Microsoft submission to the OAIC's Exposure Draft of the Children's Online Privacy Code

Introduction

Microsoft appreciates the opportunity to respond to the exposure draft of the *Privacy (Children's Online Privacy) Code 2026* (**the Draft Code**) released by the Office of the Australian Information Commissioner (**OAIC**) on 31 March 2026. We provided a submission to the OAIC's Issues Paper in July 2025 and welcome this further opportunity to engage as the Code moves towards registration.

Microsoft believes privacy is a fundamental human right and that strong, internationally interoperable data protection laws are vital to safeguarding it. We share the Government's objective of strengthening privacy protections for children online and we support the OAIC's effort to harmonise with overseas regimes, such as the UK Information Commissioner's Office's Age Appropriate Design Code (**UK AADC**).

We also commend the OAIC on the range of child- and teen-friendly public education materials developed to support this consultation. These resources are clear, accessible, and age-appropriate, and a valuable model for engaging young people on privacy issues.

This submission focuses on areas where further clarification or refinement would support consistent and practical implementation of the Draft Code, as set out in our summary of recommendations below.

Summary of Microsoft recommendations:

1. Clarify that the Code's obligations generally do not apply to enterprise, cloud, and professional services that pose low privacy risks to children and are not directed at them.
2. Clarify that, in educational contexts, Code obligations apply to the educational institution as the controller, rather than the technology provider as the processor.
3. Provide additional joint guidance from the OAIC and eSafety on age assurance setting out risk-proportionate, principles-based standards.
4. Specify a clear knowledge standard so that Code obligations apply where an entity "knows, or wilfully disregards" that a user is a child.
5. Clarify alignment with the Social Media Minimum Age (**SMMA**) and the *Online Safety Act 2021* (Cth) regulatory frameworks, including that compliance with one regime may demonstrate compliance with the other.
6. Provide guidance to clarify the "strictly necessary" standard, including illustrative examples and confirmation that it accommodates legitimate purposes such as safety, security, and service improvement.
7. Adopt a more flexible approach to consent by avoiding fixed annual consent expiry requirements and instead focusing on supporting meaningful engagement.
8. Reframe child assent requirements as requirements to deliver age-appropriate notices.

9. Provide principles and guidance on child-friendly notices, including allowing a layered approach that balances clarity, usability, and legal accuracy.
10. Replace the requirement for a public Privacy Impact Assessment register with an obligation to maintain an internal register accessible to the OAIC on request.
11. Introduce a limited cybersecurity and fraud prevention exception to the right to destruction.
12. Clarify that additional opt-out controls are not required where no targeted advertising is directed to children.
13. Provide guidance that enables flexible, outcomes-focused training approaches, allowing organisations to integrate children's privacy into broader training programs.

1. Scope of services covered by the Code

1.1 Application of obligations to enterprise, cloud and professional services that pose low risk to children

Section 5 of the Draft Code adopts the broad statutory categories of social media services (**SMS**), relevant electronic services (**RES**) and designated internet services (**DIS**) under the Online Safety Act. As previously noted, those categories are exceptionally wide and include enterprise productivity, cloud-storage, developer, and professional networking and collaboration services that are designed for, and overwhelmingly used by, working adults in a workplace setting.

The current 'likely to be accessed by children' threshold provides only limited assistance to providers of these services. As the Explanatory Statement makes clear, this threshold turns on a fact-specific analysis which must be documented service-by-service. For global providers operating diverse product portfolios — including Microsoft 365, Microsoft Teams, GitHub, LinkedIn, and Azure — this creates substantial legal uncertainty about which products fall inside or outside the Code, despite none of these products being designed to appeal to children.

Applying child-specific obligations such as those outlined in the Code (e.g. in relation to age assurance, "strictly necessary" limitations, parental consent gates, and annual re-consent) to enterprise services would impose significant cost on Australian businesses, organisations, and educational institutions that procure enterprise services under their own privacy and security governance frameworks. It may also create significant friction for legitimate workplace and educational use of enterprise software by older teens and shift effort away from the online consumer services where children are directly engaging with the digital environment as end-users and pose potentially greater privacy risks.

The Government and the OAIC's objectives for the Code involve targeting services that "expose children and young people to the highest privacy risks" such as, for example, child-directed social media, content-recommendation, and educational services. As enterprise productivity tools, business software, and developer platforms do not fit that profile, **we recommend the OAIC consider amending the Draft Code or publishing guidance to clarify that the Code's obligations generally do not apply to professional and enterprise services outside education contexts** (as further discussed below).

This would reflect the sub-categories of enterprise RES and enterprise DIS as defined under the Online Safety Codes (Unlawful Material Standards and Age Restricted Material Codes). This consistent distinction reflects the lower risk profile of an enterprise level services as well as the fact that the enterprise provider is not a data controller, nor does it manage the relationship with end-users of a service. This approach would reflect a risk-based and proportionate approach by reserving the Code's most prescriptive obligations for services that genuinely present the privacy risks the Code is designed

to address. It would also mirror the policy design under the UK AADC, which similarly generally does not apply to professional and enterprise services not directed at children.

1.2 Application to enterprise services provided to educational institutions

Section 7 of the Draft Code applies the Code to services that are both 'likely to be accessed by children' and 'primarily concerned with the activities of children'. We understand from the OAIC that the second limb is intended to capture services provided in an educational context.

While we are supportive of the OAIC's objective of raising privacy protections within educational institutions, we note that services provided in educational contexts (e.g. Microsoft 365 Education and Minecraft Education) are:

- procured by educational institutions under a contract that designates the institution as the controller of personal information
- configured and administered by school IT and by teachers, with granular tenant-level privacy controls and minimal visibility or control from Microsoft
- subject to the institution's own privacy and child-safeguarding governance
- already designed to a child-safe specification, with consumer features (advertising, social discovery, etc.) disabled.

We therefore recommend the OAIC clarify that any Code obligations applicable to enterprise services in an educational context apply to the educational institution procuring the service as the controller of how personal information is collected, used and disclosed. Code obligations should not fall on the technology provider who has minimal oversight or control over the educational institution's data practices. Similarly, the OAIC should clarify that self-directed or incidental use of services by students outside formal institutional settings does not, by itself, mean that a service is "primarily concerned with the activities of children."

2. Age Assurance

2.1 Request for further guidance and alignment with online safety regime

We support the OAIC's effort to align the Code with the eSafety Commissioner's developing approach under the SMMA and the recognition in section 8 that 'reasonable steps' will vary by risk profile and service type.

As the OAIC is aware, different services pose very different risks to children, and age assurance methods carry different privacy and accessibility trade-offs. For services with lower privacy risk for children, methods such as age-estimation, self-declaration with safeguards, or, where children or younger teens are able to use a service, family safety setting controls may achieve the policy objective at a lower cost to user privacy and accessibility.

We would welcome additional OAIC guidance on the age assurance requirements under the Code and recommend that the OAIC adopt commercially reasonable standards for age assurance with the following **three refinements**:

14. **Maintain a risk-proportionate, principles-based standard**. The 'reasonable steps' formulation should be retained and supplemented with clear factors in guidance — including data sensitivity, volume of children likely to access the service, and the existence of alternative age-appropriate controls such as default guardrails for minor accounts, contractually-restricted enterprise environments, or, where appropriate, family settings. The Code should not prescribe specific age-verification technologies, which evolve rapidly and carry their own privacy, security, equity and

accessibility trade-offs but rather preserve flexibility for providers to implement the most appropriate measures based on their service type.

15. **Specify a clear knowledge standard for triggering Code obligations**. As we have previously submitted, we recommend that the Code's substantive obligations apply where an entity 'knows, or wilfully disregards' that a user is a child. This well-established standard that avoids creating contradictory incentives for entities to monitor all users' data for age-estimation purposes and limits conflict with privacy laws in other jurisdictions (including the US) that restrict age-related profiling.
16. **Harmonise with the SMMA framework and joint OAIC/eSafety guidance**. As many providers may be regulated under both the SMMA framework and the Code, we recommend the Code clarify that compliance with one regime's age-assurance standard is generally evidence of compliance with the other to reduce duplication and consumer friction and to align the two regulatory frameworks. We also urge the OAIC and eSafety to publish joint guidance to give industry a single, consistent compliance roadmap.

3. The "strictly necessary" standard

3.1 OAIC guidance needed to clarify 'strictly necessary' standard

Section 9 of the Draft Code requires that an entity only collects, uses or discloses personal information about a child by default if it is ***strictly necessary*** to provide the entity's service. Despite being 'narrower and more protective' than 'reasonably necessary',[1] a 'strictly necessary' standard may still create significant uncertainty around purposes including:

- product improvement and bug-fixing — including diagnostics, error reporting, and improving the quality and reliability of features children use;
- user-experience research and design improvement, including aggregated and de-identified analytics directed at improving the safety, accessibility, and usability of features for children;
- safety, integrity, and trust-and-safety operations, including detection and response to harmful content, grooming, harassment, and content that violates platform rules;
- security, including fraud and abuse prevention, account-takeover detection, and protection of the service and other users from misuse; and
- legal and regulatory compliance, including responding to lawful requests and enforcing terms of service.

Under a narrow and literal interpretation of a 'strictly necessary' standard, construed as permitting only data uses without which the service cannot technically function, might prevent providers from data uses that improve outcomes for children without seeking separate consents, such as making products safer, more accessible, and more reliable and secure.

To avoid unintended outcomes and to provide industry with greater clarity and assist with implementation, **we recommend the OAIC publish guidance, ideally with a non-exhaustive list of examples including the purposes listed above**. It would also be helpful for the OAIC to clarify in the Draft Code or explanatory materials that the 'strictly necessary' standard includes the permitted general situations under section 16A of the Australian Privacy Principles.

[1] Children's Online Privacy Code, Draft Explanatory Statement, p8.

4. Managing consent and assent requirements

4.1 Managing consent burden

Section 15(4) of the Draft Code introduces a requirement that express consent must expire within 12 months of being given. While we support the principle that consent provided 'in particular circumstances cannot be assumed to endure indefinitely',[2] we are concerned that a fixed annual expiry period may create unintended practical challenges.

In particular, requiring parents to renew consent each year for every child and for each online service used risks imposing a significant and ongoing administrative burden on families. This approach is likely to result in consent fatigue among parents, reducing the likelihood that consent requests are meaningfully considered and engaged with over time. Rather than strengthening protections, an overly-frequent consent requirement could undermine the quality and effectiveness of the consent process.

As an alternative, **we recommend a more flexible approach to consents that prioritises meaningful engagement**. This could include periodic reminders to parents about existing consents, combined with renewed express consent at key transition points, such as when a child reaches an age where decision-making responsibility shifts to the teenager (e.g. at age 15) and again at adulthood. This approach would better balance user protection with practical usability, while supporting more informed and considered consent.

4.2 Practical difficulties of obtaining child assent

Section 20 of the Draft Code requires an entity to obtain 'assent' from children under 15 years in certain circumstances. We are supportive of involving children in decisions around the use of their personal information and agree with the underlying policy objective of increasing transparency, digital literacy and a level of autonomy for the child.[3]

However, requiring *active assent* from children under 15, which encompasses a large range of developmental stages, can be challenging in practice. This is especially true for children at the younger end of the range. In addition, requiring both active assent form the child *and* legal consent from a verified parent creates a confusing and burdensome framework for families, creating risks of bottlenecking sign-up flows that could inadvertently discourage families from using child-safe products and towards less safe alternatives.

To improve clarity to both providers and families, **we recommend reframing the child assent requirement as an obligation to provide an age-appropriate notice to the child**. That is, providers should be required to provide a notice designed to be understood by a child of the relevant age band that can support their digital literacy and awareness of online privacy as they grow.

5. Refinements to transparency requirements

5.1 Reconciling child-friendly notice requirements

Microsoft supports the principle that information provided to children should be clear, accessible, and age-appropriate, and has invested significantly in developing child-friendly privacy materials across its online services, and is actively engaging with young people to ensure these are fit for purpose.

---

[2] Children's Online Privacy Code, Draft Explanatory Statement, p14.
[3] Children's Online Privacy Code, Draft Explanatory Statement, p15.

However, the detailed disclosure requirements set out in Division 3 of the Draft Code may be difficult to reconcile with the concurrent obligation that privacy notices 'must not include complex or technical expressions, terminology drawn from specialist industry or legal language.'[4] In practice, it can be challenging to provide clear and accurate explanations of matters such as data subject rights or cross-border disclosures without relying to some extent on legal or technical terminology, particularly where precision is required.

To support effective and consistent implementation across industry, **Microsoft recommends that the OAIC provide principles for how code participants can help children understand privacy and data issues, including illustrative examples. Additionally, we suggest that child-friendly language requirements be limited to outward-facing notices and consent flows directed at children**. This approach would allow organisations to adopt a layered framework, combining simplified, accessible summaries with more detailed explanations where appropriate, including in circumstances where legal consent must be obtained from a parent or guardian. Such an approach would better balance the objectives of clarity, usability, and legal accuracy.

5.2 Privacy Impact Assessments register

Microsoft recognises the value of Privacy Impact Assessments (**PIAs**) as a critical internal accountability and design mechanism. However, we are concerned that the requirement in section 39(2) of the Draft Code to maintain a publicly accessible register of PIAs would impose disproportionate and ongoing compliance costs, especially for providers of a large range of products such as Microsoft which often have hundreds of PIAs. Given the technical and context-specific nature of PIAs as well as the broad range of existing transparency tools and obligations, it is unlikely that the proposed public register will result in corresponding benefits of greater transparency or public understanding,

Further, the introduction of a public register may create unintended incentives for organisations to limit the number or scope of PIAs conducted, in order to manage reputational and compliance risks, thereby undermining the objective of promoting robust privacy-by-design practices for children. To address these concerns, **Microsoft recommends that the requirement for a public register be replaced with an obligation to maintain an internal register of PIAs, to be made available promptly to the Privacy Commissioner on request**, together with relevant PIAs where appropriate. This approach would better support regulatory oversight while preserving the integrity and effectiveness of PIAs as an internal governance tool.

5. Additional matters

Finally, several additional clarifications and refinements that would assist entities to implement the obligations of the Draft Code include:

1. **A clear cybersecurity exception to the right to destruction**: While we are supportive of measures to strengthen user control over children's personal data, **we recommend that a limited exception for cybersecurity and fraud prevention to the right to destruction in section 32 of the Draft Code**. Specific and limited categories of personal data (such as IP addresses, device identifiers, account action logs, and fraud detection signals) can be critical for entities to detect and respond to harmful activity. This is particularly important in shared or collaborative environments where such data is necessary to protect both individual users and the broader ecosystem. Without such an exception, an unqualified right to destruction may unintentionally constrain the ability of online

[4] See, e.g., Draft Code section 23(5) and 26(4).

services to maintain safe and secure environments and undermine important safeguards to protect children and other users online.

2. **Opt-out controls not required if no advertising is targeted to children**: As most of Microsoft's services do not deliver targeted advertising to children, **we recommend the OAIC clarify in guidance that any entities who do not deliver targeted advertising to children at all are not required to implement additional opt-out controls** under section 29 of the Draft Code. This clarification would harmonise with other jurisdictions where targeted advertising to minors is now prohibited outright (e.g. under the EU's Digital Services Act, Article 28(2) and several U.S. state laws).
3. **Greater flexibility in training requirements**: Microsoft supports the objective of ensuring that personnel handling children's personal information are appropriately trained, as required under section 40 of the Draft Code. **We would welcome the OAIC's guidance on how to deliver and maintain the required training using a flexible, outcomes-focused approach** to support effective implementation without imposing unnecessary duplication or administrative burden. In particular, organisations should have discretion to incorporate training on children's privacy into broader, risk-based privacy, security, or compliance training programs, rather than being required to deliver standalone modules in all cases. This would allow entities to tailor training to reflect organisational roles, risk profiles, and existing governance frameworks, while still ensuring staff are adequately equipped to protect children's personal information.

Conclusion

Microsoft strongly supports the OAIC's objective of strengthening privacy protections for children in Australia. We appreciate the opportunity to share our perspectives on the Draft Code and thank the OAIC for its continued engagement with industry over a series of roundtables during the consultation period.

Microsoft is committed to working constructively with the OAIC to support the development of a Code that is clear, effective, and proportionate in its application. We would welcome ongoing engagement as the Code is refined and implemented and we are available to provide further detail on any of the points raised in this submission.