Submission to the Office of the Australian Information Commissioner

Response to Exposure Draft of the Children's Online Privacy Code

June 2026

IGEA

interactive games & entertainment association

1. Overview

The Interactive Games & Entertainment Association (IGEA) welcomes the opportunity to provide a submission to the consultation on the Exposure Draft of the Privacy (Children's Online Privacy) Code 2026 (COP Code), and accompanying Exposure Draft Explanatory Statement, led by the Office of the Australian Information Commissioner (OAIC). This consultation follows on from IGEA's previous submission to the OAIC's 2025 consultation on its issues paper.[1]

IGEA is the industry association representing and advocating for the video games industry in Australia, including developers, publishers and distributors, and the makers of the most popular game platforms, consoles and devices.

Overall, we continue to support the intention behind the COP Code to strengthen protections for children's privacy online in Australia. Our industry members have long recognised that player trust is essential, not only as an ethical obligation, but also as a foundation for commercial success. In a global market where players have abundant choice, maintaining that trust requires a sustained commitment to online privacy, safety and security.

Safeguarding personal information, particularly for children and young people, has been central to industry practice for many years. Game companies have invested significantly in privacy-enhancing tools, including age-appropriate account structures, robust parental controls, granular privacy settings, and features that limit data sharing, communication and profile visibility (including the widespread use of pseudonymous gamer tags). These measures complement broader efforts to foster positive online environments and uphold international standards for age-appropriate content – standards that the industry applies consistently across jurisdictions, including Australia.

The sector also places strong emphasis on education and empowerment. Supporting parents and young players in navigating online play safely (whether through digital literacy initiatives, guidance materials, or in-product tools) remains a core part of the industry's approach. This shared-responsibility model is essential to enabling informed and confident participation in online gaming.

Given this longstanding commitment, we consider it important that any reforms to privacy and data governance maintain a principles-based framework. Clear and flexible standards encourage responsible data practices while avoiding rigid rules that could hinder innovation, create unnecessary compliance burdens, or inadvertently compromise online privacy, safety or security. In Australia, the existing Australian Privacy Principles (APPs) provide this balance effectively.

Previously, we offered preliminary high-level views regarding aspects of the Code. With the release of the Exposure Draft Code and accompanying Explanatory Statement, we can now provide a more detailed and substantive response.

[1] See: https://igea.net/2025/07/igea-submission-to-oaic-issues-paper-on-childrens-online-privacy-code/

This submission identifies key issues that would benefit from further consultation, including through targeted amendments to the Exposure Draft and the development of accompanying OAIC guidance. While we support the policy intent of the Code, aspects of the Exposure Draft raise practical implementation challenges which, if not addressed, risk undermining its effectiveness in delivering meaningful outcomes. Given the technical and operational complexity of many obligations in the Code, ongoing consultation with industry will be critical to ensuring entities can understand and meet their obligations in a clear and workable manner. We welcome the opportunity to continue working with the OAIC as it engages with industry ahead of finalising the Code.

For ease of reference, we summarise our key recommendations made in this submission below.

Topic	**IGEA's recommendation**
Further consultation	The OAIC should undertake further targeted consultation with affected industry stakeholders, including the video games industry, on key issues identified in this submission, through refinement of the Exposure Draft Code and the development of detailed guidance to accompany the final Code.
International regulatory coherence with the UK's AADC	To support international regulatory coherence and reduce unnecessary duplication, the OAIC should: • align the COP Code with the UK's AADC to the greatest extent possible; • clearly identify areas of substantive alignment and provide guidance on where compliance with the AADC may be relied upon (in whole or in part) for the purposes of demonstrating compliance with the COP Code; and • ensure that any departures from the UK's AADC are clearly articulated and appropriately justified.
Definitions and alignment with the Online Safety Act (OSA)	To maintain alignment with the OSA and avoid definitional drift, the OAIC should confirm how the Relevant Electronic Services (RES) and Designated Internet Services (DIS) are intended to be applied under the Code, particularly in relation to online game services. It should also clarify that existing OSA interpretations remain applicable for the purposes of determining the scope, and ensure that the Codes does not expand or reinterpret these categories in a way that creates overlapping or inconsistent regulatory coverage.
Ambiguity in "likely to be accessed by children" definition	The OAIC should provide clear operational guidance on the practical application of the "likely to be accessed by children" test, drawing on lessons from the UK's AADC and comparable international frameworks. In particular, the OAIC should: • set out specific non-exhaustive criteria for assessing whether a service is "likely to be accessed by children", including factors such as: the nature and purpose of the service; whether children form a "substantive and identifiable user group"; audience composition and usage patterns; how

Topic	IGEA's recommendation
	access to the service is restricted; and recognising that not all services pose the same level of risk;[2] • clarify how existing mechanisms may be relied upon in making this assessment, including account holder age confirmation; • provide illustrative examples, including scenarios where the threshold is, and is not, met; and • consider whether, or how, elements of a "directed at children" concept could be used to interpret the "likely to be accessed by children" framework, providing a more objectively determinable reference point to support clearer and better targeted application of the test.
R 18+ games should be out of scope	To ensure consistency with existing statutory obligations, the OAIC should clarify that, in assessing whether a service is "likely to be accessed by children", relevant factors must include whether the service provides content classified R 18+ and complies with applicable mandatory access-control requirements under the National Classification Scheme (NCS) and OSA.
Interaction between age thresholds and classification categories	The OAIC should clarify how the Code's age thresholds interact with the NCS categories below R 18+, including by confirming the treatment of MA 15+ content. In particular, guidance should: • recognise that MA 15+ games are not generally directed at, or likely to be accessed by, children under 15 in a way that warrants full child-specific obligations; • clarify how parental consent operates where under-15 access occurs with parental approval or supervision under the NCS; and • avoid duplicative or conflicting consent requirements that create unnecessary friction for families (e.g. repeated or intrusive consent prompts where parental involvement has already been exercised).
Nuance around online games	The OAIC should develop sector-specific guidance that distinguishes between services whose core business model relies on the collection, aggregation and reuse of personal data, and services (such as online games) where data collection is incidental to the delivery of interactive entertainment. This should also take into account sector-specific safeguards such as classification systems and parental control mechanisms.
Proportionality and the impact on small businesses	Small businesses should receive additional support to uplift privacy practices and meet Code requirements, including reasonable commencement timeframes, and targeted and practical guidance to assist with complex obligations such as PIAs.

[2] For example, see: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/age-appropriate-design-a-code-of-practice-for-online-services/services-covered-by-this-code/#code4

Topic	IGEA's recommendation
Effective implementation of the Code	The OAIC should publish targeted and practical guidance to the final Code, and provide a reasonable implementation period of at least 24 months following the publication of OAIC guidance. This will help to support organisations to properly understand and meet their obligations under the Code.
Ascertaining age of end-users	Scope of "high privacy by default" approach: • OAIC guidance should affirm that a "high privacy by default" approach under section 8(5) of the Code is a legitimate and proportionate compliance pathway, rather than a narrow exception. • It should also clarify the circumstances in which the universal application of child-level protections is the appropriate approach, especially where age-assurance would introduce greater privacy or security risks than it would mitigate. • In addition to age assurance, the OAIC should also clarify other obligations under the Code that would not apply under a "high privacy by default" approach, such as requirements to obtain child assent and parental verification. • OAIC guidance should clarify the scope at which section 8(5) operates, including whether a "high privacy by default" approach may be applied to specific parts of a service that are directed at, or likely to be accessed by, children, rather than requiring service-wide application. Interaction with Age-Restricted Material (ARM) Code obligations: OAIC guidance should address the interaction between section 8 of the COP Code and ARM Code obligations, to ensure entities are not driven to adopt intrusive age assurance methods by default, where privacy-preserving and proportionate alternatives are available. This should include clarification on whether, and to what extent, risks arising from data-enabled features or systems are intended to inform the level of age assurance required. International regulatory coherence: The OAIC should align the COP Code, to the greatest extent possible, with established international approaches (including the UK's AADC), including in relation to recognised age assurance approaches (e.g. adult account holder models) where these support privacy-preserving and proportionate outcomes.[3]
"Strictly necessary" and high privacy by default	Sector-specific guidance: Given the unique characteristics of online games and the distinct ways in which children interact with them, the OAIC should develop sector-specific guidance on the application of section 9 of the Code to online games. This would ensure that the "strictly necessary" and "high privacy by default" obligations enhance children's privacy without

[3] For example, see: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/age-appropriate-design-a-code-of-practice-for-online-services/3-age-appropriate-application/

Topic	IGEA's recommendation
	unintentionally undermining gameplay functionality, safety or user experience. Secondary (yet necessary) purposes: The OAIC should also publish comprehensive guidance clarifying the categories of secondary (yet necessary) purposes that are consistent with the best interests of the child and permitted under a "strictly necessary" standard. Without limitation, this guidance should include a non-exhaustive list of examples covering: (1) product improvement and reliability (e.g. diagnostics, error reporting, bug-fixing); (2) user-experience research and design improvement using aggregated or de-identified data; (3) safety, integrity and trust-and-safety operations (e.g. detection of harmful conduct, grooming, harassment and content moderation); (4) security, fraud and abuse prevention; and (5) legal and regulatory compliance. Alignment with APPs: The OAIC should also clarify how the "strictly necessary" standard is intended to operate alongside the existing "reasonably necessary" test under the APPs, including any relevant child-specific considerations that inform this assessment.
Best interests of the child	UN Convention on the Rights of the Child (UNCRC) considerations: To ensure the "best interests of the child" test is applied consistently with the UNCRC, the following note should be added to sections 10 and 11 of the Code: ***Note: When assessing the best interests of the child, entities should have regard to the full range of the child's rights under the UNCRC and balance those rights holistically. This includes considering rights that may be indirectly affected, such as the child's right to play, leisure, and participation in social, cultural and recreational activities.*** OAIC guidance: The OAIC should also provide guidance on how the best interests test is to be applied in practice across different service types, including low-risk, curated environments such as online games, to ensure the test is applied in a proportionate and context-sensitive manner.
Bundled consent	The OAIC should clarify how entities can design consent processes that comply with section 14(3)(b) of the Code regarding bundled consent, while remaining child-appropriate and effective. This should include guidance on: • Distinguishing between personal information processing that is integral to delivering the core service requested by the user (which should not require separate unbundled consent), and optional purposes (where unbundled consent may be appropriate). • Examples of acceptable consent approaches, such as a single layered onboarding consent process that clearly distinguishes core gameplay and safety-related data practices from optional features, with just-in-time consent prompts used only where a materially new purpose arises.
12-month consent period	Rethinking fixed annual consent-expiry rule: Section 15(4) of the Code should be revisited. A fixed annual consent-expiry rule risks imposing a significant

Topic	IGEA's recommendation
	ongoing administrative burden on families, contributing to consent fatigue and reducing the quality of consent over time. Flexible risk-based approach: The OAIC should adopt a more flexible risk-based approach to consent renewal. In particular, where data practices are stable, low-risk and consistent with users' reasonable expectations, consent should remain valid beyond a fixed 12-month period and should not require routine renewal in the absence of a material change to data practices or user expectations. Meaningful engagement: A more proportionate approach would prioritise meaningful engagement – for example, through periodic reminders to parents and carers about existing consents, combined with renewed express consent at key transition points (e.g. when a child reaches an age where decision-making responsibility begins to shift, and again at adulthood). This approach would better recognise the persistent, long-running nature of game environments, where repeated annual renewal may be unnecessary or counterproductive where relevant data practices have not materially changed.
Assent requirements for children under 15	Proportionate and flexible approach: The OAIC should ensure that assent requirements are implemented in a proportionate and flexible manner that reflects the unique characteristics of online games. To support effective compliance (particularly for smaller businesses), the OAIC should provide clear practical guidance on age-appropriate notices that do not disrupt gameplay. This will help ensure assent mechanisms enhance children's understanding without imposing unnecessary technical burdens. Redundant assent: To avoid redundant or disruptive assent processes in circumstances where parental consent has already been clearly established, while preserving the OAIC's intent to involve children in meaningful decisions, section 20 of the Code should be amended (or clarified in guidance), inserting a new subsection, as follows: ***Assent is not required where a person with parental responsibility has already enabled functional parental control tools that govern the relevant collection, use or disclosure of the child's personal information.*** Scope of assent obligations: The OAIC should clarify the scope of the assent requirement, including that assent is not required for personal information processing that is integral to the provision of the core service or necessary for safety, integrity and compliance purposes, and should be directed toward higher-risk secondary uses of personal information. Reframing assent as age-appropriate notice: Alternatively, the OAIC should consider reframing the child assent requirement as an obligation to provide an age-appropriate notice to the child. Requiring both an active assent step from the child and verified legal consent from a parent or carer creates a confusing and burdensome onboarding experience for families, with a real risk of bottlenecking sign-up flows and pushing families toward less child-

Topic	IGEA's recommendation
	safe alternatives. This approach would still support the objective of promoting children's awareness and understanding of personal information handling as they grow.
Cumulative impact of consent and verification requirements	Holistic approach: The OAIC should take a holistic systems-level consideration of how the Code's consent and parental verification requirements operate together in practice, particularly in long-running interactive services such as games. OAIC guidance: • Additional OAIC guidance would assist entities to design consent architectures that are coherent, proportionate and genuinely supportive of informed decision-making, rather than inadvertently encouraging consent fatigue. • In particular, further OAIC guidance on parental verification is required. The potential verification methods suggested in the Code and Explanatory Statement (e.g. email contact, tokens, video calls with customer service agents, government identification) involve differing privacy, accessibility and reliability trade-offs, and may not always provide a consistent or proportionate means of establishing parental responsibility in practice. • To provide greater certainty for industry and a consistent experience for families, the OAIC should: (1) publish detailed guidance on what constitutes acceptable verification of parental responsibility across a range of low-, medium- and high-privacy-risk scenarios; and (2) consider adopting a safe-harbour approach that identifies specific verification methods which, if used in good faith, may be treated as compliant. Such an approach could be modelled on the U.S. Children's Online Privacy Protection Act (COPPA), which includes FTC-recognised verification methods, adapted for the Australian context.
Transparency and child-friendly privacy policies	Non-text material: To ensure the section 23 requirement is workable for diverse game environments, while preserving the OAIC's intent, the following amendment should be made to section 23(3)(c): *(c) where appropriate, incorporate non-text material to engage children effectively* ***in a manner that is compatible with the visual design, user experience and technical constraints of the service, and does not unreasonably disrupt its operation*** Child-friendly language requirements: The detailed disclosure requirements in Division 3 of the Code may be difficult to reconcile with the concurrent obligation that child-friendly privacy notices must not include complex or technical expressions or terminology drawn from specialist industry or legal language. To support effective implementation, child-friendly language requirements should be limited to outward-facing notices and consent flows directed at children, and entities should be permitted to adopt a layered framework combining simplified, accessible summaries for children with

Topic	IGEA's recommendation
	more detailed explanations where appropriate – including where legal consent must be obtained from a parent or carer. OAIC guidance should include illustrative examples of acceptable child-friendly notices and clarify what constitutes "legal language" for this purpose. Layered privacy disclosures: • Consistent with this approach, OAIC guidance should clarify that entities are not required to adopt a wholly separate child-specific privacy policy in all cases, particularly where layered and contextual disclosures are effective. • OAIC guidance should clarify how layered or multiple forms of privacy disclosures are intended to operate together in practice, including which version to rely upon in the event of resolving inconsistencies or disputes. Sector-specific guidance: OAIC sector-specific guidance should be provided on the application of section 23 of the Code on transparency obligations for child-friendly privacy policies, including with respect to prominent position, non-text material, and pseudonymity and anonymity.
Cross-border disclosures	Disclosure for online games: The OAIC should clarify, for the purposes of section 26 of the Code, what constitutes adequate, age-appropriate disclosure of overseas data flows in the context of online games, especially where individual developers lack direct control over, or visibility into, the specific overseas infrastructure processing personal information. Consideration should be given to the suitability of high-level disclosure that personal information may be processed overseas, clear explanation of the purposes involved, and assurance that appropriate safeguards apply regardless of processing location. Pseudonymised, de-identified or anonymised personal information: Additionally, the OAIC should clarify how this requirement applies where personal information is processed in a pseudonymised, de-identified or anonymised form. In such lower privacy risk cases, consideration should be given to whether high-level disclosure through privacy policies may be sufficient, without requiring separate age-appropriate consent for each overseas disclosure.
Automated decision-making (ADM) and access to information	Proportionate risk-based approach: The OAIC should adopt a proportionate risk-based approach to ADM disclosures under section 28 of the Code, and clarify that entities are not required to disclose proprietary algorithms or trade secrets. Sector-specific guidance: OAIC sector-specific guidance should support smaller studios in providing age-appropriate explanations of ADM without compromising gameplay integrity or imposing unnecessary technical burdens.

Topic	IGEA's recommendation
	Amendment to Code: To provide additional certainty and ensure the OAIC's intent is implemented consistently, section 28(2)(g) should be amended as follows: *whether there is any automated decision-making, including profiling, relating to the personal information and, if so, clear and meaningful information about the context of such decisions, including the logic involved* ***(excluding proprietary algorithms or trade secrets essential to service integrity)*** *and the consequences of making them.*
Consent not obtained by coercion	Proportionate risk-based approach: The OAIC should ensure that consent requirements under section 21 of the Code are applied in a proportionate and flexible manner that reflects the unique characteristics of online games and avoids assumptions based on high-risk service models. Legitimate practices: In particular, the OAIC should adopt a clear and narrow definition of "nudge techniques" that focuses on genuinely manipulative practices that are misleading or deceptive, and does not inadvertently capture creative or thematic in-game content, or legitimate, innocuous, reasonable or generally accepted gameplay design and commercial practices. Amendment to Code: To ensure that legitimate artistic expression and commercial practices are not inadvertently restricted, while preserving the OAIC's intent, the following note should be added to section 21: ***Note: This section does not capture creative or thematic content designed to maintain the immersive narrative of an interactive service, or legitimate, innocuous, reasonable or generally accepted gameplay design choices and in-game commercial practices, provided they are not misleading or deceptive.***
Opting out of direct marketing	Legitimate advertising-supported free-to-play models: The OAIC should ensure that section 29 of the Code is interpreted and applied in a manner that recognises the legitimate role of advertising-supported free-to-play models in enabling children's access to games, particularly where advertising is contextual, age-appropriate and confined to the game environment, and that application of the provision remains proportionate to the privacy risks. Best interests test: The OAIC should clarify the operation of section 29 in conjunction with the best interests test, including through guidance on how compliant direct marketing opt-out mechanisms can be implemented within immersive game environments in a manner that is practicable and achievable for providers of different sizes. Scope and application: The OAIC should provide further guidance on the scope and application of "direct marketing" under section 29, including clarifying whether non-personalised communications relating to gameplay or service updates fall within its scope. Guidance should also confirm that entities, which do not engage in targeted or profiling-based advertising to children, are not subject to unnecessary or additional opt-out requirements,

Topic	IGEA's recommendation
	and should recognise that parents or carers may appropriately manage communications preferences on behalf of younger children.
Requests to destroy personal information	Proportionate and technically feasible approach: The OAIC should ensure that section 32 of the Code is applied in a proportionate and technically feasible manner, allowing for de-identification as a valid alternative to destruction, consistent with APP 11 and existing OAIC guidance, and provide sector-specific guidance on its application to online games. De-identification: Section 32(2) should be amended to allow de-identification as an alternative to destruction, recognising that this is a privacy-protective and technically feasible approach for certain categories of shared gameplay and game-state data in complex shared game environments: *If a request is made, the entity must destroy **or de-identify** the information**, in accordance with APP 11**.* Limited exceptions: The OAIC should consider introducing a limited exception to destruction under section 32 for personal information reasonably required to support cyber security, fraud prevention and safety-related functions. Certain categories of data may be necessary to maintain safe and secure environments for children and other users. Family and household contexts: The OAIC should clarify how rights relating to personal information, including requests for destruction, are intended to operate in family or household account contexts. This should include recognising that such rights may be appropriately exercised by a parent or carer and implemented through existing profile-level tools rather than requiring separate child-facing processes. Safeguards against unreasonable requests: The OAIC should consider appropriate safeguards around the exercise of requests, including to ensure that entities are not required to respond to volumes of unreasonable requests (e.g. frivolous, vexatious or malicious), while preserving access for genuine requests.
Parental controls and geolocation monitoring	Sector-specific guidance: The OAIC should provide sector-specific guidance on the application of section 33 of the Code in the context of online games. This should cover how notification requirements can be implemented in a manner that is compatible with game interfaces. Clear guidance would support consistent implementation while ensuring transparency obligations do not inadvertently disrupt gameplay or impose unnecessary technical burdens. Minimising disruption: To ensure notification requirements are workable across diverse game environments and compatible with the immersive nature of gameplay, we recommend that section 33(3)(c) be amended as follows:

Topic	IGEA's recommendation
	The notification must: … be given in a way that reasonably ensures the child is aware of the use of the mechanism ***while minimising disruption to the primary use of the service****.* Family and household contexts: The OAIC should clarify how notification requirements under section 33 apply in family or household account contexts, including where parental controls are enabled and children are using services under parental supervision. Guidance should recognise that additional child-facing notifications may not be necessary where they would be redundant or unduly disruptive. Scope of geolocation data: The OAIC should also clarify the scope of "geolocation" for the purposes of section 33, including whether this is intended to capture only precise geolocation tracking, as opposed to incidental or functional data (e.g. IP addresses) processed as part of standard service delivery.
Child-friendly information and complaints mechanisms	The OAIC should clarify what constitutes a proportionate and compliant child-friendly inquiry and complaints mechanism for the purposes of sections 35 and 36 of the Code, having regard to the size, resources and business models of different game developers.
Mandatory privacy impact assessments (PIAs)	Proportionate and scalable approach: The OAIC should adopt a proportionate and scalable approach to PIAs under sections 38 and 39 of the Code, including the use of standardised or simplified PIA templates and scaled assessment requirements for small and mid-sized businesses, having regard to the nature, scale and risk profile of the service. Scope and operation of PIAs: The OAIC should clarify: (1) the threshold of "significant change" that triggers a new PIA obligation under sections 38 and 39 (including confirming that this refers to materially new or higher-risk features rather than incremental or iterative updates); (2) how the "best interests of the child" standard should be applied in practice; and (3) how any requirement to maintain a register of PIAs can be implemented in a manner that promotes transparency and accountability, without requiring disclosure of commercially sensitive or security-relevant information. Register of PIAs: The OAIC should reconsider the requirement in section 39(2) to maintain a public register of PIAs. Consideration should be given to alternative approaches that preserve regulatory oversight, while mitigating unintended risks and burdens, such as maintaining an internal register of PIAs that can be made available to the OAIC on request, or permitting appropriate redactions of commercially sensitive or security-relevant information prior to publication. A public register may create unintended incentives to limit the scope or documentation of PIAs and could expose information that undermines system integrity or safety controls.
Review of privacy practices	To reduce unnecessary administrative burden for smaller businesses, while maintaining accountability, section 25(1) of the Code should be amended as follows:

Topic	IGEA's recommendation
	*An entity must review and update, at least **biennially**, the practices, procedures and systems required by Australian Privacy Principle 1.2 to ensure that they comply with the Australian Privacy Principles and this Code.*
Privacy education and training	Proportionate and flexible approach: To avoid unnecessary repetition, while ensuring training remains relevant, section 40(2)(c)(ii) of the Code should be amended as follows: *at least **biennially** thereafter**, and additionally where there is a significant change to the entity's privacy practices**.* Sector-specific guidance: The OAIC should provide sector-specific guidance on privacy training obligations in the games sector. Standardised privacy training: To support proportionate compliance, particularly for smaller businesses, the OAIC should develop standardised privacy training modules that entities can adopt or adapt, reducing the need for bespoke training programs while supporting consistent understanding of obligations across the sector.

2. Best practice regulation and good public policy design

In developing this submission and the recommendations, we have been guided by established principles of best practice regulation and good public policy design. These principles reflect both our experience responding to previous consultations on the COP Code and our broader engagement with privacy, online safety, classification and other regulatory frameworks affecting the video games sector.

- Principles-based and risk-based regulation: This submission supports a principles-based regulatory framework that sets clear objectives while allowing flexibility in implementation. Our recommendations emphasise a risk-based approach that takes account of the nature of the service, the likelihood and extent of children's access, the sensitivity of personal information involved, and the actual privacy risks posed, ensuring regulatory effort is directed to areas of meaningful impact.
- Proportionality and regulatory impact: Proportionality has been a central consideration in developing our position. Regulatory obligations should scale according to risk and organisational capacity, particularly in a sector comprising many small and independent developers. Throughout this submission, we have assessed the practical, technical, and economic impacts of the proposed measures and suggested alternative approaches where compliance burdens risk outweighing privacy benefits.
- Coherence with existing regulatory frameworks: Effective regulation depends on clarity and consistency across the broader regulatory landscape. Our recommendations seek to ensure coherence between the Code and existing Australian frameworks (including the Australian Privacy Principles, Online Safety Act and National Classification Scheme), as well as international frameworks (including the UK's Age Appropriate Design Code (AADC)). This, in turn, will help to avoid regulatory duplication and overreach.

- Evidence-informed and sector-specific policymaking: Our approach draws on evidence from industry practice, long-standing Australian research on gameplay and player demographics, and lessons from comparable overseas regimes, particularly the UK's AADC. We have consistently emphasised that context matters, and that online games differ materially from higher-risk platforms, warranting proportionate, sector-specific application of requirements and guidance.
- Privacy-by-design, data minimisation and harm prevention: This submission strongly supports privacy-by-design and data-minimisation principles. Where privacy risks can be effectively mitigated through high-privacy defaults, service-wide protections or existing parental empowerment tools, we have favoured these approaches over more intrusive or data-intensive measures that may increase risks to online privacy, safety or security, particularly for children.
- A holistic understanding of the best interests of the child: Our recommendations reflect a holistic interpretation of the best interests of the child, consistent with the UN Convention on the Rights of the Child. While strong privacy protections are essential, effective policy must also recognise children's rights to play, participation, social interaction and age-appropriate digital experiences, and seek to balance protection from harm with positive and developmentally appropriate engagement.

3. Application of this Code

3.1. International regulatory coherence with the UK's AADC

The OAIC has stated its intention that the COP Code will be aligned with comparable international frameworks, including the UK's Age Appropriate Design Code (AADC). We previously noted that many of our industry members would likely already be compliant with the UK's AADC, and we strongly support international regulatory coherence, including alignment with well-established overseas regimes where possible. The UK's AADC has now been in operation for several years and is comparatively mature, with its expectations and practical implications better understood by industry.

To the extent that the COP Code closely mirrors the UK's AADC, we consider this an optimal outcome. Greater alignment would reduce fragmentation across jurisdictions, support consistent outcomes for children, and minimise unnecessary compliance duplication for organisations operating across multiple markets. However, alignment at a high level does not remove the need for careful consideration of differences in detail. Where the Code diverges from the UK approach to reflect the Australian regulatory context or policy objectives, those differences should be clearly articulated, transparently explained and well-justified.

As with any regulatory regime, there is also significant value in learning from implementation experience. Valuable lessons can be drawn from the UK's experience with the AADC, including areas where obligations have proven difficult to operationalise or where unintended consequences have arisen. These lessons should inform the development of the COP Code. In this regard, we encourage the OAIC to give strong

weight to feedback from industry stakeholders with direct experience implementing the UK's AADC, particularly where improvements or clarifications may be warranted.

There is also an opportunity for the OAIC to go further in supporting practical interoperability between the regimes. In particular, the OAIC could identify specific aspects of the AADC that it considers to be substantively equivalent or capable or being relied upon for the purposes of demonstrating compliance with the COP Code. For example, the OAIC could clarify whether Data Protection Impact Assessments (DPIAs) conducted in accordance with the UK's AADC may be treated as meeting, or substantially contributing to, the requirements for Privacy Impact Assessments (PIAs) under sections 38 and 39 of the COP Code, where they address comparable risks and safeguards.

Providing this form of cross-regime guidance would significantly reduce administrative overhead for entities operating across jurisdictions, while maintaining strong privacy protections for children. Comparable approaches have been adopted in other international contexts, where regulators have issued joint of alignment guidance to support compliance with overlapping frameworks.[4]

Critically, the more closely the COP Code aligns with established overseas approaches such as the UK's AADC, the more likely it is that regulatory burden on businesses (particularly those operating across multiple jurisdictions) will be reduced and overall compliance outcomes improved. Conversely, unnecessary or unexplained deviation from established overseas approaches is likely to increase compliance costs and create additional regulatory complexity, without corresponding privacy benefits for children.

Recommendation:

To support international regulatory coherence and reduce unnecessary duplication, the OAIC should:

- align the COP Code with the UK's AADC to the greatest extent possible;
- clearly identify areas of substantive alignment and provide guidance on where compliance with the AADC may be relied upon (in whole or in part) for the purposes of demonstrating compliance with the COP Code; and
- ensure that any departures from the UK's AADC are clearly articulated and appropriately justified.

3.2. Definitions and alignment with the Online Safety Act

We acknowledge the OAIC's clarification that the COP Code applies to providers of social media services (SMS), relevant electronic services (RES) and designated internet services (DIS) "within the meaning of the *Online Safety Act 2021*" (OSA), and where the service is "likely to be accessed by children".[5] However, the examples provided in section 5 of the Explanatory Statement suggest a broader conceptual application of these categories than

[4] For example, see: Joint Guide to ASEAN Model Contractual Clauses and EU Standard Contractual Clauses, https://asean.org/book/joint-guide-to-asean-model-contractual-clauses-and-eu-standard-contractual-clauses/
[5] *Privacy Act 1988* (Cth), section 26GC(5)(a)(i)

that typically reflected in the OSA and its subordinate instruments (including the industry online safety codes and standards).

In the context of video games, the OSA and eSafety have generally interpreted RES to apply only to multiplayer online games with communications functionality, while DIS covers certain internet services (but excludes consumer devices or equipment), which are separately defined under sections 134 and 135 of the OSA.[6]

The OAIC's example of IoT baby monitors risks blurring these established boundaries and expanding the conceptual scope of these categories beyond their settled meaning under the OSA. This creates a risk of overlapping or inconsistent regulatory application, where services may be captured differently across privacy and online safety frameworks.

Maintaining alignment with the OSA is therefore critical to ensuring that data privacy and online safety obligations (e.g. content moderation) operate within a coherent and predictable regulatory framework, and to avoid unnecessary duplication or fragmentation in how services are classified.

Regulatory coherence is essential. Any divergence in how the RES and DIS are interpreted or illustrated under the COP Code, as compared with the OSA and existing compliance frameworks, would create uncertainty for providers already subject to the National Classification Scheme (NCS) and OSA (including industry online safety codes and standards).

Recommendation:

To maintain alignment with the OSA and avoid definitional drift, the OAIC should confirm how the RES and DIS are intended to be applied under the Code, particularly in relation to online game services. It should also clarify that existing OSA interpretations remain applicable for the purposes of determining the scope, and ensure that the Codes does not expand or reinterpret these categories in a way that creates overlapping or inconsistent regulatory coverage.

3.3. Ambiguity in "likely to be accessed by children" definition

The Explanatory Statement does not provide practical guidance on the meaning of "likely to be accessed by children". As noted in our previous submission, the UK's experience with the Age Appropriate Design Code (AADC) demonstrates that, without clear guidance, this concept can be interpreted so broadly that it effectively captures large portions of the internet.

[6] Note: 'equipment' is defined to mean equipment for use by end-users in Australia of services such as SMS, RES or DIS, in connection with that service. This delineation is explicitly clear under sections 134 and 135 of the OSA. Further, eSafety refers to "devices" as "equipment that is for use by end-users in Australia of a social media service, relevant electronic service, designated internet service or internet carriage service, in connection with that service. While the Act [OSA] uses the term 'equipment' when referring to persons who manufacture, supply, maintain or install this equipment, 'devices' is a more commonly understood term." See: eSafety, Position Paper: Development of industry codes under the Online Safety Act (September 2021), p. 13, https://www.esafety.gov.au/sites/default/files/2021-09/eSafety%20Industry%20Codes%20Position%20Paper.pdf

Key questions remain unanswered:

- What level of child usage satisfies the "likely" threshold?
- How should services with predominantly adult audiences and minimal under-18 usage be treated?
- How should the concept of "children" be applied in practice to older teenagers within services not directed at children?

In the absence of clarity, providers (particularly small businesses) may adopt overly conservative interpretations to avoid compliance risk, resulting in disproportionate burdens on services not intended for children and with minimal underage usage.

Recommendation:

The OAIC should provide clear operational guidance on the practical application of the "likely to be accessed by children" test, drawing on lessons from the UK's AADC and comparable international frameworks. In particular, the OAIC should:

- set out specific non-exhaustive criteria for assessing whether a service is "likely to be accessed by children", including factors such as: the nature and purpose of the service; whether children form a "substantive and identifiable user group"; audience composition and usage patterns; how access to the service is restricted; and recognising that not all services pose the same level of risk;[7]
- clarify how existing mechanisms may be relied upon in making this assessment, including account holder age confirmation;
- provide illustrative examples, including scenarios where the threshold is, and is not, met; and
- consider whether, or how, elements of a "directed at children" concept could be used to interpret the "likely to be accessed by children" framework, providing a more objectively determinable reference point to support clearer and better targeted application of the test.

3.4. R 18+ games should be out of scope

The Explanatory Statement does not acknowledge the existing legal frameworks that already govern access to R 18+ content:

- under the NCS, R 18+ games are legally restricted to adults;
- the Online Safety (Restricted Access Systems) Declaration 2022 (RAS Declaration) requires mandatory access controls for R 18+ content; and
- the Age-Restricted Material (ARM) industry online safety codes require additional age-restriction measures including age assurance for certain services.

Together, these frameworks represent the Australian Government's chosen mechanisms for mitigating the risk of children accessing R 18+ material. In the absence of evidence of systemic enforcement failure, services that comply with these binding obligations should

[7] For example, see: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/age-appropriate-design-a-code-of-practice-for-online-services/services-covered-by-this-code/#code4

not be characterised as "likely to be accessed by children" for the purposes of the Code. The Explanatory Statement does not explain how this existing regulatory context is intended to be taken into account.

Applying the Code to R 18+ services without regard to these mandatory access-control regimes risks regulatory duplication, over-capture and inconsistency with settled statutory design.

Recommendation:

To ensure consistency with existing statutory obligations, the OAIC should clarify that, in assessing whether a service is "likely to be accessed by children", relevant factors must include whether the service provides content classified R 18+ and complies with applicable mandatory access-control requirements under the NCS and OSA.

3.5. Interaction between age thresholds and classification categories

The Code introduces multiple age-based distinctions that interact with existing age-based frameworks under the NCS in ways that are not clearly articulated, creating uncertainty for game developers and publishers assessing whether their services fall within scope and how obligations should apply in practice.

Under section 13 of the Code, parental consent is required for children under 15 in relation to personal information handling. This age threshold overlaps with the NCS's MA 15+ category, which permits parental supervised access of persons under 15. While the age thresholds align numerically, the Explanatory Statement does not address how the Code's consent model is intended to operate alongside the NCS's age-based supervision model for MA 15+ games.[8]

In particular, it is unclear whether the parental role contemplated under the Code (e.g. ongoing consent authority over personal information) assumes or extends beyond the more limited access-supervision role recognised under the NCS. This lack of clarification creates uncertainty for game developers as to how parental involvement is expected to function in practice for MA 15+ titles lawfully accessed by under-15 players.

MA 15+ games are subject to restricted access under the NCS and are not designed or marketed for younger children.[9] However, once lawfully accessed, they may be used by players aged 15 and over (including 16- and 17-year-olds) who, under the Code's age-based framework, may provide their own consent without parental involvement. For this cohort, it is unclear how and when child-specific obligations are intended to continue to apply. This creates practical uncertainty for services that are not child-directed, but that may be accessed by older children.

[8] See: https://www.classification.gov.au/classification-ratings/what-are-ratings

[9] Note: Any guidance is also complicated by the fact that MA 15+ classifications are currently under separate review by the Department of Instructure, Transport, Regional Development, Communications, Sport and the Arts. This raises the risk that obligations under the Code may be interpreted by reference to an interim or evolving classification framework. See: https://www.infrastructure.gov.au/have-your-say/modernising-and-harmonising-classification-standards

This uncertainty is commercially significant. Although MA 15+ games may represent a smaller proportion of classified titles, they encompass a commercially and culturally significant category of mainstream products aimed at adolescents and adults rather than children, meaning over-capture would impose disproportionate compliance burdens. Treating this category as presumptively in scope risks regulatory over-reach and extends child-focused obligations beyond the apparent policy intent of the Code.

Clear guidance on how the Code's age thresholds are intended to interact with classification categories below R 18+ is therefore essential to ensure consistent, proportionate and predictable application.

Recommendation:

The OAIC should clarify how the Code's age thresholds interact with the NCS categories below R 18+, including by confirming the treatment of MA 15+ content. In particular, guidance should:

- recognise that MA 15+ games are not generally directed at, or likely to be accessed by, children under 15 in a way that warrants full child-specific obligations;
- clarify how parental consent operates where under-15 access occurs with parental approval or supervision under the NCS; and
- avoid duplicative or conflicting consent requirements that create unnecessary friction for families (e.g. repeated or intrusive consent prompts where parental involvement has already been exercised).

3.6. Nuance around online games

Distinctions between online services in this submission are raised solely to explain differences in privacy risk arising from data approaches, not to imply criticism between sectors. The Explanatory Statement does not adequately acknowledge the nuanced ways in which online games operate compared to other online services.

For example, while online games may collect and use personal data incidentally to enable gameplay, they differ from services that are centred around the collection, aggregation and reuse of personal data as a core part of their service model. Online games are primarily designed for interactive entertainment, and while some games include communication or social features, these are typically ancillary to gameplay, limited or ephemeral in nature, and do not constitute the service's primary purpose. This is further reinforced by established safeguards within the sector, including formal age-based classification ratings and the widespread availability of parental control tools, which support informed access decisions and enable parents and carers to manage children's engagement in a structured and transparent manner.

As a result, the privacy risks associated with many online games often differ in nature and scale from those presented by other services. However, the Explanatory Statement does not explain how these differences are intended to be reflected in the application of obligations across providers classified as SMS, RES or DIS.

In the absence of clearer guidance, there is a risk that online games may be subject to the same compliance expectations as online services whose data practices involve the

systematic collection, aggregation and reuse of personal data as a core part of their business model. Applying uniform obligations would undermine the Code's risk-based approach and impose disproportionate compliance burdens on services whose data use is incidental to delivery of interactive entertainment and whose privacy risk profile differs materially in nature and scale.

Recommendation:

The OAIC should develop sector-specific guidance that distinguishes between services whose core business model relies on the collection, aggregation and reuse of personal data, and services (such as online games) where data collection is incidental to the delivery of interactive entertainment. This should also take into account sector-specific safeguards such as classification systems and parental control mechanisms.

3.7. Proportionality and the impact on small businesses

The Explanatory Statement does not address the disproportionate impact the Code may have on small game developers who:

- may be APP entities despite relatively low annual turnover (i.e. just above the $3 million threshold) or limited organisational capacity;
- may be captured as RES providers even where child access is incidental; and
- often lack the resources of larger platforms to implement complex compliance frameworks.

Importantly, small studios are a foundational part of Australia's games industry and its export success. Many of Australia's most commercially successful and internationally recognised games have been developed by teams of only a handful of developers. These studios operate in a highly competitive global market, and are export-oriented by necessity. Disproportionate compliance burdens, therefore, have the potential to affect not only individual studios but the sustainability and export performance of the sector as a whole.

It may be argued that entities with annual revenue of at least $3 million should be able to comply with the Code irrespective of organisational size. While we agree that all APP entities must meet their legal obligations, turnover alone is an imprecise proxy for compliance capability, particularly for small game studios with limited staff, technical and legal resources.

The issue is not whether smaller studios should comply with the Code, but whether the manner in which compliance is expected to be achieved is proportionate to the nature, scale and risk profile of the service. Applying uniform procedural expectations (e.g. in relation to the depth of privacy impact assessments (PIAs), the sophistication of governance frameworks, or the frequency of ongoing monitoring) may impose material costs without delivering corresponding improvements in children's privacy outcomes, particularly where child access is incidental or limited.

This challenge is not theoretical. For example, one independent Australian studio developing a multiplayer game sought compliance guidance from a relevant regulator regarding its obligations. The response received was that the regulator could not provide

advice. For small businesses, the absence of accessible practical guidance creates significant uncertainty and can result in overly conservative or inefficient compliance approaches that divert scarce resources away from development and safety-enhancing features.

A principles-based Code must incorporate proportionate obligations that scale according to the nature of the service and the provider's capacity. Without proportionality, the Code risks imposing burdens that do not meaningfully advance children's interests and may have the unintended effect of reducing the availability of safe and age-appropriate games.

In addition to proportionate obligations, smaller studios will require practical implementation support. Consistent with our broader position that regulatory measures should be clear, flexible and workable for providers of all sizes, the OAIC should adopt reasonable commencement timeframes to allow smaller developers sufficient time to update systems, processes and documentation. This is particularly important where the Code introduces new or expanded expectations, such as in relation to PIAs, child-specific privacy notices or ongoing monitoring requirements.

Recommendation:

Small businesses should receive additional support to uplift privacy practices and meet Code requirements, including reasonable commencement timeframes, and targeted and practical guidance to assist with complex obligations such as PIAs.

3.8. Effective implementation of the Code

To support effective compliance, the OAIC should publish targeted practical guidance alongside the final Code. Such guidance should address key interpretative and operational questions raised throughout this submission. It should also provide clear sector-specific examples of how complex requirements can be met in a proportionate and resource-efficient manner, particularly for smaller businesses. Many of the Code's obligations cannot be effectively implemented until this guidance is available. Given the scale and complexity of the changes required for organisations of different sizes, an implementation period of at least 24 months following the publication of guidance would be appropriate.

Recommendation:

The OAIC should publish targeted and practical guidance to the final Code, and provide a reasonable implementation period of at least 24 months following the publication of OAIC guidance. This will help to support organisations to properly understand and meet their obligations under the Code.

4. Ascertaining age of end-users

We welcome the OAIC's continued focus on ensuring that privacy protections for children are risk-based, proportionate, technologically flexible, and aligned with broader regulatory developments. In our previous submission, we highlighted the significant uncertainty surrounding age assurance technologies, the privacy and security risks associated with their

implementation, and the need for coordinated regulatory guidance across government. Since that time, the Age Assurance Trial has concluded, the *Online Safety Amendment (Social Media Minimum Age) Act 2024* (Cth) (SMMA Act) has commenced, and the Age-Restricted Material (ARM) industry online safety codes have taken effect. These developments make it even more important that the OAIC's guidance provides clear direction on privacy-preserving approaches.[10]

We recognise that age assurance can play a role in identifying child users in certain contexts. However, as we previously noted, age assurance mechanisms raise legitimate concerns regarding privacy, security, proportionality and broader human rights, including freedom of expression. These concerns were evidenced in public responses to the Age Assurance Trial, including the gap between theoretical support for age assurance and low levels of trust in its implementation by government and industry.[11] Many of these concerns remain unresolved, highlighting the need for a cautious risk-based approach.

In this context, we support in principle the OAIC's risk-based approach in section 8 of the Code, including the inclusion of section 8(5). This provision reflects sound regulatory design in recognising that, where robust child protections are applied universally across a service, additional age assurance may introduce greater privacy and security risks than it mitigates, without delivering meaningful additional benefits for children. Section 8(5) appropriately allows entities to achieve compliance through the universal application of child-level protections, rather than mandating age assurance as a default requirement.

At the same time, the universal application of child-level protections should not be treated as a default or precautionary substitute for age differentiation in circumstances where it is not proportionate to the service's functionality, data practices or risk profile. Services vary significantly in their design and operation, and some may present a relatively low privacy risk while still being capable of applying differentiated protections in a privacy-preserving manner. Encouraging a "high privacy by default" approach without sufficient nuance risks incentivising entities to adopt unnecessarily restrictive data practices for all users, including adults, solely to avoid age assurance obligations, even where the marginal privacy benefit is limited.

For this reason, it is important that section 8(5) is clearly positioned through guidance and regulatory interpretation, neither as a narrow exception, nor as a default expectation across all services, but as a legitimate and proportionate compliance pathway to be used where appropriate, having regard to risk. Clear guidance is needed to ensure that entities can assess when the universal application of child protection measures is justified and when alternative, more targeted approaches better reflect the Code's objectives.

---

[10] In this regard, we note that the OAIC has published guidance on age assurance technologies: https://www.oaic.gov.au/news/media-centre/privacy-commissioner-publishes-new-guidance-to-ensure-proportionate-age-assurance-as-a-gateway-to-access-online-experiences; https://www.oaic.gov.au/__data/assets/pdf_file/0017/262043/OAIC-privacy-guidance-on-age-assurance-technologies.pdf

[11] 'Age Assurance Consumer Survey', https://www.infrastructure.gov.au/sites/default/files/documents/attachment-c-key-results-research-overview-adult-and-child-june2025.pdf

It would also be helpful for the OAIC to clarify the scope at which section 8(5) is intended to operate in practice. In particular, it is currently unclear whether a "high privacy by default" approach must be applied across an entire service, or whether it may be applied in a more targeted manner to specific features, functionalities or environments that are directed at, or likely to be accessed by, children (as discussed earlier). Without this clarification, there is a risk that entities apply child-level protections across all users (including adults) in order to rely on section 8(5), which may be disproportionate and not aligned with the Code's risk-based objectives.

For the video games industry, these considerations arise in the context of existing ARM Code obligations regulated by eSafety. R 18+ online games are subject to these requirements, which may involve age assurance measures to prevent unlawful access to age-restricted content, noting that the COP Code does not displace such obligations. While the ARM Codes include privacy considerations, they are primarily content-focused and pursue a different regulatory objective from the COP Code's emphasis on data minimisation and privacy-by-design.

In this context, and given the COP Code's focus on privacy and data processing harms, it is important to distinguish between direct data processing risks (e.g. profiling, retention or disclosure of personal information) and risks that may arise from how personal data is used within features or systems (e.g. chat or recommendation systems that may shape interactions or content exposure). It would be helpful to clarify whether, and to what extent, such feature-based risks are intended to inform the level of age assurance required.

Without clear and coordinated guidance on how section 8 of the COP Code is intended to operate alongside these ARM Code requirements, there is a risk that entities default to the most conservative compliance position across both regimes. In practice, this could lead to the deployment of intrusive age assurance measures across broader categories of users than is necessary, even where section 8(5) was intended to provide a proportionate privacy-preserving alternative.

We reiterate the importance of coordinated guidance across regulators in relation to age assurance requirements under the OSA. Clear alignment between the OAIC, eSafety and other relevant agencies is essential to ensure that entities are not compelled to adopt intrusive age assurance methods by default, where privacy-preserving and proportionate alternatives remain available.

We continue to support a regulatory framework that protects children while upholding strong privacy standards for all Australians. We welcome ongoing engagement with the OAIC as it refines its guidance and implementation approach.

Recommendations:

- Scope of "high privacy by default" approach:
  - OAIC guidance should affirm that a "high privacy by default" approach under section 8(5) of the Code is a legitimate and proportionate compliance pathway, rather than a narrow exception.

- It should also clarify the circumstances in which the universal application of child-level protections is the appropriate approach, especially where age assurance would introduce greater privacy or security risks than it would mitigate.
- In addition to age assurance, the OAIC should also clarify other obligations under the Code that would not apply under a "high privacy by default" approach, such as requirements to obtain child assent and parental verification.
- OAIC guidance should clarify the scope at which section 8(5) operates, including whether a "high privacy by default" approach may be applied to specific parts of a service that are directed at, or likely to be accessed by, children, rather than requiring service-wide application.

- Interaction with ARM Code obligations: OAIC guidance should address the interaction between section 8 of the COP Code and ARM Code obligations, to ensure entities are not driven to adopt intrusive age assurance methods by default, where privacy-preserving and proportionate alternatives are available. This should include clarification on whether, and to what extent, risks arising from data-enabled features or systems are intended to inform the level of age assurance required.
- International regulatory coherence: The OAIC should align the COP Code, to the greatest extent possible, with established international approaches (including the UK's AADC), including in relation to recognised age assurance approaches (e.g. adult account holder models) where these support privacy-preserving and proportionate outcomes.[12]

5. "Strictly necessary" and high privacy by default

Section 9 of the Code introduces "strictly necessary" and "high privacy by default" obligations in relation to the default design and configuration of online services accessed by children. These raise questions about how this should apply in practice, including how default settings can be implemented to support both privacy and children's best interests.

5.1. Core purpose of online games

In assessing what is "strictly necessary", it is important to distinguish between services where the personal data use is integral to service delivery and those where the ongoing collection and reuse of personal data are a core component of the service model.

For online games, many data uses (e.g. matchmaking, moderation and safety systems) are inherent to delivering the experience users reasonably expect. These differences are essential to how section 9 should apply in practice, including the design of default settings. These data uses are typically bounded to the gameplay context and do not involve broad secondary use or long-term repurposing, resulting in a different privacy-risk profile.

[12] For example, see: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/age-appropriate-design-a-code-of-practice-for-online-services/3-age-appropriate-application/

5.2. Gameplay-related features are strictly necessary

For online games, a range of features and data uses are essential to delivering the service a child signs up for and reasonably expects to receive (including those required at the point of account creation, and for ongoing access to and use of the service). These include:

- matchmaking and session management, which require identifiers, device information and connection data;
- in-game communication, which is often ephemeral, limited to the game environment, and necessary for teamwork, coordination and safety;
- moderation and safety systems, including reporting tools, automated detection of harmful behaviour and enforcement mechanisms; and
- anti-cheat and integrity systems, which protect children from unfair or harmful gameplay environments.

These functions are not "additional elements" in the sense contemplated by section 9 of the Code. They are integral to the core service and cannot be disabled by default without undermining the gameplay experience or compromising safety.

5.3. Lower-risk in-game communication

In-game communication is typically session-based, limited in audience and retention, and not designed to support persistent identity-based interaction or the long-term accumulation of personal data. For example, it can be:

- context-specific, occurring only within gameplay sessions;
- ephemeral, not stored or used to build behavioural profiles;
- restricted, often limited to team members or pre-defined groups; and
- safety-enhancing, enabling players to coordinate, receive warnings or report harmful behaviour.

For games, disabling communication by default would prevent children from participating meaningfully in cooperative or team-based play, and would reduce their ability to access safety tools. For these reasons, in-game communication should be recognised as part of the "strictly necessary" functionality for online games.

5.4. High privacy by default

We support the principle of high privacy by default. In some cases, overly restrictive defaults may work against the child's best interests when assessed holistically, including their rights to play, participation and safe social interaction. Defaults must be proportionate and aligned with the nature of the service. If defaults are set too restrictively for online games, they may:

- prevent children from participating in core gameplay;
- reduce access to safety features such as reporting tools;
- undermine moderation systems that rely on certain data to protect players; and
- create fragmented or degraded gameplay experiences.

A balanced approach is needed to ensure that privacy-protective defaults do not inadvertently increase risks to children or diminish the value of the service they have chosen to use.

5.5. Alignment with APP 11

Section 9 links the disabling of optional features to APP 11 requirements to destroy or de-identify personal information that is no longer needed. The video games industry already complies with APP 11, which provides a practical and proportionate framework for data minimisation.

However, it is important that section 9 does not inadvertently create obligations akin to a broad "right to erasure" that the Privacy Act itself does not contemplate, which would be technically infeasible in multiplayer environments. For example, deleting all traces of a player's historical interactions could affect the data of other players or undermine the integrity of shared game environments. APP 11 already provides an effective mechanism for ensuring that unnecessary data is not retained, and this should remain the governing standard.

We discuss this issue further below on the topic of requests to destroy personal information.

5.6. Alignment with "reasonably necessary" test under APPs

More broadly, the introduction of a "strictly necessary" standard raises questions about how it is intended to interact with the existing "reasonably necessary" test under the APPs. This test (e.g. under APP 3 on collection of solicited personal information) already provides a well-established and flexible framework for assessing what is reasonably necessary for an entity's functions or activities, taking into account context, risk and user expectations.

In the absence of clear guidance, it is unclear whether "strictly necessary" is intended to replace or operate alongside this existing standard in the context of children's personal information, creating a risk of inconsistent interpretation and unnecessary divergence from established privacy law principles, including those reflected in the Privacy Act framework.

5.7. Alignment with safety-by-design

The video games industry implements safety-by-design measures as a part of global best practice. These measures also reflect legal and regulatory expectations under Australia's online safety framework, including obligations relating to the prevention of child sexual exploitation, grooming, extortion, bullying and other harmful conduct.

In this context, certain uses of personal information (e.g. age-related signals, behavioural indicators and human moderation) may be necessary to identify and mitigate safety risks. We do not consider such measures to be inconsistent with the Code's privacy-by-default framework. Rather, where implemented to meet online safety obligations or address credible risk, they represent privacy-by-design approaches that are targeted, accountable and proportionate to the harms being addressed.

Importantly, these safety measures are typically deployed within a risk-based framework. In these circumstances, "strictly necessary" should be understood by reference to what is

required to meet safety obligations and protect children from harm, rather than construed narrowly as only what is essential to basic service delivery.

Clear guidance from the OAIC would assist entities in understanding how section 9 of the Code applies where personal information is processed primarily to meet online safety obligations or industry best practice. This includes clarity on how privacy-by-design principles apply to online safety systems that rely on proportionate signal detection and moderation to protect children and other users.

Recommendations:

- Sector-specific guidance: Given the unique characteristics of online games and the distinct ways in which children interact with them, the OAIC should develop sector-specific guidance on the application of section 9 of the Code to online games. This would ensure that the "strictly necessary" and "high privacy by default" obligations enhance children's privacy without unintentionally undermining gameplay functionality, safety or user experience.
- Secondary (yet necessary) purposes: The OAIC should also publish comprehensive guidance clarifying the categories of secondary (yet necessary) purposes that are consistent with the best interests of the child and permitted under a "strictly necessary" standard. Without limitation, this guidance should include a non-exhaustive list of examples covering: (1) product improvement and reliability (e.g. diagnostics, error reporting, bug-fixing); (2) user-experience research and design improvement using aggregated or de-identified data; (3) safety, integrity and trust-and-safety operations (e.g. detection of harmful conduct, grooming, harassment and content moderation); (4) security, fraud and abuse prevention; and (5) legal and regulatory compliance.
- Alignment with APPs: The OAIC should also clarify how the "strictly necessary" standard is intended to operate alongside the existing "reasonably necessary" test under the APPs, including any relevant child-specific considerations that inform this assessment.

6. Best interests of the child

The Explanatory Statement appropriately grounds the "best interests of the child" test in Article 3 of the UN Convention on the Rights of the Child (UNCRC), and we welcome the OAIC's recognition that this concept should be applied holistically. However, the Statement frames the concept largely through a privacy-risk lens, including sections 10 and 11 of the Code. This does not fully reflect the breadth of rights protected under the UNCRC, nor the practical realities of interactive entertainment services, including online games.

6.1. A holistic interpretation of "best interests"

The UNCRC makes clear that a child's best interests encompass not only protection from harm, but also their positive rights, including:

- recognition of children's evolving capacities (Article 5);

- the right to freedom of association (Article 15);
- the right to access age-appropriate information (Article 17);
- the right to participate in social, artistic and cultural life (Articles 30 and 31); and
- the right to play and leisure (Article 31).

Online games play an increasingly vital role in children's play, creativity, socialisation and digital literacy. Overly restrictive regulation may unintentionally limit these opportunities. The best interests test must therefore be applied in a balanced and evidence-based manner, recognising that children benefit from safe and age-appropriate opportunities to engage in interactive entertainment.

6.2. Commercial interests and children's interests are not inherently incompatible

We support the Explanatory Statement's acknowledgement that an entity's commercial interests are not, by definition, inconsistent with the best interests of the child. Game developers rely on commercial models that enable ongoing content updates, safety features and parental control tools. A well-designed commercial model can support, rather than detract from, children's well-being.

6.3. Context matters: online games differ from higher-risk services

As outlined in the Explanatory Statement, the application of section 10 of the Code requires an assessment that takes into account the likely impacts of data handling practices on children. Online games differ materially from higher-risk online services in their design, communication patterns, risk profile and modes of interaction. These contextual differences between online games and other services should inform how the best interests test is applied in practice.

This is particularly important in the context of low-risk, curated game environments, where content is structured, moderated and subject to established safeguards such as classification systems and parental controls. In these environments, the application of the "best interests of the child" test should reflect the relatively lower privacy and safety risk profile, and avoid defaulting to restrictive interpretations that may unnecessarily limit children's ability to engage in age-appropriate play.

6.4. Proportionality and evolving capacities

Section 10 of the Code requires entities to consider the evolving capacities of children and the likely impacts of data practices. To give effect to these principles, the Code should adopt a proportionate, risk-based approach that takes into account:

- the likelihood and extent of children's access;
- the nature and sensitivity of data collected;
- the provider's relationship with child users;
- the actual privacy risks posed; and
- existing safeguards and parental empowerment tools.

Without proportionality, the Code risks imposing burdens that do not meaningfully advance children's interests and may reduce their access to safe and age-appropriate digital play.

Recommendations:

- UNCRC considerations: To ensure the "best interests of the child" test is applied consistently with the UNCRC, the following note should be added to sections 10 and 11 of the Code:

  Note: When assessing the best interests of the child, entities should have regard to the full range of the child's rights under the UNCRC and balance those rights holistically. This includes considering rights that may be indirectly affected, such as the child's right to play, leisure, and participation in social, cultural and recreational activities.

- OAIC guidance: The OAIC should also provide guidance on how the best interests test is to be applied in practice across different service types, including low-risk, curated environments such as online games, to ensure the test is applied in a proportionate and context-sensitive manner.

7. Bundled consent

Section 14(3)(b) of the Code prohibits bundled consent, requiring that consent be sought separately for each distinct collection, use or disclosure of personal information. In the games sector, user consent can be obtained through a single onboarding process at account creation or first launch, typically embedded within terms of service, privacy notices or a unified consent screen. This process can address multiple interconnected purposes, such as account creation, gameplay functionality, safety and moderation systems, analytics, personalisation and optional marketing communications.

Applying section 14(3)(b) in a game context would require a fundamental redesign of onboarding and in-game consent user experiences. In practice, a child (or their parent or carer) may be required to encounter and respond to multiple separate consent requests, including for:

- core account and identity information necessary to enable gameplay;
- safety, moderation and anti-cheat systems;
- gameplay analytics and performance monitoring;
- non-core personalisation or optional feature-based enhancements (e.g. customisation or gameplay-related personalisation); and
- optional marketing, advertising or cross-promotion activities.

It is also important to distinguish between personal information that is collected and used as part of delivering the core service requested by the user (e.g. account creation, authentication, gameplay functionality, safety systems and anti-cheat mechanisms), and non-essential secondary purposes. Where personal information processing is integral to the primary service and reasonably expected by users, requiring separate, unbundled consent may not be appropriate and could undermine usability and safety outcomes.

Conversely, unbundled consent is more appropriately directed toward optional uses (e.g. marketing or third-party data sharing). Certain features (e.g. safety monitoring, moderation and anti-cheat systems) are fundamental to maintaining safe environments for children and should not be treated as optional choices that can be disabled through consent mechanisms.

Without clear guidance, there is a risk that consent processes become overly complex or friction-heavy, particularly for child users. Multiple consent screens presented at account creation may result in users disengaging, mechanically clicking through notices (i.e. consent fatigue), or abandoning the onboarding process altogether, undermining the objective of meaningful and informed consent. This risk is amplified in child-directed contexts, where comprehension, attention span and parental involvement vary significantly.

Recommendations:

The OAIC should clarify how entities can design consent processes that comply with section 14(3)(b) of the Code regarding bundled consent, while remaining child-appropriate and effective. This should include guidance on:

- Distinguishing between personal information processing that is integral to delivering the core service requested by the user (which should not require separate unbundled consent), and optional purposes (where unbundled consent may be appropriate).
- Examples of acceptable consent approaches, such as a single layered onboarding consent process that clearly distinguishes core gameplay and safety-related data practices from optional features, with just-in-time consent prompts used only where a materially new purpose arises.

8. 12-month consent period

Section 15(4) of the Code proposes that consent lapses after 12 months, requiring entities to obtain fresh consent in order to continue handling a child's personal information. In the games sector, player relationships (including child and teen users) are often long running. Users commonly maintain accounts for many years on online game services. This account longevity reflects the nature of games as ongoing services rather than short-term or transactional digital interactions.

A mandatory annual re-consent requirement would have significant operational and user-experience implications. From a systems perspective, entities would need to repeatedly interrupt gameplay or platform access to seek renewed consent. From a legal perspective, failure to obtain renewal consent could technically require cessation of data handling that is integral to core service delivery, including account authentication, entitlement management, safety and moderation systems. There is also a risk that frequent re-consent prompts become routine or disregarded by users, diminishing (rather than enhancing) meaningful engagement with consent notices. This issue is further compounded with respect to bundled consent, discussed above.

The proposed 12-month window appears to be drawn from other online service contexts and does not account for the nuance in the lifecycle of a game or a gaming platform

relationship, particularly where services are stable, low-risk and well-understood by users over time.

Recommendations:

- Rethinking fixed annual consent-expiry rule: Section 15(4) of the Code should be revisited. A fixed annual consent-expiry rule risks imposing a significant ongoing administrative burden on families, contributing to consent fatigue and reducing the quality of consent over time.
- Flexible risk-based approach: The OAIC should adopt a more flexible risk-based approach to consent renewal. In particular, where data practices are stable, low-risk and consistent with users' reasonable expectations, consent should remain valid beyond a fixed 12-month period and should not require routine renewal in the absence of a material change to data practices or user expectations.
- Meaningful engagement: A more proportionate approach would prioritise meaningful engagement – for example, through periodic reminders to parents and carers about existing consents, combined with renewed express consent at key transition points (e.g. when a child reaches an age where decision-making responsibility begins to shift, and again at adulthood). This approach would better recognise the persistent, long-running nature of game environments, where repeated annual renewal may be unnecessary or counterproductive where relevant data practices have not materially changed.

9. Assent requirements for children under 15

We support the objective of involving children in decisions about their personal information and enhancing privacy literacy. The video games industry has long invested in child-specific accounts, parental control apps, customisable privacy settings, and controls over data sharing, communication and account visibility. These tools already support informed engagement by both parents and children, and we recognise the value of ensuring that children understand when their information is being collected or used for specific purposes.

However, the implementation of section 20 of the Code (requiring assent of a child under 15 years in certain circumstances) must remain proportionate, technically feasible and compatible with the unique characteristics of online games (as outlined above). The proposed two-step assent process (i.e. requiring a child to assent to (1) the handling of their information, and (2) the entity contacting their parent or carer) risks introducing unnecessary friction, particularly in immersive gameplay environments where interruptions can significantly disrupt the user experience.

This approach also represents a departure from comparable international frameworks such as the UK's AADC, which allow for parental involvement without mandating a comparable dual assent and consent model. This may therefore introduce additional compliance burden and user friction for services operating across jurisdictions.

For online game services, a person with parental responsibility has the ability to establish a child-specific account and enable parental control tools that govern the relevant collection, use or disclosure of information. While the Explanatory Statement clarifies that a child's assent is not required where parental consent has already been provided for a specific purpose, in practice this principle may be difficult to operationalise in complex online game environments. In such circumstances, children may still be presented with additional mid-game assent prompts (i.e. during gameplay), such as the entity contacting the same parent or carer, which may be redundant and unnecessary. This is especially true where parental controls already reflect the parents' or carers' informed choices about how their child's information should be handled.

More broadly, the design of assent and parental verification requirements should avoid creating incentives for increased data collection or unnecessary identification of children and parents. In particular, highly prescriptive consent and verification flows may encourage the collection of additional contact details or identifiers that would not otherwise be required, potentially undermining data minimisation and increasing privacy risk.

There is also a risk that complex onboarding processes lead parents or carers to rely on adult accounts rather than child-specific accounts designed with appropriate safeguards, thereby producing outcomes that are contrary to the policy intent. In this context, it is also unclear whether the Code would, in effect, create a requirement for parental consent under section 13 as a condition of account creation or access for users under 15, which may extend beyond what is contemplated by the Privacy Act and warrants clarification.

We therefore encourage the OAIC to ensure that assent requirements are applied flexibly and proportionately, recognising the lower privacy risk profile of most online games and the existing safeguards provided through parental control systems. Where assent is required, entities should be permitted to implement mechanisms that align with the game's interface and parental control tools, and should not be required for personal information processing that is integral to the delivery of the core service or necessary to maintain safety and integrity within the service.

Recommendations:

- Proportionate and flexible approach: The OAIC should ensure that assent requirements are implemented in a proportionate and flexible manner that reflects the unique characteristics of online games. To support effective compliance (particularly for smaller businesses), the OAIC should provide clear practical guidance on age-appropriate notices that do not disrupt gameplay. This will help ensure assent mechanisms enhance children's understanding without imposing unnecessary technical burdens.
- Redundant assent: To avoid redundant or disruptive assent processes in circumstances where parental consent has already been clearly established, while preserving the OAIC's intent to involve children in meaningful decisions, section 20 of the Code should be amended (or clarified in guidance), inserting a new subsection, as follows:

Assent is not required where a person with parental responsibility has already enabled functional parental control tools that govern the relevant collection, use or disclosure of the child's personal information.

- Scope of assent obligations: The OAIC should clarify the scope of the assent requirement, including that assent is not required for personal information processing that is integral to the provision of the core service or necessary for safety, integrity and compliance purposes, and should be directed toward higher-risk secondary uses of personal information.
- Reframing assent as age-appropriate notice: Alternatively, the OAIC should consider reframing the child assent requirement as an obligation to provide an age-appropriate notice to the child. Requiring both an active assent step from the child and verified legal consent from a parent or carer creates a confusing and burdensome onboarding experience for families, with a real risk of bottlenecking sign-up flows and pushing families toward less child-safe alternatives. This approach would still support the objective of promoting children's awareness and understanding of personal information handling as they grow.

10. Cumulative impact of consent and verification requirements

While we have separately addressed individual consent-related provisions of the Code, it is important to consider their cumulative effect in practice. Each requirement may be understandable when viewed in isolation. However, their interaction creates a compliance architecture that is significantly more demanding than any single provision suggests.

In a single act of data collection or ongoing account use within a game, an entity may be required to:

- obtain parental consent for users under 15 (section 13);
- avoid bundled consent, by ensuring consent is sought for each distinct collection, use or disclosure of personal information (section 14);
- ensure that each consent lapses and is renewed at least every 12 months (section 15); and
- in certain circumstances, seek child assent and contact a parent or carer for users under 15 (section 20).

For each of these consent and assent requirements, the Code also requires the provision of age-appropriate notices at relevant stages of the process.

The interaction between these requirements materially changes what compliance looks like for game services. Rather than a single consent decision supported by clear, intelligible information, entities may be required to design layered, recurring and highly segmented consent and verification processes that operate across onboarding, gameplay, account management and parental interfaces. In practice, this complexity poses a real risk that users (including both children and parents or carers) are faced with a barrage of prompts and notices that are difficult to navigate, easy to accept mechanically, or increasingly ignored over time.

Ironically, the cumulative effect of these safeguards may undermine the policy objective they are intended to serve, and risk extending beyond what is contemplated under the existing Privacy Act framework. Where consent mechanisms become overly complex or repetitive, there is a heightened risk that neither children nor parents/carers meaningfully engage with them, reducing transparency rather than enhancing it.

Recommendations:

- Holistic approach: The OAIC should take a holistic systems-level consideration of how the Code's consent and parental verification requirements operate together in practice, particularly in long-running interactive services such as games.
- OAIC guidance:
  - Additional OAIC guidance would assist entities to design consent architectures that are coherent, proportionate and genuinely supportive of informed decision-making, rather than inadvertently encouraging consent fatigue.
  - In particular, further OAIC guidance on parental verification is required. The potential verification methods suggested in the Code and Explanatory Statement (e.g. email contact, tokens, video calls with customer service agents, government identification) involve differing privacy, accessibility and reliability trade-offs, and may not always provide a consistent or proportionate means of establishing parental responsibility in practice.
  - To provide greater certainty for industry and a consistent experience for families, the OAIC should: (1) publish detailed guidance on what constitutes acceptable verification of parental responsibility across a range of low-, medium- and high-privacy-risk scenarios; and (2) consider adopting a safe-harbour approach that identifies specific verification methods which, if used in good faith, may be treated as compliant. Such an approach could be modelled on the U.S. Children's Online Privacy Protection Act (COPPA), which includes FTC-recognised verification methods, adapted for the Australian context.

11. Transparency and child-friendly privacy policies

We support the intent of section 23 of the Code to ensure that privacy information is accessible and understandable for children. Privacy regulation should take a clear yet flexible principles-based approach, avoiding overly prescriptive rules that could stymie innovation. This principle is directly relevant to the design and presentation of child-friendly privacy policies.

As discussed above, online games differ substantially from other online services in how information is conveyed to users. These unique characteristics of online games mean that privacy information must be delivered in ways that respect the aesthetic and technical constraints of game environments.

11.1. Flexibility in the use of non-text material

Section 23(3)(c) of the Code requires that, where appropriate, child-friendly privacy policies incorporate non-text material such as icons, images, diagrams, animations or short videos. We support the principle of making privacy information more engaging for children. However, the Code should avoid "a one-size-fits-all model" and instead adopt a proportionate and risk-based approach, and therefore this requirement must be applied flexibly.

Game interfaces are highly stylised and optimised for gameplay. Mandating specific visual formats may impose unnecessary technical burdens or disrupt the user experience. Entities should retain the ability to determine how best to present privacy information in their user interface design.

Recommendation:

To ensure the section 23 requirement is workable for diverse game environments, while preserving the OAIC's intent, the following amendment should be made to section 23(3)(c):

> *(c) where appropriate, incorporate non-text material to engage children effectively* ***in a manner that is compatible with the visual design, user experience and technical constraints of the service, and does not unreasonably disrupt its operation***

11.2. Prominence, clarity and accessibility

We support the requirement that privacy policies be easy to find and written in clear and simple language. This aligns with the industry's longstanding commitment to transparency and digital literacy, including the use of child-specific accounts and parental control tools, as well as a proactive approach to education and empowering parents and children.

However, section 23(4) of the Code (requiring privacy policies to be placed in a prominent position and presented in an accessible manner) should recognise that "prominent position" may look different in a game environment than in a traditional app or website. Flexibility is essential to ensure that prominence does not conflict with gameplay or user experience.

There is also a need to strike an appropriate balance between the Code's requirements for detailed transparency and the expectation that child-friendly privacy policies avoid complex or legalistic language. While simplified age-appropriate explanations are important, overly restrictive interpretations may make it difficult to accurately convey necessary information, particularly where legal consent must be obtained from a parent or carer.

In practice, a layered approach is more effective, combining concise child-friendly summaries with access to more detailed explanations where appropriate. Consistent with the UK's AADC, this approach supports flexibility in how privacy information is structured and may remove the need to adopt a wholly separate child-specific privacy policy (see section 23(2) of the COP Code), particularly where layered and contextual disclosures are effective. It also reflects how families engage with online services, where younger children

often rely on parents or carers to review and understand more detailed privacy information on their behalf.

While the Code does not expressly require separate privacy policies, the requirement to provide child-friendly, age-appropriate information may result in multiple forms of privacy disclosures (e.g. simplified child-facing notices alongside more detailed legal disclosures). Clarification would therefore be helpful as to how these are intended to operate together, including which version is relied upon (e.g. in the event of resolving inconsistencies or disputes).

Recommendations:

- Child-friendly language requirements: The detailed disclosure requirements in Division 3 of the Code may be difficult to reconcile with the concurrent obligation that child-friendly privacy notices must not include complex or technical expressions or terminology drawn from specialist industry or legal language. To support effective implementation, child-friendly language requirements should be limited to outward-facing notices and consent flows directed at children, and entities should be permitted to adopt a layered framework combining simplified, accessible summaries for children with more detailed explanations where appropriate – including where legal consent must be obtained from a parent or carer. OAIC guidance should include illustrative examples of acceptable child-friendly notices and clarify what constitutes "legal language" for this purpose.
- Layered privacy disclosures:
  - Consistent with this approach, OAIC guidance should clarify that entities are not required to adopt a wholly separate child-specific privacy policy in all cases, particularly where layered and contextual disclosures are effective.
  - OAIC guidance should clarify how layered or multiple forms of privacy disclosures are intended to operate together in practice, including which version to rely upon in the event of resolving inconsistencies or disputes.

11.3. Pseudonymity and anonymity

Section 23(6) requires child-friendly privacy policies to explain options for pseudonymity and anonymity. This aligns closely with existing industry practice. The use of pseudonymous gamer tags is already a core privacy and safety feature in online games, forming part of broader controls over account visibility and data sharing. The Code should recognise that pseudonymity is already a default norm in games and allow privacy policies to reflect this context.

Recommendation:

OAIC sector-specific guidance should be provided on the application of section 23 of the Code on transparency obligations for child-friendly privacy policies, including with respect to prominent position, non-text material, and pseudonymity and anonymity.

12. Cross-border disclosures

Section 26 of the Code requires express, informed and age-appropriate consent before personal information is disclosed to an overseas recipient, as a condition of relying on the exemption in APP 8.2(b)(i) of the Privacy Act.

Online games rely on offshore infrastructure and third-party services as an inherent part of routine service delivery. Many of these services process data (including personal information) across multiple jurisdictions outside Australia. In practice, translating complex global infrastructure arrangements into express, informed and age-appropriate consent mechanisms presents substantial design and comprehension challenges, particularly for younger users.

The requirement to obtain express consent for overseas disclosures also raises significant implementation questions for game developers. Documenting and disclosing each overseas data recipient and processing location would require a level of infrastructure visibility and control that studios (particularly smaller ones) do not have, especially where services are delivered through third parties such as global platforms.

These challenges are especially acute for small and mid-sized studios that rely on global service providers and cannot select or influence specific server locations. In such cases, individual developers may be contractually and technically removed from the underlying infrastructure decisions that determine where data is processed.

Without clear guidance, there is a risk that the consent requirement in section 26 becomes disproportionately burdensome and unrealistic, leading to either overly complex consent disclosures that are unlikely to be meaningfully understood by children, or conservative compliance approaches that restrict access to globally hosted services. Providing guidance would support the policy objective of transparency while recognising the shared-infrastructure reality of modern game development and distribution.

Recommendations:

- Disclosure for online games: The OAIC should clarify, for the purposes of section 26 of the Code, what constitutes adequate, age-appropriate disclosure of overseas data flows in the context of online games, especially where individual developers lack direct control over, or visibility into, the specific overseas infrastructure processing personal information. Consideration should be given to the suitability of high-level disclosure that personal information may be processed overseas, clear explanation of the purposes involved, and assurance that appropriate safeguards apply regardless of processing location.
- Pseudonymised, de-identified or anonymised personal information: Additionally, the OAIC should clarify how this requirement applies where personal information is processed in a pseudonymised, de-identified or anonymised form. In such lower privacy risk cases, consideration should be given to whether high-level disclosure through privacy policies may be sufficient, without requiring separate age-appropriate consent for each overseas disclosure.

13. Automated decision-making and access to information

We support the objective of enhancing transparency and enabling children and parents/carers to understand how personal information is handled. However, the implementation of section 28 of the Code must remain proportionate and reflect the comparatively low-risk profile of most online games. Automated decision-making (ADM) in games is generally limited to real-time or session-based gameplay functions, such as matchmaking or difficulty balancing. This differs from profiling practices used in services where personal data is aggregated over time to infer preferences or influence behaviour across contexts.

It is therefore important that the Code explicitly recognises the low-risk nuance of ADM in games. While we support the principle of providing meaningful information to children and parents/carers, entities should not be required to disclose proprietary algorithms, trade secrets or game mechanics that are essential to service integrity, competitive fairness or anti-cheat protections. Regulatory measures should avoid overly prescriptive rules that could stymie innovation and should not adopt a "one-size-fits-all model". Requiring detailed disclosure of ADM logic risks undermining core gameplay systems without delivering meaningful privacy benefits.

Section 28 should instead adopt a proportionate risk-based approach that allows entities to provide clear age-appropriate explanations of the context and consequences of ADM, without requiring disclosure of sensitive technical detail. This approach aligns with the Explanatory Statement's acknowledgement that entities are not expected to provide full technical specifications, and it ensures that transparency obligations remain workable for game developers of all sizes.

Recommendations:

- Proportionate risk-based approach: The OAIC should adopt a proportionate risk-based approach to ADM disclosures under section 28 of the Code, and clarify that entities are not required to disclose proprietary algorithms or trade secrets.
- Sector-specific guidance: OAIC sector-specific guidance should support smaller studios in providing age-appropriate explanations of ADM without compromising gameplay integrity or imposing unnecessary technical burdens.
- Amendment to Code: To provide additional certainty and ensure the OAIC's intent is implemented consistently, section 28(2)(g) should be amended as follows:

  whether there is any automated decision-making, including profiling, relating to the personal information and, if so, clear and meaningful information about the context of such decisions, including the logic involved ***(excluding proprietary algorithms or trade secrets essential to service integrity)*** *and the consequences of making them.*

14. Consent design and direct marketing opt-out

In the context of consent design and marketing choices, we support the objective of ensuring that children can make informed and voluntary decisions about the handling of their personal information. In the video games industry, this objective is commonly

supported through child-specific accounts and parental control tools, enabling customisable privacy settings and controls over data sharing, communication and account visibility. These features already promote transparency, shape how consent and choices are presented, and support informed engagement by both parents/carers and children.

14.1. Consent must not be obtained by coercion

We agree that consent should be obtained through lawful and fair means, and should not involve genuinely manipulative practices that are misleading or deceptive, as intended under section 21 of the Code. While the Explanatory Statement uses a game-based example to illustrate "confirm-shaming", such practices should not be taken as representative of online games generally, where consent processes are typically functional and contextual, tied to gameplay or platform-level parental controls.

At the same time, it is important that the Code does not inadvertently capture creative or thematic in-game text that forms part of a game's narrative or artistic style. Games often use humour, stylised language or character-driven dialogue to maintain immersion. These elements are not intended to influence privacy decisions and should not be treated as "nudge techniques".

To avoid regulatory overreach, the Code should adopt a clear and narrow definition of "nudge techniques" that focuses on genuinely manipulative practices that are misleading or deceptive. This would avoid capturing legitimate, innocuous, reasonable or generally accepted gameplay design and commercial practices.

Recommendations:

- Proportionate risk-based approach: The OAIC should ensure that consent requirements under section 21 of the Code are applied in a proportionate and flexible manner that reflects the unique characteristics of online games and avoids assumptions based on high-risk service models.
- Legitimate practices: In particular, the OAIC should adopt a clear and narrow definition of "nudge techniques" that focuses on genuinely manipulative practices that are misleading or deceptive, and does not inadvertently capture creative or thematic in-game content, or legitimate, innocuous, reasonable or generally accepted gameplay design and commercial practices.
- Amendment to Code: To ensure that legitimate artistic expression and commercial practices are not inadvertently restricted, while preserving the OAIC's intent, the following note should be added to section 21:

  Note: This section does not capture creative or thematic content designed to maintain the immersive narrative of an interactive service, or legitimate, innocuous, reasonable or generally accepted gameplay design choices and in-game commercial practices, provided they are not misleading or deceptive.

14.2. Opting out of direct marketing

We support the requirement for entities to provide simple and accessible means for children to opt out of direct marketing under section 29 of the Code. In-game communications are generally limited, contextual and designed to support gameplay, rather than to promote unrelated products or services. Where direct marketing does occur, it is typically delivered through platform-level systems that already provide clear opt-out mechanisms and parental controls.

It is also important to consider the interaction between section 29 and the best interests of the child framework in sections 10 and 11. A significant proportion of games accessed by children (particularly on mobile devices) operate under an advertising-supported free-to-play model. This model plays a legitimate and important role in enabling children to access games without upfront purchase costs, including for families who may be unable to afford premium titles or ongoing subscriptions.

Advertising within games typically differs materially from other online services. It would also be useful to clarify the scope of "direct marketing" in this context, including whether non-personalised communications (e.g. updates, new content releases or seasonal features within the same game) are intended to fall within the definition.

In-game advertising is generally contextual, confined to the game environment, and does not typically rely on tracking or aggregation of personal data across multiple services. As a result, the privacy risks associated with such advertising differ materially from models that rely on extensive profiling or secondary data use, which should be taken into account when applying section 29.

Contextual advertising of this kind also delivers direct user benefits. For example, it ensures promotional content is relevant to a user's general location, so that a child is not served advertising for events or offers unavailable to them. It should therefore be recognised as a low-risk processing activity that supports the sustainability of free-to-play services and enables relevant, appropriate experiences for users including children, in full alignment with privacy-by-design principles.

Read together, these provisions on direct marketing to children under 15 and the application of the best interests test risk producing disproportionate outcomes if applied as a blanket prohibition, without regard to the nature of the service or the advertising involved. In some cases, the best interests of the child may be served by the continued availability of well-moderated age-appropriate free-to-play games that rely on limited contextual advertising to remain viable.

The implementation of section 29 should therefore remain proportionate and flexible. The Code should avoid overly prescriptive rules that assume high-risk advertising models or adopt a one-size-fits-all approach across different categories of online services. This is particularly important for smaller businesses, which may lack the resources of larger platforms.

Recommendations:

- Legitimate advertising-supported free-to-play models: The OAIC should ensure that section 29 of the Code is interpreted and applied in a manner that recognises the legitimate role of advertising-supported free-to-play models in enabling children's access to games, particularly where advertising is contextual, age-appropriate and confined to the game environment, and that application of the provision remains proportionate to the privacy risks.
- Best interests test: The OAIC should clarify the operation of section 29 in conjunction with the best interests test, including through guidance on how compliant direct marketing opt-out mechanisms can be implemented within immersive game environments in a manner that is practicable and achievable for providers of different sizes.
- Scope and application: The OAIC should provide further guidance on the scope and application of "direct marketing" under section 29, including clarifying whether non-personalised communications relating to gameplay or service updates fall within its scope. Guidance should also confirm that entities, which do not engage in targeted or profiling-based advertising to children, are not subject to unnecessary or additional opt-out requirements, and should recognise that parents or carers may appropriately manage communications preferences on behalf of younger children.

15. Requests to destroy personal information

We support the objective of giving children and parents/carers meaningful control over their personal information. As discussed above, the video games industry already complies with APP 11, which provides a practical and proportionate framework for data minimisation and ensures that unnecessary personal information is not retained.

However, section 32 of the Code (requiring entities to destroy personal information about a child upon request) must recognise the unique technical characteristics of online games. Unlike online services where personal data is primarily individualised, online games often operate within shared real-time environments where player data is inherently relational. In these environments, not all gameplay data operates as standalone account information that can be removed without consequence.

In particular, certain categories of player-related data (e.g. achievements, ranked history, leaderboards, tournament results, and participation in persistent online worlds) are inherently relational. This information is often visible to, and directly affects, the experience and records of other players.

For example, deleting a player's data may alter shared leaderboard rankings that other players have legitimately earned through competition, or distort persistent game-world states to which many players have contributed. Similarly, competitive match and tournament records cannot be removed for one participant without affecting the integrity of other players' performance histories.

In these circumstances, the destruction of such data is not merely operationally complex, but often technically infeasible without undermining fairness, historical accuracy and the integrity of the shared game environment. While such data may contain personal information, it also forms part of a multiparty system of records that cannot be surgically removed on an individual basis.

It is also important to recognise that, in online game environments, it is not unusual for children to access services through family or household account structures controlled by a parent or carer. In these contexts, rights relating to personal information (including access, correction and destruction) are typically exercised through the adult account holder and implemented via profile-level tools, rather than through separate child-facing processes. This approach is also broadly consistent with comparable international frameworks, including the UK's AADC and U.S. COPPA, which recognise the role of parents or carers in supporting and exercising children's privacy rights.

For these reasons, it is essential that section 32 be applied in a proportionate and technically feasible manner. The Code currently states that de-identification is not sufficient to meet a destruction request. This position departs from the approach taken under APP 11 of the Privacy Act, as interpreted by the OAIC, which expressly recognises de-identification as a valid alternative to destruction where re-identification is not reasonably possible.[13]

Recognising de-identification as a valid alternative to destruction requests, reflects both the technical realities of online games and the risk-based approach underpinning APP 11. This also avoids elevating form over substance in circumstances where re-identification risk has been eliminated. It would enable entities to uphold children's privacy rights while preserving safety, fairness, and the stability of multiplayer and persistent game environments.

Consideration should also be given to the appropriate safeguards around the exercise of requests. This includes safeguards to ensure that entities are not subject to volumes of unreasonable requests (e.g. frivolous, vexatious or malicious), which could create disproportionate operational burden at the expense of genuine requests.

Recommendations:

- Proportionate and technically feasible approach: The OAIC should ensure that section 32 of the Code is applied in a proportionate and technically feasible manner, allowing for de-identification as a valid alternative to destruction, consistent with APP 11 and existing OAIC guidance, and provide sector-specific guidance on its application to online games.
- De-identification: Section 32(2) should be amended to allow de-identification as an alternative to destruction, recognising that this is a privacy-protective and technically

[13] See: https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/handling-personal-information/de-identification-and-the-privacy-act

feasible approach for certain categories of shared gameplay and game-state data in complex shared game environments:

If a request is made, the entity must destroy ***or de-identify*** *the information****, in accordance with APP 11***.

- Limited exceptions: The OAIC should consider introducing a limited exception to destruction under section 32 for personal information reasonably required to support cyber security, fraud prevention and safety-related functions. Certain categories of data may be necessary to maintain safe and secure environments for children and other users.
- Family and household contexts: The OAIC should clarify how rights relating to personal information, including requests for destruction, are intended to operate in family or household account contexts. This should include recognising that such rights may be appropriately exercised by a parent or carer and implemented through existing profile-level tools rather than requiring separate child-facing processes.
- Safeguards against unreasonable requests: The OAIC should consider appropriate safeguards around the exercise of requests, including to ensure that entities are not required to respond to volumes of unreasonable requests (e.g. frivolous, vexatious or malicious), while preserving access for genuine requests.

16. Parental controls and geolocation monitoring

We support the intent of section 33 of the Code to ensure that children are aware when parental control tools or geolocation-sharing mechanisms are active. As outlined in our submission, the video games industry has long invested in child-specific accounts and parental control apps, enabling customisable privacy settings, and controls over data sharing, communication and account visibility. These tools play a key role in supporting parents and carers and promoting safe online experiences for children, and we welcome the recognition of their value in the Explanatory Statement.

At the same time, it is essential that the implementation of section 33 remains proportionate, flexible and compatible with the unique characteristics of online games. This is particularly relevant for online games, where interfaces are highly stylised, immersive and optimised for uninterrupted gameplay. Notifications must therefore be designed in ways that are age-appropriate and effective, while also minimising disruption to the primary use of the service.

Sections 33(1) and 33(2) require entities to notify children when parental controls or geolocation-sharing mechanisms are active. We support the principle of transparency, noting that such notifications can help children understand how their information is used and support the development of digital literacy. However, the Code should allow flexibility in how these notifications are delivered. In gameplay environments, persistent on-screen indicators may not be appropriate or technically feasible. In these cases, alternative approaches that are less disruptive but offer similar outcomes may be more effective.

Sections 33(3) and 33(4) require that notifications be age-appropriate, timely and easily accessible. These principles align with existing industry practice. As noted in our submission, in-game features are typically confined to on-platform interactions, and are often ephemeral, limited in scope and designed to enhance the gameplay experience. The same design philosophy can be applied to notifications: they should be clear and understandable to children, while also respecting the flow of gameplay and the technical constraints of the service.

Recommendations:

- Sector-specific guidance: The OAIC should provide sector-specific guidance on the application of section 33 of the Code in the context of online games. This should cover how notification requirements can be implemented in a manner that is compatible with game interfaces. