Office of the Victorian Information Commissioner

Phone: 1300 00 6842
Email: enquiries@ovic.vic.gov.au
PO Box 24274
Melbourne Victoria 3001

4 August 2025

Ms Carly Kind
Australian Information Commissioner
Office of the Australian Information Commissioner

By email only: copc@oaic.gov.au

Dear Ms Kind,

Thank you for the opportunity to make a submission to the Office of the Australian Information Commissioner's (**OAIC**) Children's Online Privacy Code consultation for industry, civil society, academia and other interested stakeholders.

The Office of the Victorian Information Commissioner (**OVIC**) is the Victorian integrity agency with oversight of privacy, freedom of information and information security in Victorian Public Sector (**VPS**) organisations. This oversight is enabled by both the *Privacy and Data Protection Act 2014* and the *Freedom of Information Act 1982* (Vic).

OVIC is supportive of the development of a Children's Online Privacy Code (**the Code**). Acknowledging that this is a multi-disciplinary and complex area, OVIC's submission will cover the following:

- Maximising children's control of their personal information and privacy decision-making capacities
- Increasing transparency of all aspects of personal information relating to children's online services
- Improving understanding of the barriers to genuine consent in the context of children.

If you would like to discuss this submission any further, please contact [redacted], Senior Policy Officer, via [redacted]

Yours sincerely

Sean Morrison
Victorian Information Commissioner

OVIC submission to the OAIC's Children's Online Privacy Code industry consultation

The rapid development, democratisation and uptake of the Internet of Things (IoT) has outpaced the speed with which effective regulatory mechanisms can be established. While this may have allowed for faster realisation of the benefits of the IoT, it has also accelerated the realisation of harm, particularly for vulnerable cohorts like children. The IoT has placed the world within a child's reach and enabled their interaction within communities at a younger age. Conversely, it has exposed children to new privacy risks that their parents may not have been exposed to until they were adults.

Applications, social media services and online content distribution platforms (online services) can only exist at scale if they are able to monetise their consumer base. It makes sense that these online businesses try to diversify the ways in which this monetisation occurs. However, without proper regulatory guardrails around these practices, parents and children are left exposed to harms that contravene their rights, and other harms that they may not even be aware of.

While regulatory guardrails can minimise these harms, they should be designed with consideration of other harms that children may be exposed to. For example, the Children's Code will have tangible ramifications for victims of family violence. The Children's Code should, therefore, consider the complex interplay between children's online safety, family dynamics and family violence. This should include rigorous protections for victims of family violence.

OVIC agrees fully with the OAIC's position that the point of a Children's Code cannot be to prevent children from engaging in the digital world.[1] Rather, the Children's Code should mandate that online services consider, protect and uphold children's right to privacy. In doing so, some of the harms of the IoT and online services can be mitigated and risks minimised.

Scope of services covered by the Code

1. OVIC is supportive of the broad inclusion of online services within the scope of the Code. While the flexibility mechanism allows the OAIC to specify additional APP entities for inclusion or exclusion, a comprehensive explanation should be provided and published where an online service has been excluded. This would improve transparency and maintain public confidence in the Code.

2. Recognising that while this is an online privacy code, the OAIC may wish to consider how to deal with similar non-internet based services. For example, iMessage on an iPhone will presumably be captured by the Code, whereas an SMS message will not. In this case, the functionality is similar, though only one service is captured by the Code. Excluding some online services from the Code may make them more desirable to children. It may be worthwhile evaluating the effect the implementation of the Code will have on children's use of non-internet based services such as SMS.

[1] OAIC Children's Online Privacy Code Issues Paper. p 6.

3. Similarly, there may be online services or apps that are designed to be used with children's personal information but operated by an adult. This may include digital learning tools and apps intended for use by teachers, early childhood educators, childcare workers and others who work with children. The OAIC should consider whether these online services could be included within the Code.

