X Corp.

865 FM 1209, Building 2
Bastrop, TX 78602

Private & Confidential 5 June 2026

The Office of the Australian Information Commissioner ("**OIAC**")
GPO Box 5218
Sydney NSW 2001

By email: copc@oaic.gov.au

Dear Sirs / Madams,

Submission on the Exposure Draft of the Privacy (Children's Online Privacy) Code 2026

X Corp. ("**X**") welcomes the opportunity to provide feedback on the Exposure Draft of the Privacy (Children's Online Privacy) Code 2026 (the "**Code**").

X is deeply committed to user safety and responsible data practices, and we recognize the role that proportionate and risk-based regulation can play in ensuring that users - particularly children - have safe experiences online. We strongly support the goal of strengthening privacy protections for children and young people online through measures which are evidence-based and concordant with Australia's broader regulatory framework - all whilst enabling their safe and beneficial participation in digital spaces.

Overall, while we acknowledge efforts to align the Code with international practice and existing regulatory frameworks in Australia, we remain concerned about the proposals to layer the Code on top of an already complex and duplicative regulatory environment.

In the spirit of constructive engagement, we offer the following comments on the Code.

I. Proportionality and the absence of thresholds or tiered obligations

X, as a platform, is not widely used by minors, currently has no lines of business that actively target minors, and does not allow advertisers to target minors. Additionally, in compliance with existing Australian law, X:

(a) maintains a social media minimum age of 16 and offboards accounts which do not meet this requirement[1];
(b) applies additional protective defaults and restrictions for known minors permitted on the platform so as to ensure a safer experience for them[2]; and
(c) deploys multi-layered and privacy-preserving age assurance measures[3].

[1] https://help.x.com/en/rules-and-policies/australia-resources
[2] https://help.x.com/en/rules-and-policies/information-for-parents-and-minor-users
[3] https://help.x.com/en/privacy

As a foundational point, the Code is predicated on the concept of a service being "*likely to be accessed by children*"[4] (or "*primarily concerned with the activities of children*"). However, there is currently no clear definition or detailed guidance on how "*likely to be accessed by children*" should be interpreted or assessed. Without clear criteria or guidance on how this threshold is to be interpreted and applied, regulated entities face material uncertainty as to whether the Code applies to their services, and risk inconsistent or overly broad application of the Code's obligations.

Once a service is considered to meet the "*likely to be accessed by children*" threshold, the Code applies a uniform set of prescription obligations, without any meaningful differentiation based on platform size, user demographics, or risk profile. The only size-related relief currently available is the small business exemption under the Privacy Act, which uses an annual turnover threshold of AUD $3 million that is too low to provide any practical relief to most platforms.

A strict, uniform application of the Code will therefore disproportionately impact mid-sized and smaller platforms.

To address these concerns, X Corp. recommends that the Code incorporate proportionality thresholds or tiered obligations, and clear guidance on the meaning and application of "*likely to be accessed by children",* consistent with the risk-based approach already reflected in the Code[5].

II. Regulatory coherence and the risks of a fragmented regime

X Corp. supports the shared objective of the Australian Government of protecting children online. We note that there are some efforts to align the Code with instruments other than the Privacy Act 1988 ("**Privacy Act**") and Australian Privacy Principles ("**APPs**"): for example, the adoption of definitions under the Australian Online Safety Act 2021 ("**Online Safety Act**") with respect to "*designated internet service", "relevant electronic service",* and "*social media service"*; as well as the obligation to take "*reasonable steps*" to implement age assurance in a way which is privacy protective and minimises data. These are all welcomed.

However, in addition to the Code, Privacy Act, and APPs, there is a complex patchwork of intersecting regulatory instruments (both existing and contemplated) which touch on data privacy issues, including:

(a) OAIC guidance on age assurance technologies, children's data, and privacy-by-design (including the Privacy for Kids hub and specific SMMA guidance);
(b) the Social Media Minimum Age provisions (under Part 4A of the Online Safety Act 2021), which include dedicated privacy safeguards (s63F) that strictly limit the use of age-related personal information;
(c) eSafety Industry Codes and Standards, which impose age assurance requirements and mandate privacy law compliance and data minimisation for certain services;
(d) the proposed overarching Digital Duty of Care under the Online Safety Act (which explicitly requires coherence with privacy law reforms);
(e) the Consumer Data Right scheme and its ongoing expansions and assessments;
(f) the Scams Prevention Framework (which includes data sharing and privacy obligations);

[4] Section 5 / 7 of the Code
[5] For example, at Section 8 of the Code pertaining to age assurance

(g) the Safe and Responsible AI consultation and principles (data and privacy implications);
(h) the Digital Platform Regulators Forum working papers on algorithms, AI, and privacy;
(i) OAIC enforcement priorities and guidance on children's data, facial recognition, and platform obligations; and
(j) the Anti-Money Laundering and Counter-Terrorism Financing Act reforms.

The risk of conflicting obligations is therefore very high.

Furthermore, X observes that the proposed framework creates multiple conflicting age thresholds across different regulatory instruments, namely:

(a) the Code, which aims to set the age at which a child may generally consent to the collection, use or disclosure of their personal information at 15;
(b) the Social Media Minimum Age, which prohibits children under 16 from holding accounts on designated platforms); and
(c) the Age-Restricted Materials Codes, which require protections for under 18s.

The coexistence of these differing age thresholds may give rise to complexity for platforms and users in understanding their respective rights and obligations. The potential for regulatory tension is particularly evident when considering the Code's strong emphasis on data minimisation and consent against the existing obligations under the Online Safety Act.

The Code places strong emphasis on data minimisation: the adoption of a "*strictly necessary"* collection approach (section 9); prompt destruction of certain data (including age-assurance data) (section 8(4)); and a prescriptive consent framework. In particular, it establishes 15 as the age at which a child may generally consent to the handling of their personal information; requires platforms to take reasonable steps to verify parental consent for children under 15; and outlines specific scenarios in which a child's consent must be specifically obtained.

By contrast, the Online Safety Act imposes broad duties on platforms to take "*reasonable steps*" to prevent foreseeable harm to users, including children, and a broad range of safety obligations which may involve the processing of personal information (including that of children), depending on the specific measures adopted by the platform.

X considers that greater clarity regarding the interaction between these frameworks, particularly in relation to data minimisation, consent, and the handling of children's personal information, would assist platforms in meeting their obligations consistently across the regimes.

III. Other Feedback on Specific Provisions

Section 8 – Ascertaining the age of end-users

We support the risk-based, non-prescriptive approach to age assurance and the explicit permission to allow the reuse of existing, data-minimised age results. However, we recommend explicit guidance clarifying the potential interactions with other Commonwealth laws.

Section 9 – Privacy by default / "strictly necessary"

X already provides its users with controls over personalization, data sharing, and visibility. However, the "*strictly necessary*" requirement sets an unreasonably high bar for a social media service whose core functionality (discovery, recommendations, safety signals, network effects) inherently relies on data processing.

We strongly recommend that the OAIC publish guidance, with concrete examples, on how best to distinguish core service elements from optional or additional features.

Sections 10 and 11 – Best interests of the child (collection, use, disclosure, and direct marketing)

We agree in-principle with having the "*best interests of the child*" as the foundational anchor informing the interpretation of the Code. We also support the additional layer on top of APP 3 and the twin requirements of consent and child's best interests for most uses and disclosures. However, the inquiry of "*best interests*" is inherently highly contextual and value-laden. Clear guidance on how exactly to apply the "*best interest*" test in interpreting the specific requirements under the Code will be essential in order to avoid regulatory confusion, inconsistent enforcement, or inadvertent chilling effects as platforms err on the side of caution in order to demonstrate compliance.

Sections 13 to 20 - Consent

Whilst noting the inherent conflicts with other laws, we support setting the age of consent in the context of privacy at 15 as this aligns with existing OAIC guidance. We further support the requirements that consent be voluntary, informed, current, specific, and unambiguous.

The triple requirement for under-15s - namely of parental consent with reasonable verification steps; age-appropriate notification to the child; and assent in defined circumstances such as sensitive information, secondary uses, or direct marketing - are novel and highly protective. Whilst they increase transparency and digital literacy particularly amongst young persons, these will require significant compliance costs and engineering efforts as brand new product flows which are internationally unprecedented will have to be developed. This would in turn overly and unduly penalise small and mid-sized platforms, or platforms which do not target minors (such as X).

We strongly recommend that the OAIC maintains an outcomes-based, technology-neutral approach, and provide explicit guidance in the form of illustrative examples of reasonable verification methods. We further recommend that guidance and explicit affirmation of a risk-based, proportionate approach to seeking consent would be deemed compliant and acceptable.

***

X Corp supports the goals of the Code and believes its risk-based, child-centric design can deliver meaningful protections while preserving beneficial online experiences. The requirements are ambitious; success will depend on clear, practical guidance,

proportionality, and recognition of existing good-faith measures (including age assurance already rolled out on our platform).
We are also committed to working constructively with the Australian Government, the Office of the Australian Information Commissioner (OAIC), the eSafety Commissioner, industry partners, and wider society on these important issues. We remain available to discuss these comments or provide further information during future engagements. We look forward to more constructive dialogue during this interim period leading up to the finalisation of the Code.

Finally, given the significant engineering and product changes required to implement the consent framework and other obligations, we recommend a reasonable transitional period (for example, 18 months from registration) and/or phased commencement for higher-burden requirements. This would allow platforms to implement changes effectively while maintaining existing child-safety protections.

We reserve all our rights under law.

Sincerely,

X Corp.