

Submission to the consultation on the Children's Online Privacy Code

July 2025

For further information or questions about this submission please contact:

[REDACTED]
[REDACTED]
UNICEF Australia
[REDACTED]
[REDACTED]

Table of Contents

Executive Summary 3

Summary of Recommendations..... 3

Detailed Recommendations..... 4

 1. Children’s rights as a guiding principle for the Children’s Online Privacy Code 4

 2. The scope and application of the Children’s Online Privacy Code 4

 3. The collection and use of children’s data 5

 4. Direct marketing towards children 6

 5. Children correcting and reclaiming their data..... 7

 6. Implementation and enforcement of the Children’s Online Privacy Code 7

Executive Summary

Guided by the United Nations Convention on the Rights of the Child (CRC) and informed by our work in over 190 countries improving the lives of children including in digital environments, UNICEF Australia welcomes the opportunity to provide a submission to the consultation on the Children's Online Privacy Code.

The current generation of children are the first true digital natives. They will never know a world without smartphones. Constant connectivity is their norm. They will have an online presence almost immediately after birth, and they already disproportionately occupy online spaces more than any other group, meaning the design of those spaces will have a greater impact on them and for longer than any other generation before them. This is particularly the case given their unique developmental vulnerability.

UNICEF Australia envisions an online world which minimises risks and harms to children's safety and wellbeing, at the same time as providing all the positive benefits when we enable them to thrive in an increasingly digital world. We know that data from children and young people is treated as a commodity - collected, traded and sold at unprecedented rates. Yet for young children, concepts like privacy can be difficult to understand, and they may unwittingly divulge information to third parties that places them at risk.

UNICEF Australia's own research shows that young people in Australia are both highly aware of privacy as an issue, and uncomfortable with the current state of affairs. We surveyed over 2,000 teenagers and found that:

- 86% regularly take steps to protect their privacy
- 14% do nothing to protect their privacy
- 72% are uncomfortable with their personal data being collected by apps and websites, and
- 66% are uncomfortable with companies predicting their behaviours and preferences based on personal data.ⁱ

The development of Australia's first-ever Children's Online Privacy Code (the Code) is a significant opportunity to address these concerns that young people hold. In this submission, UNICEF Australia offers a series of recommendations in response to the questions outlined in the issues paper. These range from the Code being guided by children's rights, to adopting a broad definition of services likely to be accessed by children, requiring child-friendly privacy policies and maximum privacy settings by default to protect children's data, and giving children the ability to reclaim their data through a right to erasure.

UNICEF Australia has been pleased to see the genuine nature with which the Office of the Australian Information Commissioner has approached the consultation on the Code, particularly their engagement with children and young people. As with all regulation, we are unlikely to arrive at the perfect endpoint with our first attempt. But this is just the first step, and with a continued commitment to genuine consultation, we are confident that children's best interests will remain at the forefront of this important reform.

Summary of Recommendations

1. Children's rights as a guiding principle for the Children's Online Privacy Code

- *Establish the best interests of the child as the key guiding principle of the Children's Online Privacy Code.*

2. The scope and application of the Children's Online Privacy Code

- *Adopt a similar model to the United Kingdom and Ireland for determining when a service is likely to be accessed by children.*
- *Include EdTech services as an additional entity covered by the Children's Online Privacy Code.*

3. The collection and use of children's data

- *Include as a reasonable step a requirement that entities communicate privacy policies in child-friendly and age-appropriate formats, including information on how children can realise their privacy rights.*
- *Require that maximum privacy settings be switched on by default for children.*

4. Direct marketing towards children

- *Include a presumption against the collection and use of children's data for targeted advertising, unless in their best interests.*

5. Children correcting and reclaiming their data

- *Require that entities provide a remedy which allows children to have their data erased upon request.*

6. Implementation and enforcement of the Children's Online Privacy Code

- *Ensure adequate resourcing for the Office of the Australian Information Commissioner, commensurate to their expanded role in delivering, implementing and enforcing the Children's Online Privacy Code.*

Detailed Recommendations

1. Children's rights as a guiding principle for the Children's Online Privacy Code

The CRC is the most ratified treaty in the world and its forward-looking principles remain deeply relevant today including for the role that government and industry play in ensuring the best interests of children, a key child rights principle.ⁱⁱ UNICEF Australia believes the CRC's principles should be reflected in our online governance frameworks to ensure the respect, protection and fulfilment of all children's rights.