When and how the Code should apply to APP entities

1. OVIC considers that the 'likely to be accessed by children' test should be a risk-based assessment that considers:
    a. Whether there are restrictions on children's access
    b. The type of content and whether it would be appealing to children
    c. Whether children are known to use the service or any evidence that the service may be accessed by children (peaks in traffic during school holidays)
    d. The quantity of known child users as a proportion of the total users of the service
    e. The marketing of the online service.

2. Children may seek out other similar online services that are excluded from the Code if they are unable to access an online service (or aspects of that service) that is included in the Code. This means the 'likely to be accessed by children' test will be affected by whether or not an online service is included in the Code. Put another way, exclusion from the Code may make an online service more desirable to children, particularly those that are on the threshold of inclusion or just outside inclusion. Therefore, guidance on the Code should reflect that if an APP entity is unsure whether their online service is likely to be accessed by children, then that APP entity should take steps to comply with the Code in respect of that online service.

3. Online services that sell or sell access to personal information should have particular requirements under the Code. Children and parents should be made aware that an APP entity is selling or selling access to their personal information and the notification should be obvious and easy to understand. The notification should be additional to its inclusion in the APP entity's privacy policy and should require the user's acknowledgement. This would increase transparency and help children and parents to understand that their personal information will be sold beyond the online service itself.

Age range-specific guidance

4. OVIC is supportive of age range-specific guidance.

5. The guidance in the Code should complement broader privacy guidance for each age range. This broad guidance would help those who work with children understand the most appropriate privacy actions and conversations to be having with a particular cohort. This is necessary as early childhood educators are increasingly using digital learning tools that use children's personal information.

APP 1 – open and transparent management of personal information

6. The Code should be about returning control of personal information back to children and, in many cases, their parents or guardians. One way to do this is through openness and transparency about the APP entity's management of personal information. OVIC is very supportive of enhancing the transparency of how APP entities use, disclose, handle, store and dispose of children's personal information. This transparency also helps parents and guardians understand the risks their children are exposed to, and whether a particular online service is appropriate for their child's use.

7. Privacy-related enquiries or complaints should be accessible and easy to make. Children, parents and guardians should be able to make enquiries before giving personal information to an online service.

APP 2 – anonymity and pseudonymity

8. Consideration should be given to the ability to use online services without a requirement to set up an account and subsequently log in at each use.

9. The creation of a username, even a pseudonymised username, should be restricted to online services where that username is necessary for the online service to function. In all other instances, it may be appropriate for there to be no option for children to enter a username. This restriction should extend to other personal information such as location, age and contact details.

10. Where a name is necessary for the online service to function, children may not understand that they do not have to use their real name. Online services should make it clear that users do not have to use their real name or encourage them to use a pseudonym. Further, the Code should prohibit free text boxes that ask for a last name or a full name, where this information is not necessary for the online service to function.

APP 3 – collection of solicited personal information

11. The Code should stipulate that children's personal information must only be collected where it is reasonably necessary to their use of the online service. APP 3 may enable the collection of data that is necessary to the function of the APP entity, such as an entity that sells access to data, but is not necessary for the use of one of that entity's online services. Due to children's vulnerability and lack of understanding of privacy, the collection of their information should be restricted to their immediate use of the online service.

12. The OAIC may wish to consider a blanket prohibition on the collection of young children's biometric information by an online service. Biometric information is particularly sensitive because it cannot be changed if compromised.

13. Genuine consent will be a consideration for online services that require sensitive, biometric or health information to function, such as menstrual cycle tracking apps. Genuine consent is discussed further at paragraphs 22 – 24.

14. There should be specific guidance provided to online services that collect biometric information. Those services must be required to do what is reasonably necessary to ensure the user has sufficient understanding of the sensitivity of biometric information.

15. The Code should empower children to take control of their privacy as much as possible. Outsourcing a child's privacy decision-making capacity to a parent or guardian may negatively impact that child's relationship with privacy in the future. For example, that child may not understand the importance of protecting their own personal and sensitive information when they are an adult because they have not interacted with privacy decision-making before.

APP 4 – dealing with unsolicited personal information

16. OVIC is of the view that unsolicited personal information should be deleted within a particular timeframe.

17. Developers should minimise the use of free text boxes when designing pages that collect personal information. This should reduce the risk of the collection of unsolicited personal information.

APP 5 – notification of the collection of personal information

18. The purpose of a notice of collection is to increase transparency around an entity's use of personal information and help users take control of their personal information.

19. Children under a certain age cannot be expected to understand the purpose and contents of a notice of collection. If an online service is likely to be accessed by that specific age range, then that online service should take reasonable steps to notify the parent or guardian or ensure the parent or guardian is aware of the collection of personal information.

20. Older children may be able to understand a notice of collection. However, the notice should be made accessible to this specific age range using multimedia and age-appropriate language.

21. A prominent 'I don't understand' button could be provided alongside a notice of collection so that online services can receive feedback where their APP 5 obligations may not have been fulfilled. This button will enable children, parents and guardians to initiate a dialogue with that online service to better understand how personal information is being collected, used, stored and disposed of.

APP 6 – use or disclosure of personal information

22. Children under a certain age cannot provide genuine consent. The House of Lords decision of *Gillick v West Norfolk Area Health Authority* [1986] A.C 112 stands for the principle that 'the parental right to determine whether or not their minor child below the age of sixteen… terminates if and when the child achieves sufficient understanding and intelligence to understand fully what is proposed.'[2] The decision was applied in Australia in *Secretary of the Department of Health and Community Services v JWB and SMB* [1992] HCA 15.[3] Online services should consider how they can assess whether a child possesses this sufficient understanding and intelligence.

23. The APPs outline situations where consent is required such as secondary disclosure or the collection of sensitive information. Where user consent is required, online services could offer modified, reduced functionality access to those that do not provide consent. This gives users greater control of their personal information because their participation in the online service is not conditional to handing over greater control of their personal information to the online service. This is particularly pertinent for online services where a refusal to participate could impact a child's social and psychological wellbeing.

24. Genuine consent cannot be provided where it is encouraged through 'dark patterns' – that is, design features that manipulate the user into choosing a particular option. For example, big, green 'Let's get started' buttons to indicate consent contrasted with hidden or red 'I don't want to use this service' buttons. Another example is where an online service makes the user feel guilty or rushed in the process of providing consent.

25. The Code should expressly address how an online service can seek genuine consent from children and parents. This guidance should discuss 'dark patterns', coerced consent and other barriers to genuine consent.

26. The reasonably expected test may prohibit the secondary use and disclosure of young children's personal information. Children under a certain age may not be able to have reasonable expectations and older children may have a very limited understanding of what an APP entity may do with their personal information. The Code should explain that children of different ages have different expectations to adults and so what a reasonable child reasonably expects will be different to what a reasonable adult reasonably expects.

27. The Code should provide guidance to APP entities on how best to safeguard the confidentiality, integrity and availability of children's personal information. Safeguards to prevent misuse of children's personal information can include:

[2] *Gillick v West Norfolk Area Health Authority* [1986]. Accessible at https://www.bailii.org/uk/cases/UKHL/1985/7.html
[3] *Secretary of the Department of Health and Community Services v JWB and SMB* [1992] HCA 15. Accessible at https://jade.io/article/67674

a. Training of staff within the APP entity
b. Strict access controls and an access log
c. Implementing a robust information security framework.

28. The OAIC should consider whether online services that are intended for children should have an executive staff member with a working with children's check or similar. This ensure that the governance body of a children's online service contains a person who has been screened to work with children.

APP 7 – direct marketing

29. OVIC is of the view that young children's personal information should not be used or disclosed for the purpose of direct marketing. At the same time, older children may have a preference to receive advertising that is targeted to them.

30. In many cases, direct marketing requires the user to be profiled. This profiling helps advertisers and online services identify what content to push to which users. This means a child with a particular profile will continually be fed content that aligns with the online service's view of their identity. As children's identities are fluid and evolving, consistently consuming content aligned with a singular perspective may be harmful to their development. In extreme cases, this content may be psychologically harmful to the child where they have been identified as someone with a particular characteristic such as mental illness or social isolation. The profiling of children under a certain age should be prohibited. Profiling and its potential harms should be communicated to older children before they begin using the online service.

