



Business Council of Australia

30 July 2025

Office of the Australian Information Commissioner  
via email: [copc@oaic.gov.au](mailto:copc@oaic.gov.au)

Dear Commissioner,

**OAIC Children's Online Privacy Code – Issues Paper**

The Business Council of Australia (BCA) welcomes the opportunity to provide a submission to the Office of the Australian Information Commissioner's (OAIC) Issues paper on the Children's Online Privacy Code (the Code).

The BCA represents and advocates for its members, comprised of more than 130 of Australia's largest employers. We are a member-led organisation, and our submissions reflect engagement with those members and the expertise and practical experience they bring.

Following the completion of the Privacy Act Review (the Review) by the Attorney-General's Department and the passage of the *Privacy and Other Legislation Amendment Act 2024*, Australian businesses have shifted focus to strengthening their privacy frameworks and preparing for the next wave of reforms, including the proposed Code, additional changes that may emerge from the government's response to the Review's recommendations (tranche 2 reforms), and broader regulatory developments affecting digital platforms.

We welcome the OAIC's approach to this consultation process. Its commitment, thorough research, and clear consultation timeframes are to be commended. We also acknowledge and appreciate the time it has dedicated to engaging with our members throughout this process. We look forward to continuing to work collaboratively with the OAIC as the next stages of the Code's development progress.

Over the past decades, investment in privacy controls, awareness, and compliance frameworks has grown significantly - not merely in response to evolving legal obligations - but in recognition of community expectations around the collection, use, and protection of personal information. Our members recognise that privacy is a core element of their brands and their relationships with their customers.

The privacy frameworks established by each of our members are reflective of not only Australian legal requirements, principally the *Privacy Act 1988*, but also international jurisdictions in which our members operate, and specific requirements set out by their own customers.

We acknowledge the government's ongoing commitment to strengthening privacy protections in Australia, particularly in relation to safeguarding vulnerable individuals, most notably, children. When the Privacy Act first commenced in 1988, it was designed for a world dominated by analogue records, long before the dominance of the internet and digital platforms. Today, the next generation of Australians face an entirely different set of privacy risks, as the Attorney-General noted in the second reading speech introducing the 2024 amendments:

*While all Australians face privacy risks in the online environment, children are particularly vulnerable. For many Australian children, social media has been part of their lives from the time they were born. They have never lived in a world without it.*

*It's been estimated that by the time a child turns 13, around 72 million pieces of data will be collected about them<sup>1</sup>.*

The OAIC rightly points out that the aim of the Code is not to prevent children from engaging online, but to ensure their personal information is protected.<sup>2</sup> We believe this is an important objective as, notwithstanding the potential risks that come with being online, there are enormous opportunities for young Australians that come with digital engagement and digital literacy. The OAIC should be mindful that, in developing the Code, it does not inadvertently create regulatory barriers that hinder the development of innovative and beneficial online content for children. Care should also be taken to avoid introducing new risks, such as those arising from the collection of additional personal information to verify an individual's age or from mandated privacy default settings that may inadvertently increase exposure to fraud or scams. We recommend the Code takes a principles-based approach, where any applicable measures are proportionate to any privacy harms posed by a particular APP entity.

In Attachment 1, we outline responses to some of the detailed questions included in the Issues Paper. Our key observations and recommendations are below.

1. Our members, like many other businesses in Australia, already have extensive privacy controls and privacy awareness campaigns specifically designed to enhance the privacy of vulnerable groups of Australians, including children.

**Recommendation:** In drafting the Code, the OAIC should consider the existing tools and safeguards already deployed in the market to protect children's privacy, including data minimisation practices, age-based access restrictions, and parental control mechanisms.

