CHILDREN & MEDIA AUSTRALIA

Thriving in a digital world

31 July 2025

Office of the Australian Information Commissioner

By email to: copc@oaic.gov.au

SUBMISSION ON CHILDREN'S ONLINE PRIVACY CODE

Thank you for the opportunity to provide a submission to the development of this timely and important Code.

Children and Media Australia (CMA) is the national peak not-for profit body representing the interests of children as media consumers. Its mission is to support families, industry and decision makers in building and maintaining an enjoyable media environment that fosters the health, safety and wellbeing of Australian children. Its membership includes major national and state education, welfare and parent organisations and individuals.

CMA's core business is to collect and review research and information related to children and the media; to provide information and advice on the impact on children of print, electronic and screen-based media; to provide reviews of current movies and apps from a child development perspective; to advocate for the needs and interests of children in relation to the media; and to conduct and act as a catalyst for relevant research.

The chief aim of the CMA submission to the Issues Paper is to provide input as to how the Children's Online Privacy Code can best address the special privacy rights and needs of children (as expressed in UN *General Comment 25 on Children's Rights in Relation to the Digital Environment* (2021)).

This submission sets out CMA's considered views on selected questions in the Issues Paper on which we have an informed view. For other matters we commend the submission being prepared by Reset.Tech Australia, which is more comprehensive, and which benefits from that organisation's considerable expertise in the matter of online privacy. We also endorse Reset.Tech's range of Policy Briefings relevant to this inquiry, available here.

Further information about this submission can be obtained from [redacted],

Children and Media Australia
PO Box 1240, Glenelg South SA 5045
61 8 83762111 61 8 83762122
info@childrenandmedia.org.au
www.childrenandmedia.org.au

Answers to selected questions

1.1 Are there additional APP entities, or classes of entities, that should be covered by the Code?

It is not immediately clear whether the list of services covered includes the makers of entertainment apps. The *Online Safety Act's* definition of 'designated internet service' is 'a service that allows end-users to access material using an internet carriage service', suggesting that it would cover app stores, or platforms that enable the playing of games online, but not the makers of apps that users download and play on their own devices. Therefore these entities would be covered by the COPC only if they are APP entities, which in turn would require that they have an annual turnover of more than $3 million.

In 2021 CMA's project *Apps can trap: privacy tips and checks* made some disturbing findings about the overt and covert tracking behaviours of popular apps used by children, and consequent invasions of children's privacy. CMA would strongly suggest that there is no type of service whose coverage by the Code would be more justified. If we are right in thinking that the category of 'designated internet service' does not include the makers of downloadable apps, CMA submits that the COPC should be extended to apply to those entities, whether or not they meet the standard definition for an APP entity.

CMA is strongly of the view that educational technology (EdTech) and advertising technology (AdTech) companies should be covered by the Code. The former, in particular, exist primarily to attract young users, often with a business model that relies heavily on the collection and onsale of data. The OAIC would be aware of ongoing litigation in the USA against EdTech companies for their data-gathering practices. We would go so far as to say it would be a travesty not to include them in the Children's Online Privacy Code.

The latter group, AdTech platforms, are not quite so obvious an inclusion, but given the very widespread use of business models that rely on targeted advertising that covers children and young people, and the general recognition among children's professionals that advertising to children is problematic and possibly unethical, CMA suggests this opportunity to regulate AdTech should not be missed.

It is possible, should such entities be covered, that other aspects of the Code would need to be revisited and made more nuanced. For example, it might not always make sense to talk about 'users' of AdTech, considering that advertising is normally presented to users of other services, without those users having chosen to see it.

2.1 What threshold should determine when a service is 'likely to be accessed by children'?

CMA applauds the use of a 'likely to be accessed' (LTBA) test in the COPC. Many other regulations which ostensibly aim to protect children's interests use a test of 'aimed at',

'directed at' or similar – as if the intent of the creator or distributor of content is the key determinant of children's rights. The LTBA test recognises the reality that children access much material that is not (primarily) intended for them, in places that are not designed for them. In doing so the test is considerably more likely to provide effective protection from undesirable experiences. If nothing else, it removes the loophole whereby creators and distributors can sidestep regulations simply by making a declaration of their own intent, or at least open up an argument about such matters, where children are all too often the losers. Moreover, the test centres children's needs and takes their rights seriously. In the words of the Convention, it treats 'the best interests of the child [as] a primary consideration' (article 3).

Similarly, CMA would oppose any kind of test that were based on the platform's 'actual knowledge' that children are accessing it, as this only encourages platforms to turn a blind eye – that is, actively to avoid learning about their users. An LBTA test encourages curiosity and action in these matters, which can only enhance the consideration given to children's interests.

Regarding the question of a threshold, a rights-protection approach would counsel as broad an application as possible, in order to maintain a realistic approach about children and how their lives are lived. In that spirit, CMA would suggest a threshold to cover services that are:

1. Likely to be accessed because they are directed to or intended for children, or a sub-group of children; or
2. Likely to be accessed by children as demonstrated by either:
   a. Evidence that the number of children using the service is more than minimal; or
   b. The type of service being one that is likely to attract children, or a sub-group of children (even if it is not directed to or intended for them).

2.3 What steps should APP entities reasonably be expected to take to assess whether children are likely to access their services?

