Submission to: Office of the Australian Information Commissioner (copc@oaic.gov.au)

Consultation: Draft Children's Online Privacy Code

[redacted]

Date: 3 June 2026

This submission if for public viewing.

Contents

1. Types of Entities using children's personal information

The legislation/code could go further in defining who this applies to.

A. Entities should be grouped into types based on how they use a child's information

To bring this code/legislation in line with the realities of the online world, it would help to clearly delineate the types of organisations dealing with children's information in a "real world" or physical world sense. There should be a simple hierarchical grouping which places entities into different types for example 1. social service entities (including government and semi government), 2. Online tech-driven entities (Including internet search engines, social media, gaming among others) and 3. retail commercial entities.

A-1 Social service organisations

Organisations which have traditionally held information about children, were mainly institutions with a social service leaning. This included medical profession, schools, hospitals, physical community groups, sports groups among others. These are purpose led organisations with the goal of providing meaningful services to people. Many are even not for profit. Holding people's personal information was a function of providing the service in particular, with the aim of having contact with family in the case of emergency. The organisaions do not need to keep a copy of a person's identifying documents on hand. By convention, it is simply enough to verify who a person is by sighting a document and recording that it has been seen. In these scenarios the information may be written down on an application paper or in a register and would probably never (or rarely) see the light of day again. Today these organisations do perhaps hold more personal information but only for purposes that relate to the service they are providing. It would be considered unethical to use that kind of information for marketing or sales purposes.

A-2 Online tech-driven entities

The kinds of online tech-driven entities (including search engines, social media, gaming and other entities) which are seeking to engage with people (including children) today are first and foremost profit making organisations. They have shown themselves to be uber-commercial profit takers. As a part of this they use a person's information, and online behaviour, to maximize profits in the most extreme way, by using technology to profile as much as possible about a person and their behaviour as they can, because this provides current and future opportunities to make money from that information. This group includes interactive search engines, gaming industry, social media, online marketplaces, influencers and online sellers of extremely cheap products. They interact strongly with end-users and have power over them.

In addition this group also has power over the other groups of business entities as described here (ie. social service organisations and retail commercial organisations).

A-3 Retail commercial entities

This is the third group of entities which have characteristics in different measures to both of the above. These are 'other' retail commercial businesses which sell products and services for a profit. Possibly the biggest group, by numbers of businesses, they are essentially retail product and service businesses. These include: grocers, chemists, newsagencies, building trade business, exercise services, beauty and grooming services, law firms, insurers, car sellers, psychologists etc and many more. Some of these organisations have a relatively high level of customer profiling as a part of their businesses, however there is a wide variety as to how much this occurs across this sector and they do not have as much profiling ability as the online tech-driven entities.

All of the above three groups of business entities may have online components of their administration of personal information, however, these groups are very different and the way they use information is very different. This should be spelt out in the legislation/code and also, it could be used as a basis to look at the consent given to these different groups of entities and treat them differently.

In other words, having different entity classes would facilitate a clearer delineation of the different types of consent. Online services particularly games, social media etc should be treated with much more restriction than services of people enlisted to help those in need for instance. This is because online uber-commercial entities have much more access to and power over a person's information.

B. The question of why info is needed should inform the code

The purpose of what information is used for, by entity types should also be considered.

Online companies seek information just for the purpose of profiling to make money off individuals using algorithms. This is quite different from the other kinds of organisations as described above.

Algorithms and avatars have not even been mentioned in the exposure draft and this may indicate a lack of understanding of the hegemonic nature of algorithms and tech-driven entities in the online sphere. They are part of the online sphere and the legislation may benefit by the use of more recent relevant terminology, such as these words age-inference and other terms used in the explanatory statement.

C. Inordinate power differential of entities in the online tech-driven sphere requires special treatment

Uber-commercial, tech-driven companies roam the digital sphere asking for consent and there is no option but to give it if you wish to use the product, other than to say no and therefore not engage with the product. The odds are stacked in favour of the online entities to such an extent

that they have created an environment in which they represent a hegemony. Unfortunately, this environment is a large part of the everyday life of many people today.

Algorithms are an incredibly powerful use of technology which underlines much of the activity of online tech-driven entities. They represent the power of online entities over the people using the online product, whatever it may be. Computers use calculations to make software respond in a certain way. As an example, this is like when you click a box to save the information you have just entered - perhaps an order of a book or other product and the computer goes and makes an invoice or summary page or takes you to the cart etc. Algorithms are like this but they are used to keep a record of everything you do and to analyze it for patterns, which are then used in further calculations to interact with you. It is an early kind of AI and it is going to become even more powerful as the use of AI increases.