2. Consistent with the UK Age-Appropriate Design Code, we understand the Code will be limited to some online services that are 'likely to be accessed by children'. It is unclear from initial discussions as to how an APP entity would interpret an ambiguous term such as 'likely'. Businesses will be looking for clear guidance on whether the Code applies or not,

**Recommendations:**

- The threshold question of 'likely to be accessed by children' must be clearly defined and backed with unambiguous guidance.
- To maximise clarity for Australian businesses, the OAIC should, wherever possible, consider explicitly excluding certain APP entities from the scope of the Code at the outset. For example, those whose services are not primarily delivered online or who deliver enterprise or business to business services only. This could be achieved by either introducing a clear and comprehensive definition of *online service* or by narrowing the existing definitions of social media service, relevant electronic service, and designated internet service to apply only to their online components.

3. The Code must be compatible with other government legislation and priorities.

**Recommendations:**

- Any new obligations that require the deletion of personal information must be considered against all legislative provisions requiring the retention of personal information.

---

<sup>1</sup> [ParlInfo - BILLS : Privacy and Other Legislation Amendment Bill 2024 : Second Reading](#)

<sup>2</sup> Page 3, [OAIC Children's Online Privacy Code](#)

- Similarly, any new obligations requiring age assurance or the collection of additional personal information for age assurance purposes should be considered against other legislative obligations and international standards for age assurance.
- We would also recommend that the Code's obligations be reviewed against applicable industry and sector laws, regulations and standards and codes to ensure that they work alongside each other and do not introduce conflicting obligations. For example, under the *Telecommunications (Interception and Access) Act 1979* telecommunications providers are required to retain specific types of telecommunications data for at least two years.

4. Extensive privacy protections exist in the current regulatory framework.

**Recommendation:** Any additional safeguards introduced under the new Code must be proportionate and risk-based, ensuring that regulatory focus is directed towards preventing the greatest potential for privacy harm for children.

5. Safeguards that can be put in place to strengthen privacy risks can inadvertently create other risks. For example:

- If geolocation services are blocked by default, then this would undermine digital services such as banking services which rely on geolocation services to prevent fraud.
- If formal age-gating is mandated, digital services may be required to collect more personal information than would otherwise be necessary for user engagement. This approach risks undermining the principle of data minimisation.
- Many APP entities, particularly in the retail sector, employ a significant number of young people aged 15 to 18. Care should be taken to ensure that any new safeguards do not create unnecessary barriers to youth employment. Additionally, measures introduced under the Code should not unduly impact how APP entities engage with employees in this age group, including the marketing of staff-only discounts and other internal communications relevant to their employment.
- If organisations have only limited legal bases to process data lawfully under applicable privacy laws, this may hinder their ability to safeguard young people and uphold the integrity of services designed to prevent the sharing of harmful content. For example, relying solely on consent may not be an appropriate or practical basis for all uses of data necessary to promote safety and platform integrity.

**Recommendation:** All additional safeguards included in the Code must be risk assessed for unintended consequences.

6. Establishing regulatory obligations for obtaining consent to collect, use, or disclose personal information remains a significant and complex challenge for all participants in the digital ecosystem.

**Recommendation:** The Code should rightly encourage APP entities to explore new and innovative approaches to obtaining consent for the collection, use, and disclosure of children's personal information. However, care must be taken to ensure that the implementation of additional safeguards does not inadvertently diminish the significance of consent or contribute to further 'consent fatigue' among users.

7. Many internet services are built for a global audience. Bespoke Australian regulatory requirements will not carry the same priority as the regulatory frameworks of larger economies. The less aligned Australian regulations become with those of larger economies, the more likely we are to miss out on new and innovative internet services.

**Recommendation:** Where practical and feasible, the Code should consider harmonisation with other international standards. Noting Australia's market size relative to other markets of some internet services, an 18-month transition period should be considered so international businesses can account for specific Australian requirements.

