Microsoft submission to OAIC's Children's Online Privacy Code

Microsoft appreciates the opportunity to provide a submission on the Office of the Australian Information Commissioner's (**OAIC**) development of a Children's Online Privacy Code (the **Code**) under the *Privacy and Other Legislation Amendment Act 2024* (the **Act**).

We believe that privacy is a fundamental human right and that strong data privacy laws are vital for safeguarding it. We agree that children may face unique privacy and safety risks online and welcome the development of the Code, building on effective international regulatory models such as the UK Information Commissioner's Office's Age-Appropriate Design Code (**UK AADC**).

1. Scope of services covered by the Code

As the Issues Paper notes, the Code will apply to APP entities that provide a *social media service*, *relevant electronic service*, or *designated internet service* that is 'likely to be accessed by' children. As these categories of services potentially cover a wide range of online services – spanning social media, messaging apps, websites and cloud storage services[1] – it is important that the OAIC has discretion to clarify which classes of APP entities are inside and outside scope of the Code.

In light of the diversity of online services, we urge the OAIC to take **a risk-based and proportionate approach that is tailored to the unique nature of each service** in exercising its discretion on what it means for a service to be 'likely to be accessed by children'. The UK AADC sets out an example of effective criteria, assessing whether a service is within scope by considering (1) whether the content and design of a service is likely to appeal to children; and (2) any measures in place to restrict or discourage children's access.[2]

With the benefit of the insights from children and young people that have informed the OAIC's consultation so far, we consider that some potential categories of higher risk services that may be considered within scope of the Code might include online services aimed at enabling or facilitating social interaction with children; driving engagement via algorithmic recommendations of content likely to appeal to children, and enabling the creation and sharing of user generated content likely to appeal to children. These classes of services, when designed to appeal to users that include children, carry higher privacy risks to children as expressed in the OAIC's initial consultation, including greater privacy risks relating to oversharing of personal information, profiling, or targeted advertising.

We therefore recommend the OAIC specifies **enterprise services, cloud storage services, and professional networking or professional collaboration services as outside the scope of the Code**. These classes include services like productivity tools, business software, and workplace collaboration

[1] OAIC, Children's Online Privacy Code Issues Paper, 12 June 2025 ('*Issues Paper*'), p3.
[2] UK AADC, Annex A: Services covered by the code flowchart.

services which are typically used in a professional setting by adults. These services carry low risks of privacy harms to children, as they are not designed to appeal to children and often involve additional measures to restrict children's access.

2. Age assurance and identifying child users

A related issue to the scope of the code is how child users should be identified. On this issue, we recommend that the Code allows entities enough flexibility to apply a range of potential measures to identify child users, which should take into account the level of risk arising from the data processed by that service and whether users are authenticated via logging-in to a service.

In particular, we recommend that the obligations of the Code should only apply **when the entity 'knows, or wilfully disregards' that a user is a child**. This involves well-established standards of actual knowledge with imputed knowledge (i.e. where an entity purposely ignores the fact that an individual is a child). Applying such clear and objective knowledge standards avoids requiring entities to infer a user's age, which can inadvertently create contradictory and privacy-invasive obligations for entities to monitor the data of all users for the purposes of age estimation and may also conflict with privacy laws in overseas jurisdictions such as in the US.

Microsoft recognises that there are some contexts in which age assurance methods can play an important role in helping to identify child users. However, over-reliance on age assurance can raise competing considerations, including privacy, security, equity and freedom of expression. As such, we recommend that the **implementation of any age assurance measures should be privacy-protective** and include rules around data minimisation and building systems under the principles of privacy by design to minimise the amount of data-sharing with third parties. Any age assurance guidance could also be developed to support harmonisation with emerging international best practices, such as Ofcom's guidance on Highly Effective Age Assurance for the purposes of the UK's Online Safety Act.

Finally, we note that the eSafety Commissioner's office is currently working with industry on guidance around the 'reasonable steps' required to implement social media age restrictions in Australia.[3] We note that 'age-restricted social media platform' for the purposes of the social media minimum age restrictions is defined slightly more widely than 'social media service' for the purposes of the Code.[4] As such, it would increase clarity for industry if the Code includes, at a minimum, the same classes of exemptions as are applied in the social media minimum age restriction rules. Given the overlapping nature of these two regimes, it is also important for any age assurance requirements under the Code

[3] eSafety Commissioner's Office, Social media age restrictions.
[4] See sections 13 ('social media service') and 63C ('age-restricted social media service') under the *Online Safety Act 2021* (Cth).

to be coordinated with the expectations of the eSafety Commissioner's office. Joint guidance from the OAIC and eSafety on this issue would be invaluable in increasing regulatory clarity and consistency.

3. Age range-specific guidance

We welcome the OAIC's consideration of the different needs of different age ranges to ensure that children of all ages are appropriately protected. In general, we support the UK AADC's approach to setting out a **flexible standard that allows entities to consider the various age and developmental stages of their users** when designing their online services and to identify and mitigate potential risks.

For age-specific requirements to be effective and scalable, it is important that entities have the flexibility to decide how best to take into account various ages and developmental capacities of their users by allowing entities the space to design their products and services in accordance to the groups of users most likely to access the service.

For some services with logged-in users, it may be appropriate to differentiate between two broader categories of age ranges: young children under 13 and teens between 13-17:

- **Young children under 13** should receive the strictest privacy protections as well as robust parental controls. This reflects the reality that young children generally cannot meaningfully consent or manage complex privacy choices. As a result, services should generally default to collecting minimal personal data from under-13 users and parents or guardians should be empowered to supervise and control young children's accounts, including their privacy settings.
- **Teens between 13-17** have a greater understanding of online services and may wish to have greater autonomy and control over their privacy settings. For example, a recent UNICEF Australia survey found that 86% of Australian teens between 13-17 take steps to protect their online privacy.[5] Appropriate protections for this group should continue to focus on transparency and privacy by default, but with additional controls that can allow teens to safely choose to share more information on a social profile or to opt-in to receive personalised content recommendations. Importantly, we believe that teens between 13-17 should make their own decisions about what personal information to share. This helps avoid overburdening parents with consent notifications and is in line with global norms.

These broader age bands would align with data protection requirements overseas, including in the US, as well as with the age ranges used in other regulations, such as the National Classification Scheme covering publications, films, and computer games in Australia.

[5] UNICEF Australia, Press Release, 5 March 2025.

4. Microsoft's approach to children's privacy and safety

We welcome the OAIC's objective focused on strengthening privacy protections for the handling of children's personal information while continuing to encourage children to engage in the digital world.[6] Microsoft has long recognised our responsibility to support safe online experiences for all our users, including children. This is reflected in our robust policies and settings on child accounts that enhance the privacy and safety of young people, which include:

1. **Data minimisation**: Microsoft implements strict data minimisation policies for child accounts to collect only the minimum data required to be provided for the product or service.
2. **No personalised ads**: Microsoft does not serve targeted ads to t children under 18 based on their age.
3. **Preventing unwanted contact**: Microsoft products include a range of features to minimise unwanted communications from strangers, including privacy by default settings.
4. **AI training:** Microsoft does not train AI models on the personal data of children under 18.
5. **Comprehensive parent/guardian oversight**: Microsoft gives parents and guardians tools like the Microsoft Family Safety dashboard and Xbox Family Settings app to oversee and adjust their child's privacy settings, including the ability to view and delete a child's data.

Some specific examples of how these policies and settings apply across our diverse services are set out below:

- **Xbox** and **Microsoft 365 apps** including Office and Teams do not collect any additional data from the accounts of children under 13 beyond what is necessary to provide these services.[7] Xbox accounts use different presets for 'child', 'teen', or adult'. 'Child' accounts have the most restrictive presets where the child's profile details are hidden from the public and many social features are turned off by default.[8]
- **Minecraft Education** contains our age-appropriate education material to empower young people online. The Cyber Safe curriculum is aimed at children ages 7-11 and focuses on teaching kids the fundamentals of privacy, cybersecurity, digital civility, and new technologies like cloud computing. Our Cyber Fundamentals, aimed at children ages 10-14, explores cybersecurity concepts including malware, encryption, and network components with a focus on making cybersecurity tangible.[9]

---

[6] Issues Paper, p6.
[7] See Privacy for young people and Xbox data collection for kids.
[8] See Xbox Privacy & You.
[9] See Empowering the next generation of cyber heroes with new classroom-to-career Minecraft curriculum.

- **LinkedIn** does not permit children under 16 to join the platform.[10] For teen members aged 16-17, LinkedIn implements protections by default, such as excluding members under 18 from age-based ad targeting.[11]

Microsoft has a long-standing commitment to child safety and privacy and we support the introduction of a Children's Online Privacy Code in Australia. In particular, we support approaches to protecting children's privacy and safety that are consistent and interoperable with global standards, which avoids creating a fractured experience for users across different jurisdictions and may result in confusion for children and parents alike. We therefore encourage Governments and regulators worldwide to leverage existing models such as the UK AADC as much as is appropriate in Australia.

We appreciate the OAIC's consideration of our views in this consultation process and look forward to remaining engaged throughout the development process.

[10] See FAQs for age-based protections on LinkedIn.
[11] See Increasing Your Privacy as a Teen on LinkedIn.