The best interests of the child is both a substantive child right and a dynamic principle, which always requires an assessment appropriate to the specific context of a child or children.ⁱⁱⁱ In considering the best interests of children we should 'have regard for all children's rights, including their rights to seek, receive and impart information, to be protected from harm and to have their views given due weight, and ensure transparency in the assessment of the best interests of the child and the criteria that have been applied.'^{iv}

The Committee on the Rights of the Child's General Comment 14^v provides an even more detailed examination of the best interests principle and how it should be applied in practice. For the tech industry, in practice this may mean making decisions in relation to children which seemingly clash with the interests of companies, such as not capturing and processing children's data in ways that are detrimental to them, for example, in persuasive design, behavioural advertising, and biometrics collection.^{vi} As an example, Meta has developed a [best interests of the child framework](#) to help apply the principle to their products and experiences.^{vii}

In both the development of the Children's Online Privacy Code and in its eventual implementation, children's rights should be a guiding principle, with regard always given to the best interests of the child. Given the intention of the Code is to place children at the centre of privacy protections in Australia, when decisions become complex and tough to make, or where the weighing of one set of priorities or demands over another truly tests us, then the best interests of the child should be the prevailing consideration.

Recommendation

Establish the best interests of the child as the key guiding principle of the Children's Online Privacy Code.

2. The scope and application of the Children's Online Privacy Code

Establishing the scope and entities covered by the Children's Online Privacy Code is a crucial first step. In this regard, services likely to be accessed by children is an important test, acknowledging that children will interact with both services designed for them (which should obviously be covered by the Code), and with services not designed for them.

We can look to international jurisdictions for guidance on how to best establish the "likely to be accessed" standard, including the UK's *Age Appropriate Design Code*^{viii} and the Irish *Fundamentals to a child-oriented approach to data processing*.^{ix} These models take an approach that cover services that are both intended for children, and those not intended for children but likely to be used by them.

Services targeting children should clearly be covered by the Code. Concerning services not targeted at children but likely to be used by them, guidance from these international jurisdictions says that likely to be used means a significant number of children using the service, although this doesn't necessarily mean a numerically large number of children. Rather, it just needs to be used by a non-trivial number of children, and that the privacy risks associated with their use should be considered as well.^x

If the intention of the Children's Online Privacy Code is to better protect children, then these emerging international norms from the UK and Ireland on services likely to be accessed by children are preferred. They allow for flexibility whilst helping to ensure maximum coverage of privacy protections for children. Aligning Australia with international jurisdictions should also help reduce the regulatory burden for platforms.

Recommendation (Question 2.1)

Adopt a similar model to the United Kingdom and Ireland for determining when a service is likely to be accessed by children.

With respect to entities covered by the Code, in addition to social media services, relevant electronic services, and designated internet services, EdTech services should also be included. For Australian children in 2025, education and technology have become synonymous with each other.

UNICEF research on COVID-19 school closures found that 90 per cent of education ministries worldwide used some form of EdTech to provide remote learning for an estimated 268 million children.^{xi} In Australia, the EdTech industry generates \$4.2 billion in revenue a year.^{xii}

Although it is crucial for learning in Australian schools, EdTech presents a variety of privacy risks for children and their parents. There can be a lack of understanding of what consenting to the significant data collection required involves, and where that data may end up, be it for advertising or some other means.^{xiii} And EdTech offered in schools may lack scrutiny or rigorous evaluation of the pedagogy that underlies it, with under-resourced schools often not in a position to insist on the contrary.^{xiv}

Given the pervasiveness of EdTech, the amount of Australian children it impacts, and the level of data collection involved, EdTech services should also be included as an entity covered by the Children's Online Privacy Code.

Recommendation (Question 1.1)

Include EdTech services as an additional entity covered by the Children's Online Privacy Code.

3. The collection and use of children's data

We know that Australian young people are often uncomfortable with how their data is collected and used, with a lack of informed consent and control of their data being a common theme. A helpful guiding principle of the CRC in this regard is the evolving capacities principle, which acknowledges that as children develop and grow, so to do their competencies, and in turn they need less direction and have an increased capacity to make decisions that affect their lives.^{xv}

Just as children grow and change, so to must our governance frameworks, to ensure they balance the need for legal certainty with the diverse and evolving capacities of children.^{xvi} One area where the Children's Online Privacy Code could address this is through the requirements of services with regard to communication about privacy policies.

Children are generally less able to understand the long-term implications of consenting to their data collection, often presented in notices and policies that even adults struggle to comprehend.^{xvii} UNICEF Australia's research found that only

23% of Aussie teens regularly read privacy policies.^{xviii} If collection notices and privacy policies were presented in child and age-appropriate formats, they would help children to be able to provide informed and freely given consent.^{xix}

Examples of more child-friendly privacy policies could include using images, videos, and plain-language wherever possible. The efforts of platforms like [LEGO](#) and [Microsoft](#) are illustrative here. Child-friendly communications about privacy policies should also include information (where relevant and appropriate) about children’s privacy rights, inquiry, complaint, appeal, and redress mechanisms, and links to support services when needed.

Recommendation (Question 4.1 and 4.4)

Include as a reasonable step a requirement that entities communicate privacy policies in child-friendly and age-appropriate formats, including information on how children can realise their privacy rights.

Another measure which can provide greater privacy protections for children is a requirement that maximum privacy settings be switched on by default for those under the age of 18. This would help alleviate some of the concerns that young people have about their data being collected and used – our research found that 85% of Aussie teens are uncomfortable with their data being used in ways they don’t know about.^{xx}

Requiring maximum privacy settings by default would help bring us into line with international norms, for example, with the UK’s *Age Appropriate Design Code*^{xxi} which requires high privacy by default unless there is a compelling reason not to.^{xxii} It would also help with harmonisation with other digital reforms in Australia, such as the development of the Online Safety Codes under the Online Safety Act, in which some codes have requirements for maximum privacy settings by default for children under the age of 16 but not 18.

The Children’s Online Privacy Code is the natural vehicle for requiring that entities enable the highest privacy settings by default for children in Australia. Children will always have the ability to then customise their settings as they see fit, but privacy-by-default should be our starting point.

Recommendation (Question 6.5 and 9.4)

Require that maximum privacy settings be switched on by default for children.

4. Direct marketing towards children

Young people in Australia express a great deal of distrust when it comes to their data being used for practices that aim to predict and capitalise on their digital behaviours. UNICEF Australia’s own research found that:

- 75% of teens are uncomfortable with companies creating profiles of them based on their data
- 66% of teens are uncomfortable with companies predicting their behaviours based on their data, and
- 51% of teens are uncomfortable with being shown targeted advertising based on their data.^{xxiii}

Due to both the level of data collection involved and the impacts of the use of that data, targeted advertising can violate the rights of children. Techniques designed to influence children’s behaviours carry risk given children’s cognitive capacities and critical thinking skills are still developing.^{xxiv} This use of data to influence, when done in harmful ways, affects children’s freedom and agency, and opaque algorithms and non-transparent nudge techniques may limit diversity of experiences and positive developmental opportunities.^{xxv}

Internationally, the emerging global norm is moving towards a presumption against targeted advertising for children. The UK and Ireland include a presumption against targeted advertising towards children in the *Age Appropriate Design Code*^{xxvi} and *Fundamentals to a child-oriented approach to data processing*^{xxvii} respectively. And even the tech industry has moved away from the practice, with Instagram, Facebook, YouTube and TikTok not using children’s data to deliver targeted advertising.^{xxviii}

In keeping with these international best-practice standards, and to better protect Australian children, the Children's Online Privacy Code should include a presumption against targeted advertising towards children, unless it can be justified as in their best interests.

Recommendation (Question 10.3)

Include a presumption against the collection and use of children's data for targeted advertising, unless in their best interests.

5. Children correcting and reclaiming their data

The vast majority of Australian teenagers – 72% of them – are uncomfortable with their data being collected by apps and websites, regardless of the purpose.^{xxix} The Children's Online Privacy Code presents an opportunity to flip that equation and give young people a greater semblance of control over their data.

One pathway towards this is a right to erasure or having their data deleted. This idea has been floated before. The UN Committee on the Rights of the Child's General Comment 25 says that children should have a right to delete their data when they think it is stored unnecessarily.^{xxx} It is also present in comparable international regulatory frameworks, including in the European Union's *General Data Protection Regulation*^{xxxi} and in the UK's *Age Appropriate Design Code*.^{xxxi} Similarly, a number of large tech platforms already allow users to request the deletion of their data including Instagram, Facebook,^{xxxiii} TikTok^{xxxiv} and Snapchat.^{xxxv}

Alongside the other measures floated in this submission, the inclusion of a right to erasure would help children and young people better exercise their privacy rights, ultimately ensuring the Children's Online Privacy Code provides greater protection for Australia's children.

