of personal information

APP 6 states that APP entities must only use or disclose personal information for the primary purpose for which it was collected, unless an exception applies. Exceptions include if the individual consented to the use or disclosure, or the individual would reasonably expect the entity to use or disclose the information for that secondary purpose.[31]

Questions:

9.1 How can APP entities obtain genuine consent from children, or their parents or guardians, for the use or disclosure of their personal information, while ensuring that they comprehend the implications of such use or disclosure?

9.2 What safeguards should APP entities put in place to prevent the misuse of children's personal information for secondary purposes without appropriate consent or where other exceptions apply?

9.3 What secondary uses or disclosures of personal information could be reasonably expected by children, and how should these expectations vary by age and stage of development?

9.4 Do you have any specific views on how APP 6 should be applied or complied with in relation to the privacy of children?

10. APP 7 – direct marketing

APP 7 prohibits APP entities from using or disclosing the personal information that it holds for direct marketing purposes, unless specific conditions are met. These conditions include obtaining consent from the individual, or if the individual would reasonably expect the organisation to use or disclose the information for that purpose.[32]

Questions:

10.1 Can an APP entity ensure that it creates a 'reasonable expectation' that it may use or disclose children's personal information for the purposes of direct marketing? And if so, how?

[31] Chapter 6: APP 6 Use or disclosure of personal information | OAIC

[32] Chapter 7: APP 7 Direct marketing | OAIC

10.2 How can APP entities ensure mechanisms are in place for children to opt-out of receiving direct marketing communications, in a simple and accessible way?
10.3 Do you have any specific views on how APP 7 should be applied or complied with in relation to the privacy of children?

11. APP 8 – cross-border disclosure of personal information

APP 8 requires APP entities to take reasonable steps in the circumstances to ensure that an overseas recipient of personal information does not breach the APPs, except under certain circumstances. This includes circumstances where the individual has been informed and consents to the disclosure, or the overseas recipient is subject to laws or binding schemes that offer substantially similar protection to the APPs.[33]

Questions:

11.1 How can APP entities ensure that cross-border transfers of children's personal information are conducted in a way that protects children's privacy rights, especially when laws in other countries may not offer equivalent protections?
11.2 What steps should APP entities take to communicate with children (or their parents or guardians) about the risks of cross-border data transfers?
11.3 Do you have any specific views on how APP 8 should be applied or complied with in relation to the privacy of children?

12. APP 10 – quality of personal information

APP 10 mandates that APP entities take reasonable steps in the circumstances to ensure that the personal information they collect, use or disclose is accurate, up-to-date, complete and relevant.[34]

Questions:

12.1 What does 'accurate', 'up-to-date', 'complete' and 'relevant' mean in the context of children's personal information? How should these terms be applied specifically for children, given their evolving developmental and digital engagement stages?
12.2 How can APP entities effectively ensure that the personal information they collect from children remains accurate and up-to-date, considering the dynamic nature of a child's life and the potential challenges in maintaining this data?

[33] Chapter 8: APP 8 Cross-border disclosure of personal information | OAIC

[34] Chapter 10: APP 10 Quality of personal information | OAIC

12.3 Do you have any specific views on how APP 10 should be applied or complied with in relation to the privacy of children?

13. APP 11 – security of personal information

APP 11 requires APP entities to take reasonable steps in the circumstances to protect the personal information they hold from misuse, inference, loss and unauthorised access, modification or disclosure (security risks).

The Act introduced APP 11.3, which clarifies that 'reasonable steps' include both technical and organisational measures. This means that APP entities must not only implement technological safeguards (like encryption, MFA or strong passwords) but also adopt organisational controls such as employee training and standard operating procedures and policies for securing personal information. APP entities must also consider whether it is necessary to retain personal information and take reasonable steps in the circumstances to destroy or de-identify it when it is no longer needed.[35]

Questions:

13.1 Are there any additional or specific *technical* measures that APP entities should adopt to safeguard children's personal information from security risks, considering their heightened vulnerability?

13.2 Are there any additional or specific *organisational* measures that APP entities should adopt to safeguard children's personal information from security risks, considering their heightened vulnerability?

13.3 How can APP entities ensure their data retention policies are appropriate for children's data, including timely deletion or de-identification when the information is no longer needed?

13.4 Do you have any specific views on how APP 11 should be applied, or complied with, in relation to the privacy of children?

14. APP 12 – access to personal information

APP 12 provides individuals with the right to access their personal information held by an APP entity, subject to certain exemptions. APP entities must respond to access requests within a reasonable period (or 30 days if they are an Australian Government agency) and provide the information in the manner requested by the individual, if it is reasonable and practicable to do so. If access is refused, the entity must provide the individual with a written notice outlining the reasons for the refusal, mechanisms to complain about the refusal, and any other matters prescribed by the regulations.[36]

Questions:

[35] Chapter 11: APP 11 Security of personal information | OAIC

[36] Chapter 12: APP 12 Access to personal information | OAIC

14.1 What mechanisms are needed to ensure children can easily access their own personal information?
14.2 In what circumstances might providing a child access not be in their best interests? What would help entities navigate these situations responsibly?
14.3 In what circumstances should a parent or guardian be able to make an access request on their child's behalf and receive a copy of their child's personal information? How should the balance be struck between a parent's right to protect the best interests of their child and the child's right to privacy, when APP entities are dealing with access requests for a child's personal information?
14.4 What timeframe should be considered a 'reasonable period' for responding to a child's access request?
14.5 In what manner or format should personal information be provided to a child when an access request is made, so that it is both practicable for APP entities and developmentally appropriate for children of different ages and capacities?
14.6 Do you have any specific views on how APP 12 should be applied or complied with in relation to the privacy of children?

15. APP 13 – correction of personal information

APP 13 requires APP entities to take reasonable steps in the circumstances to correct the personal information they hold, to ensure that it is accurate, up-to-date, complete, relevant and not misleading. If an individual requests a correction to their personal information, the entity must respond within a reasonable period (or 30 days if it is an Australian Government agency), and, if the correction is made, take reasonable steps in the circumstances to notify any third parties to whom the information has been previously disclosed.[37]

Questions:

15.1 What does 'accurate, 'up-to-date', 'complete', 'relevant' and 'not misleading' mean, in the context of children's personal information, given their evolving developmental and digital engagement stages?
15.2 What processes or mechanisms should be established to allow children to request corrections of their personal information easily?
15.3 In what circumstances should a parent or guardian be able to make a correction request on their child's behalf?
15.4 What timeframe should be considered a 'reasonable period' for responding to a child's correction request?
15.5 Do you have any specific views on how APP 13 should be applied or complied with in relation to the privacy of children?

[37] Chapter 13: APP 13 Correction of personal information | OAIC