31. Children should be given the option of resetting all profiling data collected about them. This option should be thoroughly communicated and easy to access within the online service. Upon resetting, all profiling data should be immediately destroyed.

32. Since the direct marketing conditions in the *Privacy Act 1988* (Cth) are similar to those for use and disclosure, the discussion of genuine consent and reasonable expectations in paragraphs 21 – 25 are also relevant.

33. Children should not be required to opt-out of direct marketing and profiling. All direct marketing should be off by default and require the user to opt in.

APP 8 – cross-border disclosure of personal information

34. Users should be informed, regardless of the circumstances of cross-border disclosure, where and to whom their personal information is going. This should be mandatory in cases where consent for cross-border disclosure is sought from parents, guardians or older children. Further, where consent is being relied on, users should be told whether their personal information will be subject to similar protections in the jurisdiction where their data is going.

APP 10 – quality of personal information

35. Online services should provide an easy, self-engaged method for children to vary their details to reflect an accurate, up-to-date, complete and relevant understanding of who they are at any given point in time. Similarly, online services should enable the ability to delete reference to former personal information attributes.

36. However, the dynamism of a child's life and identity should not justify online services continually prompting that child to update their personal information. This may collect more information than is necessary and create a digital footprint of that child's life and decisions. This digital footprint is personal information and is likely not necessary for that online service to be delivered.

APP 11 – security of personal information

37. Online services should enable maximum privacy settings by default. Younger children should need parental or guardian approval to modify these setting. Parents, guardians and older children should be informed of what implications each setting has for their control of their personal information when attempting to modify default settings.

38. Without adequate protections, third party arrangements can introduce risks to the confidentiality, integrity and availability of children's personal information. The Code should provide guidance to APP entities on the engagement of contracted service providers and how children's privacy protections can be passed on to those providers.

39. OVIC recommends the OAIC consider the automatic deletion of children's personal information from an online service after a period of inactivity. Children may experiment with different online services and subsequently not return to those platforms. A specified period of inactivity on the platform should indicate that the retention of that child's personal information is no longer necessary for the functions of that online service. It follows that the APP entity should delete this information. Automation would ease the administrative burden of this process. Automated deletion of personal information should be included in a notice of collection to improve transparency and inform children, and/or their parents and guardians that their privacy will be safeguarded in this context without them having to take any action.

40. The approach to destruction and retention should be reasonable and balanced. However, the Code should consider how destruction could be used to inflict harm. For example, using a social media platform to cyber bully another child and requesting that all evidence be deleted immediately after the harm is inflicted. A victim's ability to produce evidence should be protected.

APP 12 – access to personal information

41. Enabling children's access to their own personal information includes designing an access policy and process that children can navigate. Accessibility can be enhanced with:

a. Clear, age-appropriate plain language
b. Short messages delivered in various formats
c. Avoiding block text and long paragraphs
d. Considering the relevant age range and diverse backgrounds of children likely to access the online service.

42. Access to personal information introduces risks of harm to children that, like destruction and retention, must be balanced in the Code. The OAIC should consider how access to personal information could harm children. For example, an abusive parent or guardian attempting to access their child's personal information or a child accessing information on how an online service has profiled them. OVIC broadly supports increased access to information and supports the Code incorporating greater nuance and balance in its access guidance to account for the vulnerability of children.

APP 13 – correction of personal information

43. The accuracy, completeness and relevance of a child's personal information that is held by an online service is ultimately decided by the child as they develop and move through digital engagement stages. APP entities have a responsibility to ensure that their online service is maintaining accurate records.

44. As the accuracy of a child's personal information is decided by that child, a parent or guardian should only be able to make a correction request where:
    a. The online service can, where practicable, verify that the child has given consent
    b. Where a guardian can substantiate a significant risk of harm to the child
    c. If the child is deceased.

45. As discussed in paragraph 34, children should not be subject to constant reminders to update their personal information. However, online services can ensure that there are a variety of ways that children can request a correction of their information. These requests should be self-initiated, simple and easy to navigate.