The ownership of online data should invest in the person who it pertains to or in the case of children, their parent/responsible person and not any organisation. There is a huge difference between other business (including social service organisations and retail commercial businesses) and online tech-driven entities (many of whom operate in an anonymous environment) which is completely unsafe to anybody entering it, in particular children. This is an important distinction and essential difference, which is often overlooked and misunderstood. This anonymous environment does equate to, and should be equated to, the “wild west” and the outcomes in this online wild west so far, have been very poor. This is why it is very important to regulate this strongly and as soon as possible. These organisations have access to a large amount of powerful information about people. Even when personal information is not provided online tech-driven entities can make assumptions by using technology to analyse end-user behaviour with remarkable accuracy.

The online tech-driven sector is by far the biggest exploiter of people, including children and should be regulated accordingly.

The references to 30 and 60 day provisions in the exposure draft, are irrelevant in the online sphere, in particular where actions can be taken by the end-user themself. It is applying an out of date dynamic and needs to be updated urgently, to give the legislation/code relevance to the online sphere. It is also giving online tech-driven entities a free kick by not requiring them to implement systems which give end-users control of their own data, including to delete it themself. Online tech-driven entities can and should do this and perhaps if legislation required them to (especially if there were penalties for being in breach) then they would.

D. An illustrative scenario to show the difference between uber-commercial online tech-driven entities and other business entities

Although this legislation/code is being devised with the objective of allowing young people under the age of 15 (or preferably 16) to be protected in the online environment and participate in online

activities in a way which proves their age, it is inadvertently exposing them. This seems to be an unintended consequence of the legislation/code. Companies likely say that they need to know how old a person is so that they do not serve them the incorrect information however, the protection of children in the real world does not require them to carry around their personal ID and pull it out every time they walk into a shop. The online environment needs equate to the real world.

The code/legislation appears to have the following intentions:

- the code intends that the personal information of young people/children is used to prove their age;
- the code intends that young people/children will provide their personal information (presumably items such as identity cards or birth certificates) to show how old they are.

None of this equates to the real world and is in fact an inversion of it.

In the real world people of legal age are required to show their age credentials, so that they can participate in adult activities, not the other way around. In the real world children/young people are protected by their parents/responsible person. (There are obviously exceptions, however the accepted convention which is a part of our societies practices and laws, is that parents or responsible persons are responsible for the welfare and decisions relating to children.)

The online sphere is a very different and far less safe (and often anonymous) place than the real world, where actors, in particular online tech-driven entities, are face to face with individuals invading their personal space, asking the individual constant questions and seeking compliance in ways that cover the entity and expose the individual. Whilst there are many people in the real world who we don't know as we walk past them in the street, these people or businesses do not constantly come up to you and invade your personal space to seek answers from you or constantly ask for consent or put adverts right in front of you - between you and whatever you are doing. It is a big difference. There is a distance between the anonymous actors in the real world and those in the online world. In the online world there is no distance.

Maintaining the standard of the real world in this regard (ie. a distance between actors) has important safety ramifications. In the real world children/young people do not need to walk around with an ID to show that they are underage and it is essential that the equivalent situation is created online. This could be done by a system which allowed for the dual login for both a child and their parents/responsible adult to be created. For details please see section 4 of this submission.

RECOMMENDATION 1: Divide business entities into classes of meaningful groups from the perspective of their use of individuals' personal information and how they interact with individuals. Use these classes to define how entities are allowed to manage personal information and to define different types of consent. This in particular should take into account that online tech-driven entities are different to all others and have power over

individuals through their use of algorithms. Legislate that online tech must provide the ability for individuals to delete their own data.

2. Best Interests of a child

Consent for children belongs with parents/responsible person and decisions about giving a child's information to any organisation, should invest in them, not with the child and not with any external organisations (including online tech-driven companies, government agencies or commercial retailers etc).

The legislation seems to place some decisions about what is in a best interest of a child with the organisations holding the child's information.

As described in section 1 of this report the purpose of online tech-driven businesses is purely to make profit. This is very different from the purposes of social service and retail commercial organisations.