Recommendation (Question 15.5)

Require that entities provide a remedy which allows children to have their data erased upon request.

6. Implementation and enforcement of the Children's Online Privacy Code

The Office of the Australian Information Commissioner (OAIC) should be commended for the approach they have taken in their consultation on the Children's Online Privacy Code, particularly their engagement with children and young people. Should the Code realise the ambitions that young people hope it will, it will represent a step-change in how children's data is governed in Australia.

Accordingly, this step-change (coupled with broader reforms to the Privacy Act) is likely to see an expansion of the responsibilities of the OAIC, whether that be in monitoring, compliance and enforcement, raising public awareness of our new data framework for children, or continuing to consult with a variety of stakeholders to ensure the Code is indeed achieving its intended aims. To that end, the OAIC should be properly resourced to perform this revamped role, if we hope to see the benefits of the Children's Online Privacy Code passed on to Australia's children.

Recommendation

Ensure adequate resourcing for the Office of the Australian Information Commissioner, commensurate to their expanded role in delivering, implementing and enforcing the Children's Online Privacy Code.

- ⁱ UNICEF Australia (2025), A Generation Online: Ensuring children and young people thrive in a digital world, [unicef.org.au/publications/a-generation-online](https://www.unicef.org/publications/a-generation-online)
- ⁱⁱ UNICEF (2021), *The Case for Better Governance of Children's Data: A Manifesto*, <https://www.unicef.org/globalinsight/reports/better-governance-childrens-data-manifesto>.
- ⁱⁱⁱ Committee on the Rights of the Child, *General comment No. 25 (2021) on children's rights in relation to the digital environment*, 86th sess, CRC/C/GC/25 (2 March 2021).
- ^{iv} Committee on the Rights of the Child, *General comment No. 25 (2021) on children's rights in relation to the digital environment*, 86th sess, CRC/C/GC/25 (2 March 2021).
- ^v Committee on the Rights of the Child, *General comment No. 14 (2013) on the right of the child to have his or her best interests taken as a primary consideration (art. 3, para. 1)*, 62nd sess, CRC/C/GC/14 (29 May 2013).
- ^{vi} UNICEF (2021), *The Case for Better Governance of Children's Data: A Manifesto*, <https://www.unicef.org/globalinsight/reports/better-governance-childrens-data-manifesto>
- ^{vii} Elaine Montgomery and Elaina Koros (2022), *Meta's Best Interests of the Child Framework*, <https://www.ttclabs.net/news/metas-best-interests-of-the-child-framework>
- ^{viii} UK Information Commissioner's Office *Age Appropriate Design Code 2020* <https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/age-appropriate-design-a-code-of-practice-for-online-services/>
- ^{ix} Ireland, Data Protection Commission 2021 *FundamentatIs for a Child Oriented Approach to Data Protection* https://www.dataprotection.ie/sites/default/files/uploads/2021-12/Fundamentals%20for%20a%20Child-Oriented%20Approach%20to%20Data%20Processing_FINAL_EN.pdf
- ^x TaylorWessing 2024 *Likely to be accessed* <https://www.taylorwessing.com/en/global-data-hub/2024/february---childrens-data/likely-to-be-accessed-by-children>
- ^{xi} United Nations Children's Fund and International Telecommunication Union, "How many children and young people have internet access at home? Estimating digital connectivity during the COVID-19 pandemic." UNICEF, New York, 2020.
- ^{xii} EduGrowth (2025), *Help us map the Australian EdTech Ecosystem*, <https://edugrowth.org.au/2025/05/09/help-us-map-the-australian-edtech-sector/>
- ^{xiii} UNICEF (2021), *The Case for Better Governance of Children's Data: A Manifesto*, <https://www.unicef.org/globalinsight/reports/better-governance-childrens-data-manifesto>
- ^{xiv} UNICEF (2021), *The Case for Better Governance of Children's Data: A Manifesto*, <https://www.unicef.org/globalinsight/reports/better-governance-childrens-data-manifesto>
- ^{xv} UNICEF (2021), *The Case for Better Governance of Children's Data: A Manifesto*, <https://www.unicef.org/globalinsight/reports/better-governance-childrens-data-manifesto>
- ^{xvi} UNICEF (2021), *The Case for Better Governance of Children's Data: A Manifesto*, <https://www.unicef.org/globalinsight/reports/better-governance-childrens-data-manifesto>
- ^{xvii} UNICEF (2021), *The Case for Better Governance of Children's Data: A Manifesto*, <https://www.unicef.org/globalinsight/media/1771/file/UNICEF%20Global%20Insight%20Data%20Governance%20Summary.pdf>
- ^{xviii} UNICEF Australia (2025), A Generation Online: Ensuring children and young people thrive in a digital world, [unicef.org.au/publications/a-generation-online](https://www.unicef.org/publications/a-generation-online)
- ^{xix} Committee on the Rights of the Child, *General comment No. 25 (2021) on children's rights in relation to the digital environment*, 86th sess, CRC/C/GC/25 (2 March 2021)
- ^{xx} UNICEF Australia (2025), A Generation Online: Ensuring children and young people thrive in a digital world, [unicef.org.au/publications/a-generation-online](https://www.unicef.org/publications/a-generation-online)
- ^{xxi} UK Information Commissioner's Office *Age Appropriate Design Code 2020* <https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/age-appropriate-design-a-code-of-practice-for-online-services/>
- ^{xxii} UK Information Commissioner's Office *Age Appropriate Design Code 2020* <https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/age-appropriate-design-a-code-of-practice-for-online-services/>
- ^{xxiii} UNICEF Australia (2025), A Generation Online: Ensuring children and young people thrive in a digital world, [unicef.org.au/publications/a-generation-online](https://www.unicef.org/publications/a-generation-online)
- ^{xxiv} UNICEF (2021), *The Case for Better Governance of Children's Data: A Manifesto*, <https://www.unicef.org/globalinsight/reports/better-governance-childrens-data-manifesto>
- ^{xxv} UNICEF (2021), *The Case for Better Governance of Children's Data: A Manifesto*, <https://www.unicef.org/globalinsight/reports/better-governance-childrens-data-manifesto>
- ^{xxvi} UK Information Commissioner's Office *Age Appropriate Design Code 2020* <https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/age-appropriate-design-a-code-of-practice-for-online-services/>
- ^{xxvii} Ireland, Data Protection Commission 2021 *FundamentatIs for a Child Oriented Approach to Data Protection* https://www.dataprotection.ie/sites/default/files/uploads/2021-12/Fundamentals%20for%20a%20Child-Oriented%20Approach%20to%20Data%20Processing_FINAL_EN.pdf
- ^{xxviii} Who turned off the ability for advertisers to target children, and the use of 'online engagement' to drive their advertising algorithm in January 2023. See Meta 2023 *Continuing to Create Age-Appropriate Ad Experiences for Teens* <https://about.fb.com/news/2023/01/age-appropriate-ads-for-teens/> ; Google 2025 *Ad-serving protections for teens* <https://support.google.com/adspolicy/answer/12205906?hl=en> ; TikTok 2025 *Protecting minors on TikTok: advertising initiatives*, <https://ads.tiktok.com/help/article/protecting-minors-on-tiktok-advertising-initiatives>
- ^{xxix} UNICEF Australia (2025), A Generation Online: Ensuring children and young people thrive in a digital world, [unicef.org.au/publications/a-generation-online](https://www.unicef.org/publications/a-generation-online)
- ^{xxx} Committee on the Rights of the Child, *General comment No. 25 (2021) on children's rights in relation to the digital environment*, 86th sess, CRC/C/GC/25 (2 March 2021).
- ^{xxxi} Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
- ^{xxxii} UK Information Commissioner's Office *Age Appropriate Design Code 2020* <https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/age-appropriate-design-a-code-of-practice-for-online-services/>
- ^{xxxiii} Meta 2025 *Delete your Information or Account* <https://www.facebook.com/privacy/policy/>
- ^{xxxiv} TikTok 2025 *Can a User Request to Have their Data Removed?* <https://usds.tiktok.com/can-a-user-request-to-have-their-data-removed-and-deleted-from-tiktok>
- ^{xxxv} Snapchat 2025 *How do I Clear my Data on Snapchat?* <https://help.snapchat.com/hc/en-us/articles/12324650978964-How-do-I-clear-my-data-on-Snapchat>