8. The proposed age ranges of:

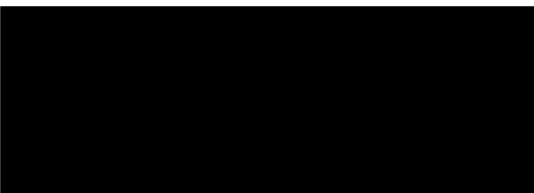
- 0-5: pre-literate and early literacy
- 6-9: core primary school years
- 10-12: transitional years
- 13-15: early teens, and
- 16-17: approaching adulthood

do not align to all age restrictions already established by other regulatory frameworks. For example, basic banking services are generally available to children over 14, while in apps stores apps can be rated 4+, 9+, 12+, and 17+ based on content.

**Recommendation:** To minimise potential misalignment between the developmental age ranges considered in the Issues Paper and those established under other regulatory frameworks, we propose that if age bands are included in the Code they should be considered advisory only and a guide for industry.

We would welcome the opportunity to discuss these comments further and remain available to engage as the OAIC finalises the Code.

Yours sincerely



## Attachment 1 – Issues Paper response to questions

Question	BCA response
<b>1. Scope of services covered by the Code</b>	
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	The scope is sufficiently wide with the inclusion of services media services (SMS), relevant electronic services (RES) and designated internet services (DIS) <sup>3</sup> .
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?	<p>This will be heavily dependent upon the type of safeguards that are included in the registered Code. If, for example, the Code required geolocations services to be defaulted to off, then the Code should exclude online banking services. By complying with such a safeguard, this may conflict with a financial services organisations' existing obligation to detect fraudulent activity and protect customers from external threats and scams. Similarly, telecommunications providers should be excluded given the importance of geolocation to network integrity.</p> <p>We also see merit in the OAIC</p> <ul style="list-style-type: none"> <li>▪ Explicitly excluding certain sectors—such as telecommunications providers (Carriers and Carriage Service Providers), which are already subject to comprehensive data regulatory frameworks—from the scope of the Code to avoid confusion regarding its application.</li> <li>▪ Excluding APP entities whose services are not primarily delivered online from the scope of the Code. This could be achieved by either introducing</li> </ul>

<sup>3</sup> Social media service, relevant electronic service and designated internet service are all within the meaning of the Online Safety Act 2021

	<p>a clear and comprehensive definition of “online service” or by narrowing the existing definitions of Designated Internet Services (DIS), Social Media Services (SMS), and Relevant Electronic Services (RES) to apply only to their online components. We also note that the Code adopts definitions from the Online Safety Act 2021 (OSA), including those for DIS, SMS and RES. Given that these definitions are contained in a separate legal instrument and may be subject to change -particularly in light of recommendations from the recent independent statutory review of the OSA<sup>4</sup> - the OAIC will need to consider how any such changes may affect the operation and interpretation of the Code once it is registered.</p> <ul style="list-style-type: none"> <li>▪ Excluding Enterprise or Business to Business services, as they would not meet the “likely accessed by children” threshold.</li> </ul>
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?	We recommend the OAIC consider excluding classes of entities where they may breach a different regulatory obligation by complying with the Code.
<b>2. When and how the Code should apply to APP entities</b>	
2.1 What threshold should determine when a service is considered ‘likely to be accessed by children’?	<p>All parts of the digital ecosystems should be able to clearly identify when and how the Code applies to them. This not only includes APP entities themselves, but also designers and users of those services.</p> <p>If formal age-gating is mandated, digital services may be required to collect more personal information than would otherwise be necessary for user engagement. This approach risks undermining the principle of data minimisation.</p>
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?	

<sup>4</sup> [Report of the Statutory Review of the Online Safety Act 2021](#)



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?	
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	
3.1 Would age-based guidance be appropriate and assist APP entities in tailoring protections and interfaces appropriately and effectively?	<p>The age ranges do not align with all age restrictions already established by other regulatory frameworks. For example, basic banking services are generally available to children over 14, while apps available through the various app stores can be rated 4+, 9+, 12+, and 17+ based on content. Principles-based guidance that gives organisations sufficient discretion to design relevant solutions is preferable to prescriptive guidance that forces organisations to operationalise children's privacy in a way that does not account for the nature, scope, usage, technical complexity, etc. of a service.</p> <p>In designing the Code, the OAIC should be mindful of potential misalignment between the proposed age ranges and those established under other regulatory frameworks. This misalignment has the potential to cause conflict between different regulatory regime and additional compliance burdens for APP entities.</p> <p>Any age ranges applied under the Code should be advisory only.</p>
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	
4. APP 1	
4.1 What communication methods should APP entities use to ensure privacy policies are meaningfully understood by children of different ages, abilities and backgrounds?	In drafting the Code, the OAIC should consider the existing communication strategies, tools and safeguards already deployed in the market to protect



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?	children’s privacy, including awareness campaigns, data minimisation practices, age-based access restrictions, and parental control mechanisms.  In a principles-based framework, organisations should have discretion to design solutions that are appropriate for their industry and services etc.
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?	
5. APP 2	
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?	We do not offer specific observations or recommendations in response to questions 5.1 to 5.4.
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	
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?	<p>The Code should encourage APP entities to explore new and innovative approaches to obtaining consent for the collection, use, and disclosure of children's personal information. However, care must be taken to ensure that:</p> <ul style="list-style-type: none"><li>▪ The implementation of additional safeguards does not inadvertently diminish the significance of consent or contribute to further 'consent fatigue' among users.</li><li>▪ The Code should not require APP entities to collect more personal information than they otherwise would to provide the service, for example, for the purpose of age verification. Doing so would conflict with the principle of data minimisation and could deter individuals from using beneficial online services.</li></ul> <p>In our view, there needs to also be a recognition within the Code that consent is not always the most appropriate lawful basis on which data should be used to promote safety and integrity of online services.</p>
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?	
7. APP 4 – dealing with unsolicited personal information	
7.1 What processes should APP entities implement to identify and appropriately handle unsolicited personal information related to children?	We do not offer specific observations or recommendations in response to questions 7.1 and 7.2.
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	
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?	Regulators and businesses must continually balance the need for consent mechanisms that are clear, transparent, and easily understood with the inherent difficulty of explaining complex technological processes and diverse data-use scenarios.



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?	<p>Traditionally, consent for collection has been sought through lengthy privacy policies or statements. It is therefore unsurprising that the Issues Paper highlights ‘jargon and length’ as key barriers to understanding how and why personal information is collected, used, or shared.</p> <p>Some of our members already have invested in additional controls after assessing the risks of their digital services, this includes:</p> <ul style="list-style-type: none"><li>▪ Default private settings for under-18 users.</li><li>▪ Providing safety nudges that encourage responsible use.</li><li>▪ Have parental oversight tools to support family engagement in privacy management.</li></ul>
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?	
<b>9. APP 6 – Use or Disclosure of personal information</b>	
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?	<p>Further to our comments above, we note that some of our members already have additional controls including:</p> <ul style="list-style-type: none"><li>▪ A range of safeguards to support children’s privacy, including tools that allow parents or guardians to oversee and adjust their child’s privacy settings, and to view or delete the child’s data.</li><li>▪ Raising awareness of privacy settings and protections, including targeted communications during initiatives such as Privacy Awareness Week.</li><li>▪ Sharing examples of best practice in communicating privacy policies and notices to different customer cohorts, including children.</li></ul>
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	
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?	<p>We acknowledge the research presented in the Issues Paper, which highlights that direct advertising (and therefore direct marketing) is concerning to children. We note:</p> <ul style="list-style-type: none"><li>▪ Australian consumers, regardless of age, are also protected from unsolicited marketing (spam) through the very stringent requirements in the Spam Act 2003.</li><li>▪ Privacy is a core element of our members’ brands and value proposition. Should businesses overstep what is considered a reasonable expectation, then there are significant ramifications for an organisation through customer turnover and brand value decline.</li><li>▪ Many of our members offer a variety of avenues for individuals to opt out of direct marketing including through ‘unsubscribe’ options, phone, email, webform, in store or by post. Should alternative channels be proposed, we would welcome the opportunity for further consultation.</li></ul>
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?	
APP 8 – Cross-border disclosure of personal information	
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?	<p>We do not offer specific observations or recommendations in response to questions 11.1 to 11.13. Although we note:</p> <ul style="list-style-type: none"><li>▪ Most cross-border transfer schemes across the globe do not have transfer safeguards that are unique to children; most are data subject-agnostic. The OAIC should avoid creating separate and unprecedented transfer obligations.</li><li>▪ APP entities already disclose the existence of cross-border transfers in their privacy policies / notices.</li></ul>
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?	
APP 10 – Quality of Information	
12.1 What does ‘accurate’, ‘up-to-date’, ‘complete’ and ‘relevant’ mean in the context of children’s personal	We do not offer specific observations or recommendations in response to questions 12.1 to 12.3.



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?	
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?	
11. APP 11 – security of personal information	
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?	<p>We acknowledge the research presented in the Issues Paper, which highlights:</p> <ul style="list-style-type: none"><li>Children’s awareness of privacy risks: The evidence demonstrates that children are acutely aware of the need to protect their personal information from malicious actors. In our view, APP 11 remains sufficient to safeguard all types of personal information. It requires APP entities to protect, manage, and responsibly dispose of personal information through a context-sensitive, risk-based approach supported by appropriate technical and organisational controls. Should further options be proposed to improve how APP 11 protections are communicated to children, we would welcome continued consultation.</li><li>Children’s desire for control over their data: The Issues Paper reflects children’s preference for being able to delete their data and to provide explicit consent before their information is collected, shared, or used. Similar sentiments have been echoed publicly by the Privacy Commissioner.<sup>5</sup> As noted in the government’s response to The Review, the Privacy Act operates within a broader digital and data regulatory ecosystem. We do not consider it appropriate to impose standalone</li></ul>
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?	

<sup>5</sup> [Children's Online Privacy Code will give Australian children a 'right to forget' digital data collected from online games or educational apps. | The Australian](#)

	<p>deletion requirements without due consideration of the wider legislative framework. We therefore support the Privacy Act Review's recommendation that the Commonwealth undertake a review of all legislative provisions requiring the retention of personal information to ensure they balance policy intent with the privacy and cyber security risks associated with holding large volumes of personal data.</p>
<b>12. APP 12 – access to personal information</b>	
14.1 What mechanisms are needed to ensure children can easily access their own personal information?	<p>We do not offer specific observations or recommendations in response to questions 14.1 to 14.6, other than to note:</p> <ul style="list-style-type: none"> <li>• If the definition of 'personal information' is expanded, as recommended in The Review, corresponding changes will be required to the mechanisms for accessing and correcting personal information — particularly where the information is not readily accessible or is inferred rather than directly collected.</li> <li>• The majority of our members offer a variety of avenues for individuals to access their personal information in their privacy policies, including by phone, email, webform, in store or by post. Should alternative channels be proposed, we would welcome the opportunity for further consultation.</li> <li>• Many age-agnostic data access tools (e.g., self-service tools) are designed with all customers in mind. OAIC should avoid creating a subset of access rights and mechanisms that are unique to children as they would introduce disproportional operational and technical burdens and would be a departure from global norms.</li> </ul>
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?	

13. APP 13 – correction of personal information	
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?	<p>We do not offer specific observations or recommendations in response to questions 15.1 to 15.5, other than to note:</p> <ul style="list-style-type: none"> <li>• If the definition of ‘personal information’ is expanded, as recommended in the Review, corresponding changes will be required to the mechanisms for accessing and correcting personal information, particularly where the information is not readily accessible or is inferred rather than directly collected.</li> <li>• The majority of our members offer a variety of avenues for individuals to correct their personal information in their privacy policies, including by phone, email, webform, in-store, or by post. Should alternative channels be proposed, we would welcome the opportunity for further consultation.</li> </ul>
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?	