This legislation/code would be much stronger if it mandated that children dealing with the entities that this code applies to, who are under 16, must have a parent/responsible person make the consent decisions for them.

The exemptions to this should be particularly narrow and limited. For instance, in the interests of a child's safety, in a police or counsellng situation, there may be a need to obtain assent of a child in addition to or instead of their responsible person. Section 20 of the exposure draft (*Assent of child must be obtained in certain circumstances*) should deal with these kinds of exceptions and yet it seems to benefit businesses (online entities) which seems to be the opposite of the intent of this legislation. This is likely to be the result of lobbying by online tech-driven business entities and seems like another unintended consequence of the legislation.

Exemptions such as those in *Section 20 Assent of child must be obtained in certain circumstances* or *Section 32 Subsection (3) Request to destroy personal information about a child* **should never apply to online tech-driven entities.** Instead, Section 20 of the legislation seems to give the child an ability to deal with entities without the input of their parent/responsible person.

Section 32 Subsection (3) should state that social media and other online tech-driven entities should destroy personal information immediately after it has been used to obtain an age and that the entity can only record the year and month of a person's birthday.

Whilst children may want to have an online life they are still subject to their parent's wishes and this is an accepted convention in use in Australian society, business and everyday life. It is even more important in the online sphere. Inadvertently removing this convention could severely disrupt

parents/responsible persons' abilities to manage their children's best interests both online and in the real world.

It is difficult enough for adults to negotiate what is happening in the rapidly changing digital sphere and it is going to only get faster with the introduction of AI. It seems many of us, including government personnel, don't understand the hegemonic power that digital companies have over them.

We have already seen the tragedies which have occurred to children engaging in the internet, which has been facilitated by the lack of regulation on online business entities and the anonymity of many of these sites which allows predators to pretend they are a friend.

The current draft of this legislation/code is too weak and does not take the above into consideration, but rather seems to treat all organisations with a paradigm that was suitable to bricks and mortar business before the year 2000. This is no longer fit-for-purpose and as has been illustrated, there are significant differences between all three classes of business entities which should be addressed in different ways.

To use the allusion to the wild west in section 1 above (Types of entities, page 4) the idea of letting your child go off for an exploration in the wild west on it's own would horrify most people. The idea of doing this oneself is unappealing enough. Further, the idea of identifying children in an anonymous environment by giving their documents to an online organisation, when millions of adults around them are anonymous, is completely horrifying and should be avoided at all costs. This is the implication and an unintended consequence of this legislation/code.

RECOMMENDATION 2: Throughout the legislation/code adhere to the principle that the only people that can give consent for a child under the age of 15 or 16 are their parents or responsible person/s and rewrite the entire code accordingly, including scrapping Section 20. This principle should also underpin what is in the best interests of a child as an accepted convention which already exists in our society.

3. Proposal for Dual Login with parental authentication

The premise of this draft legislation/code contains an assumption that we need to know the age of children in the online domain in order to protect them as minors. This may have been understandably prompted by the under 16's social media ban.

However, there are alternative ways of protecting children in the online environment without exposing their personal details to organisations, including ways which more closely resemble the

real world. One such way this could be achieved is with a dual login which includes additional authentication, which would be sent to the parent/responsible person any time that consent was needed or money to be spent or other activities in which children would normally be supervised. This would potentially resolve a lot of loose ends in this legislation/code.

This would require that when a child registers for a new online service/app/game etc, they would need their parent/responsible person to do it for and with them. In this way the parent/responsible person would have the login and it would need to be authenticated via contact with the parent/ responsible person. The young person would have an avatar with a unique name. Any requirement for consent to be given would trigger an authentication request code to the parent/responsible person.

This system might include the requirement that the parent/responsible person would use a piece of identifying ID (preferably a licence or ID Card) which would be verifiable. The parent/responsible person would only need to verify that the child is legitimate rather than providing the personal information of the child. The online agency would only need to have on it's files the month and year of the child. This means that the status of child would expire in the month rather than strictly on their birth date.

The details of how to make it work technically would need to be discussed with the technical people at the government agencies which administer licences and ID cards and other IT people. However, please do not accept an argument that this cannot be done, particularly if it is coming from online tech-driven entities.

RECOMMENDATION 3: Keep children's identification documents off the internet as a form of ascertaining their age. Use the principle that children under the age of 15 or 16 cannot provide consent themself but it must be given by their parent/responsible person. Invent a system where the parent/responsible person uses their ID to vouch for the child in a dual login method including additional authentication via the parent/responsible person.

4. Unintended Consequences of this legislation could be serious

There is a key difference in the way that the online tech-driven entities and other business entities, have access to, handle and use personal information. Online tech-driven entities have access to so much information about how an end-user behaves that they profile people and create algorithms to interact psychologically with an individual. Instead of using these insights in a beneficent way to help people and sometimes take a fair profit (or no profit at all), they use them for the sole goal of maximising making money in a blatantly exploitative manner.

This legislation in several ways, as described throughout this submission, assists online tech-driven and other business entities by reducing the ability of the parent/responsible person of children to have the appropriate say over a child's consent. In effect, this has the potential to substitute parental rights and influence on their children with an 'industry attachment'. This is already occurring and is devastating for some families.

This is a result of an understandable failure on behalf of Governments around the world to regulate online tech-driven entities as the industry emerged, despite warnings from industry insiders such as in The Social Dilemma, (2020 from Netflix). That doesn't mean it is too late to introduce responsible legislation and the recent social media ban was one important step. This *Privacy (Children's Online Privacy) Code* is another step in the right direction, however, it needs to take into consideration the power differential that exists between online tech-driven entities and humans. The current exposure draft doesn't seem to give enough consideration to this but it does give benefits to business entities at the expense of children's privacy and in it's current form would be a disservice to children, parents/responsible persons and Australia as a whole. There is an opportunity here to create a valuable piece of legislation that is potentially being missed by making it too weak.

Not only could these unintended consequences increase the current difficulties families are having in their homes, but they could also give online tech-driven businesses a large stake in children's lives and cause the the commercialisation of childhood — a time which should be free and unchained.

There are many things in the non-online world that need to be preserved and this legislation may as an unintended consequence wipe some of that out. This includes the ability to interact with other humans on an in-person basis. Interacting in person has special qualities that can only come from lived experience. There is a deeper experience of humility, compassion, trust etc when engaging in human to human communication, and this is still not equalled in the online sphere. While these things can be understood online they are not part of the core business of online tech-driven interactive commercial entities.

The biggest casualty would be the ability of parent/responsible adult to make decisions for their children. Some parts of this legislation effectively give responsibility to the children and the effect of this is to potentially erase their childhood because they become a responsible person too soon and do not get to enjoy the no worry time of innocence of childhood.

This would also create conflict between parent/responsible person and the child. There are many examples of where this has already been seen in the last 10-15 years where children have been allowed to go into the online realm without any supervision making decisions for themselves, becoming addicted to the 'high' response to constant gratification (ie. the pings, the likes and fast moving interaction). There are many parents who have lost control of their children and in many

cases, children have lost their lives in these unsupervised realms, mainly because predators lurk there. The responsibility of this legislation to assist in the prevention of further loss of life is a heavy, serious and urgent one.

RECOMMENDATION 4: Change the content of this draft legislation/code to ensure that the decision making about consent for children resides entirely with their parent/responsible person and never is given to organisations dealing with children, not even via the children themself.

5. Further consultation required

The legislation/code appears to benefit business rather than safeguard children and in line with the existing privacy legislation it seems very weak. It should be held off and undergo a further full public discussion, which does not seem evident.

It would be a disservice to Australia to implement the exposure draft as it is. The digital world is such a big part of our every day life and children from today onwards, are those who will experience it more than those of us who remember a different reality.

The number of respondents to the earlier consultation being only 61 and a few hundred school children having filled in surveys (as referenced on the OAIC website) are deeply concerning, low figures for such an important consultation with very serious and long-term ramifications for children (now and when they grow up), their parents/responsible persons and the wider Australian society.

RECOMMENDATION 5: Undertake a further consultation which should be promulgated to all schools and state Education Departments to raise awareness of this extremely important issue. To raise then interest in this issue the OAIC consultation website should also contain a counter showing how many people have filled out the online forms and workbooks and how many submissions have been received.
AI should not be used to make any arbitrating decisions about anything in this code.

6. Comments on specific sections of the legislation/code exposure draft

Comments on various sections of this legislation/code are provided in the following table.

Submission: Draft Children's Online Privacy Code

Item	Section number and wording	Comment	Suggested alternative/action
	On several occasions an entity is defined as being an organisation among other things, eg section 10 subsection (6) (c)	What does an "entity that is an organisation" mean?	Perhaps include in *Definitions* the meaning of "organisation" such as in "an entity that is an organisation".
	8 Ascertaining the age of end-users of an entity's service Division 1 - General Requirements	This section should have a purpose added. There are too many exemptions and they should be dramatically reduced in number. This could be achieved by investing responsibility for providing the information to an entity in the *parent / responsible adult* .	The purpose might be something like "ascertaining a person's age and exemptions".
	8 (3) *The entity may collect personal information about an end-user of the entity's service before ascertaining the end-user's age only to the extent that the information is necessary for the entity to comply with subsection(1)]*	This seems to negate the intended effect of subsection (1) especially if this code is primarily for online use, as seems to be indicated in **Part 2 Application of this code**. It also seems to create a circular situation, which should be avoided.	This could potentially be solved by having a dual kind of login which required the child's *parent/responsible adult* to create the login with their adult identification and to create a joint login for the child at the same time. Therefore, all communications to the child for consent should be directed to the *parent/responsible adult* and any entity which did not do so would be in breach. This might at first sound difficult but it wouldn't be…. It would just be a matter of technical configuration. In addition, a dual login would potentially safeguard children from putting their information on the internet at all.

Item	Section number and wording	Comment	Suggested alternative/action
	8 (4) *The entity must, as soon as practicable after complying with subsection (1), destroy sensitive information that is collected as mentioned in subsection (3) if: (a) the information is not contained in a Commonwealth record; and (b) the entity is not required by or under an Australian law, or a court/tribunal order, to retain the information.*	This subsection seems to negate the idea of safeguarding children's personal information altogether. For instance, it seems to be saying that an entity can keep a child's date of birth (which is a Commonwealth record) on record. Entities such as online games and social media really do not have a reason to keep a child's personal information and in fact the *parent or responsible adult* should vouch for a child so that the details of their information is kept away from online companies, as is satisfactory in the real world.	Using a dual login attached to a parent or responsible adult would avoid the need for a child's identifying personal information to be given to online anonymous gaming or social media sites. A child (through the above dual process) should only need to provide their month and birth year to prove their age for the purposes of online interactive activities.
	8 (5) *This section does not apply if the entity applies this Code, other than this section, in relation to the entity's service regardless of the age of end-users of the service.*	This subsection should be deleted. This appears to have the potential to completely override the idea of safeguarding the personal information of children in the online sphere. It seems ambiguous and unclear. Children should be protected in whichever environment they are in, be it online or in person.	
	Div 2 Consent		
	13 (1) *Consent to the collection, use or disclosure of personal information about a child may be given by the child only if the child is at least 15 years of age.*	The age for consent should be 16 years old rather than 15 and this should be changed throughout the code. This would be consistent with social media minimum age requirements. Any child under 16 logging into any site or dealing with any entity should have a login which has been created by their parent/responsible person who would receive an authentication request.	Change the age from 15 to 16 years in the code and in any relevant related legislation and use dual login.

Item	Section number and wording	Comment	Suggested alternative/action
	14 (1) *Consent to the collection, use or disclosure of personal information about a child must be voluntary.*	This seems tricky and could be difficult for entities. How can they ask for consent if it is to be voluntary. Perhaps this could be worded better. In addition a portal upon entering the site/app etc could come up (like sites selling alcohol) but could be more effective because once a person has registered with the dual login of their responsible adult, they would then have a login.	"*Notwithstanding that an entity must advise an individual that consent is required in order to use their service,* consent to the collection, use or disclosure of personal information about a child must be *given voluntarily*."
	14 (2) In determining whether consent is voluntary, an entity seeking consent from an individual must consider: (a) the alternatives open to the individual if the individual does not consent; and (b) the seriousness of any consequences for the individual, the individual's family members or the individual's associates if the individual does not consent.	This subsection puts too much importance on the consequences if consent is *NOT* given. It would seem better to state it in the positive.	"In determining whether consent is voluntary, an entity seeking consent from an individual must consider: (a) the consequences to the individual if the individual gives consent; and (b) the seriousness of any consequences for the individual, the individual's family members or the individual's associates if the individual gives consent; and (c) the alternatives open to the individual if the individual does not consent; and (d) the seriousness of any consequences for the individual, the individual's family members or the individual's associates if the individual does not consent.

Item	Section number and wording	Comment	Suggested alternative/action
	16 (2) *Consent is current if:* *(a) the entity sought the consent from the child, or a person with parental responsibility for the child, at the time the information was collected, used or disclosed; and* *(b) the consent has not been withdrawn; and* *(c) either: (i) the period mentioned for the purposes of paragraph 15(3)(c) has not expired; or (ii) the entity obtained further consent to the collection, use or disclosure of the information before that period expired.*	This section would benefit by including a period within which the consent needs to be updated such as one (1) year.	Change this to include a time period of one (1) year. Consent is current if: (a) the entity sought the consent from the child, or a person with parental responsibility for the child, at the time the information was collected, used or disclosed; and (b) (b) the consent has not been withdrawn; and (c) (c) either: (i) the period mentioned for the purposes of paragraph 15(3)(c) has not expired; or (ii) the entity obtained further consent to the collection, use or disclosure of the information before that period expired; or (iii) a period of one year has NOT passed since consent was obtained.

Item	Section number and wording	Comment	Suggested alternative/action
	17 *Consent can be withdrawn* *(1) An individual who has given consent to the collection, use or disclosure of personal information about a child may, at any time, withdraw the consent.* *(2) An entity must provide a clear, simple and easily accessible means for individuals to withdraw consent for the purposes of subsection (1).*	This section should include a time limit within which the consent withdrawal must be acted upon. This is an example of where the difference between social service organisations and online tech-driven organisations should be clearly delineated. Social service organisations could be subject to the 30 and 60 day rules as outlined in several sections of the code already whereas online tech-driven entities should be required to either provide a facility where the end-user can withdraw consent immediately (doing it themself online) or within 14 days if there is a technology malfunction affecting an entity which prevents the withdrawal/deletion from occurring instantly. The 30 and 60 day allowances are not fit for purpose in the online world where most things are able to be enacted by the press of a button. The legislation should be modernised to take this into account and to make tech-driven organisations accountable. Technology organisations are accustomed to dealing with outages etc and also driven by ensuring those outages are rectified as quickly as possible. Outages affect their core business and they would not need anything like 30 days to fix something like this.	17 (3) *(1) If a child requests to withdraw their personal information from an entity that is a social service organisation, then (despite Australian Privacy Principle 12.4(a)(ii)), the entity must respond to the request:* *(a) if a reasonable period to respond to the request is less than 30 days after the request is made—within that reasonable period; or* *(b) if subsection (2) applies—within 60 days after the request is made; or* *(c) otherwise—within 30 days after the request is made.* *(2) This subsection applies if:* *(a) the entity reasonably considers that, having regard to the complexity and number of requests for access to personal information the entity is dealing with, more than 30 days is needed to respond to the request; and* *(b) the entity notifies the child that the entity will respond to the request within 60 days after the request was made and of the reasons why the response cannot be provided within 30 days; and* *(c) the notice is given within 30 days after the request is made.* *17 (4)* *Any entity that is an online tech-driven organisation, must include in their website/app or similar technical vehicle (including game boxes residing in customer's homes) by which the online service is provided, a facility which allows for instant withdrawal of consent and/or deletion of a customer account and this should remove all details of the child and the child's parent or responsible adult's information from the records of the organisation.* *.....Continued next row*

Item	Section number and wording	Comment	Suggested alternative/action
	17 continued		*(a) If a child requests to withdraw their personal information from an entity which is an online tech-driven organisation, then (despite Australian Privacy Principle 12.4(a)(ii)), the entity must respond to the request by having ensured that the facility to delete is already available in the product before it is marketed.* *(b) If subsection (2) applies—the entity must respond within 14 days after the request is made.* *(2) This subsection applies if:* *(a) the entity experiences a technical malfunction that prevents the withdrawal/deletion facility from working properly; and* *(b) having regard to the complexity of the malfunction the entity is dealing with, more than 7 days is needed to rectify the malfunction; and* *(c) the entity notifies the child that the entity will respond to the request within 14 days after the request was made and of the reasons why the response cannot be provided immediately; and* *(d) the notice is given within 7 days after the request is made.* *17 (5)* *(a) Technology (including AI) should not be used to make any arbitrating decision on how an account is deleted other than technology being used to facilitate the end-user to withdraw/ delete their account instantly, as described in section 17 subsection (4) for online tech-driven organisations or for raising reports for human attention.* *(b) An entity must keep a record of the customer account number (but not including the personal information of the customer) and the dates for which the account was active as a part of their auditing process.*

Item	Section number and wording	Comment	Suggested alternative/action
	18	This section is very good and should not be allowed to be watered down	Maintain and ensure it is not watered down.
	19	This section is very good and should not be watered down	Maintain and ensure it is not watered down.
	20 Assent of child under 15 years must be obtained in certain circumstances *(1) This section applies to an entity if:* *(a) a child under 15 years of age is an end-user of the entity's service; and* *(b) the child enables the entity to: (i) collect sensitive information about the child; (ii) use or disclose personal information about the child for a purpose other than the purpose for which it was collected; or (iii) use or disclose personal information about the child for the purpose of direct marketing.*	20 Parts of this section are very weak [including all of 20 (1) and 20 (2) & also 20 (6)] and seem to negate the intention of this piece of legislation and some of the other sections. Indeed it seems to put the best interests of the child BELOW the best interests of the business entity. Section 20 seems to benefit online organisations based on a premise that if a child has consented to something the business entity has some right, despite the intent of the code, to prevent access to children's information. Section 20 may apply if the consent has been given prior to the implementation of the legislation/code. This should be acknowledged as an exceptional circumstance. If it occurs after the implementation then the business should be subject to penalties. A child under the age of 15 (or preferably 16) should not be able to give consent without the parent or responsible person knowing and being contacted. In particular this is going to be more prevalent with online interactive tech-driven services such as games and social media etc	"Assent of child under 15 years must be obtained in certain circumstances" could become "*In addition to the consent of the parent or responsible adult the* assent of a child under ~~15~~ 16 years must be obtained in certain circumstances". Using a dual registration for children which includes their parent or responsible adult could prevent the assent being given by children without their parent/responsible person knowing because it would require third party authentication whenever a consent/assent is required by the entity. Entities would be required to use their technology to request permissions/consents and these should go to the responsible adult registered with the child. Whilst companies might claim they cannot do this it would be an inaccurate claim. Doing this would be modernizing legislation to appropriately make online tech-driven entities more accountable and penalties should apply if a child has given assent/consent without the authentication request being sent to their parent/ responsible person. *….continued next row*

Item	Section number and wording	Comment	Suggested alternative/action
			This is another example of a circular situation where the consent or assent should not have been given according to the rest of this code. This should be re-written as a penalty to organisations which have obtained consent/assent from a child without the knowledge of their parent/responsible adult. The title of section 20 ***"Assent of child under 15 years must be obtained in certain circumstances"*** should be re-written as "*Assent of child under 15 years must be **reversed** in certain circumstances"*
	20 (2) The entity must seek the assent of the child: (a) to that collection, use or disclosure; and (b) for the entity to contact a person with parental responsibility for the child for the purposes of obtaining consent to that collection, use or disclosure.	Again this section is a circular situation and should be removed because the child should not give assent or consent without the responsible person knowing.	
	20 (6) (b)	This does not read well and seems illogical. This may contain a typo - there is no period mentioned in 5 (b) (ii)	
	21	This section is very good and should not be allowed to be watered down	Maintain and ensure it is not watered down.
	Division 3 Transparency		
	25 (2) (a)	25 (2) (a) The should stipulate that the records should be permanent	"(a) keep *permanent* records of the reviews undertaken for the purposes of subsection (1); and"

Item	Section number and wording	Comment	Suggested alternative/action
	28 (1) “28 Right to request information about handling of personal information (1) If a child, or a person with parental responsibility for a child, requests access to personal information about the child under Australian Privacy Principle 12.1, the child or person may also request information about the entity’s handling of the child’s personal information, to the extent the entity holds that information.”	The words *“to the extent the entity holds that information”* provide an option for organisations to outsource the holding of their information to another body (that they own or don’t own) and use it as a loophole to avoid upholding the requirements of this part of the code. They are responsible for the personal information they obtain, whether they have outsourced management of it, or not, and should be accountable. In addition, the use of algorithms is a part of the way in which online entities handle personal and sensitive information. The algorithms should also be able to be requested. Even better still mandate that this information is accessible at any time via the online platform itself.	28 (1) Remove the words “to the extent the entity holds that information”. ie: “28 Right to request information about handling of personal information (1) If a child, or a person with parental responsibility for a child, requests access to personal information about the child under Australian Privacy Principle 12.1, the child or person may also request information about the entity’s handling of the child’s personal information, ~~to the extent the entity holds that information~~.” Consider the following additions: “Algorithms must be available to the end-user in a form that can be understood in common English, so that they know how they are being assessed and impacted.” “Algorithms must be accessible at any time via the online platform itself.”

Item	Section number and wording	Comment	Suggested alternative/action
	29 Opt out of direct marketing (3) The means must not incorporate processes or features that make it difficult to make the request. (4) Information about the means must be: (a) located in a prominent position and displayed in a font size and type that is easy to read; and (ii) Age appropriate.	29 (3) should specify that this includes not having to login again somewhere else. 29 (4) (ii) It appears there is a typo and that (ii) should read (b)	Add extra phrase to (3): (3) The means must not incorporate processes or features that make it difficult to make the request “and without the need to login to another site/form/portal or similar”. (4) Fix typo
	Division 4		
	Div 4 Purpose section is missing	It would be helpful if Division 4 included a purpose section, as it helps in understanding the intent of the section.	

Item	Section number and wording	Comment	Suggested alternative/action
	Div 4 Access to, and correction of, personal information about children	A system which requires that information not be held about children is better and should be mandated through this code. Access to one's information should be available along with the ability to delete the information. The knowledge of a child's age and status is invested in the child's parent/s or responsible person. In the real world this is good enough when it comes to participating in a game or leisure activities for children.	Provide a system of dual registration that requires a parent or responsible adult to be registered with a child and therefore the child's information does not need to be shared. The provision by the responsible person should only need to include the birth year and month. The responsible person will provide their own information and this will be used as assurity about the child's information. The parent/responsible person should not be able to be approved without their information. They bare the liability for their child. Alternatively, the viewing of information (via the parent/ responsible person) could be adequate to verify a child's age and the personal information does not need to be kept on record. In this scenario the online entity would record the child's birth year and month only.
	Division 5		
	Div 5 Purpose section is missing	It would be helpful if Division 5 included a purpose section, as it helps in understanding the intent of the section.	
	Division 6		
	Div 6 Purpose section is missing	It would be helpful if Division 6 included a purpose section, as it helps in understanding the intent of the section.	

Item	Section number and wording	Comment	Suggested alternative/action
	Division 7		
	7 (34) This Division sets out how entities are to comply with Australian Privacy Principle 1 in relation to enabling inquiries and complaints about the entities' handling of personal information about children.	The grammar in 7 (34) seems incorrect. This can be important as it can change the meaning of words. Please check this and rectify it.	7 (34) might be better as : This Division sets out how entities are to comply with Australian Privacy Principle 1 in relation to enabling inquiries and complaints about ~~the~~ an entity's (or entities') handling of personal information about children.
	Division 8		
	38 (2) Note: Harms and impacts may include *(but are not limited to)* those of a physical, emotional, developmental or material nature.	It may be more comprehensive if the *note* included the words "*but are not limited to"*	38 (2) Note:could be written as Note: Harms and impacts may include *(but are not limited to)* those of a physical, emotional, developmental or material nature.
	38 (3) The privacy impact assessment must be conducted before the new service or activity is made available to end-users, or the new or changed way is implemented.	Could this section include a clause to say that penalties will apply under some other criminal code (if appropriate) if the impact statement is not conducted? Could this legislation require the submission of an impact statement to the privacy commission whenever it is done?	

Item	Section number and wording	Comment	Suggested alternative/action
	40 (1) An entity must ensure that all persons who are employed or otherwise engaged by the entity and who have regular or frequent access to children's personal information in the course of performing their duties participate in education and training about protecting personal information about children.	This should state that the education must be provided by a recognised and accredited educational institution, which is independent of the entity obtaining the training. This would be an example of where it may be helpful to distinguish between types of entities, because staff providing actual social services to children have already undergone child safety checks and may have education that is aligned with safety and other WHS type safety certificates. These would not normally be needed in staff of organisations providing online tech-driven activities.	40 (1) (i) An entity must ensure that all persons who are employed or otherwise engaged by the entity and who have regular or frequent access to children's personal information in the course of performing their duties participate in education and training about protecting personal information about children. (ii) The education and training shall be conducted by a recognised and accredited educational institution, which is independent of the entity obtaining the training.
	40 (2) (c) (ii)	Education and training should only be required at onboarding and/or every 3-5 years or if there is a substantial change to the legislation or a change to an entity's privacy impact assessments as specified in section 38 of this code. It is unproductive to do it every year.	