Many APP entities and internet services sell advertising space, and in this context are known to make claims about their audience demographics, including the numbers of children of various ages. In such cases, there are no additional steps required; rather, the entities need only make that information public in the regulatory context.

Whether or not such information is available, the threshold described above points the way to three distinct approaches to assessing whether children are likely to access a service:

1. If a service is directed to or intended for children, one would normally expect that this would be obvious to all, including the APP itself. If there is any doubt, the service would presumably be considered under paragraph 2a above; see point 3. below.
2. Gathering of evidence about children's use of the service, and a clear definition of what would amount to a 'minimal' number of children. This should be an absolute number

rather than a proportion of children overall. The existence of a large proportion of children who do not access the service does not alter the protection needs of those who do. In addition, based on children's tendency to follow trends set by their peers, low usage at one point can't be assumed to mean low usage at a later point.

3. Regarding the question of 'likely to attract children', this too will often be obvious. However, it would be appropriate to have an independent watchdog with resources to monitor the services available, whether they are likely to attract children, and whether they are recognised as such by the APP in control of them. Such resources should include regular access to child development specialists who can make an informed assessment based on an up to date, evidence-based knowledge of children's preferences and habits. That is, it should not be a matter of guesswork by the APP itself. If a service is found to be likely to attract children, and the APP in question has not recognised it as such, there should be provision for directing it to do so and adapt its practices accordingly.

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

CMA is strongly in favour of any system that recognises children's stages of development and acts as a reminder to all concerned that for most regulatory purposes we cannot simply lump all under-18s together. The appropriate and effective tailoring of protections and interfaces could be a somewhat complex matter, but it is certainly worthwhile having a conversation about how it could work. In any case, APPs should always remember that even some very young children access online services – so platforms cannot assume even that all their users can read, let alone that they understand even simply written terms and conditions, for example.

3.2 In terms of providing guidance for the processing of children's information by APP entities covered by the Code, how appropriate do you consider the [nominated] age ranges would be?

In CMA's considered opinion, the nominated age bands (0–5, 6–9, 10–12, 13–15, 16–17) are appropriate for guiding data processing, as they reflect key developmental differences in children's capacity to understand and manage online privacy.

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.

CMA would suggest the following:

- **0–5**: No meaningful understanding of data; highest protection required.
- **6–9**: Emerging independence but minimal comprehension; highly vulnerable to persuasive design.
- **10–12**: Increasing autonomy, but limited abstract reasoning; require strong default protections.
- **13–15**: Developing understanding, but still susceptible to manipulation and social pressure; clear, age-appropriate guidance essential.
- **16–17**: Closer to adult capacity but not fully mature; enhanced agency with ongoing safeguards.

This structure aligns with children's cognitive, social, and emotional development and supports a 'privacy by design' approach that evolves with age and capacity.

4.2 How should APP entities ensure APP1 obligations are met when their services are used both by adults and children, particularly when children are not the intended primary users?

CMA would question the relevance of the identification of 'intended primary users'. For reasons explained above, where children's rights are in play, intent is beside the point. Therefore, if an entity meets the test for inclusion in the COPC, it should abide by appropriate standards; and if this means there is additional openness and transparency for adults as well, so much the better.

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?

CMA imagines there may be a degree of trial and error in these matters; therefore the best approach would be to set up a dedicated mechanism for ongoing monitoring and guidance. This could operate from within a civil society organisation, a unit within the regulatory body, or the APP entities themselves. Wherever based, those involved should be informed by the most up to date evidence about child development.

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?

As with other questions touching on the concept of evolving capacities, CMA submits that this should be seen as a process, rather than a matter of ‘set and forget’. That is, there should be a dedicated mechanism for keeping up to date with emerging research about child development, and adjusting rules, policies and practices accordingly, in close consultation with experts in the field.

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?

CMA submits that there should be a comprehensive definition of ‘personal information’; and requirements that children’s privacy be protected at systems levels through data minimisation and ‘privacy by default’.

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?

CMA submits that the determination of such methods is a job for the dedicated mechanism referred to elsewhere in this submission.

8.3 Are there circumstances in which an APP entity would be justified in taking no steps to notify children are aware about data collection practices?

CMA has been unable to identify any such circumstances.

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?

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?

CMA mentions these two questions together because our answer to each is essentially the same: the questions refer to things that simply should not happen.

Children should not be targeted with direct marketing communications; indeed, we would suggest a minimum age for them to be able to opt in.

Nor should cross-border transfers of personal information be allowed at all, for the principal reason that appears in the question itself: it then becomes impossible to protect that information.

12.1 What does 'accurate', 'up-to-date', 'complete' and 'relevant' mean in the context of children's personal information? How should these terms be applied specifically for children, given their evolving development and digital engagement stages?

CMA notes that information about children and their lives is likely to change and become out of date more rapidly than the equivalent information for adults. Therefore it would be appropriate to have different rules for children, where entities have an enhanced duty to verify accuracy etc, and to delete information of which they cannot be sure.

Conclusion

CMA thanks the OAIC once again for the opportunity to comment on children's needs and rights in relation to the Code. In summary, we are of the view that children's best interests need to be front and centre in all aspects of data gathering and handling, and we trust that the Code will ensure that such is the case. We also believe it is crucial to the Code's success that adequate resources be dedicated to ongoing monitoring of its operation and continuous updating of the information and evidence on which it is based.

**********END OF SUBMISSION**********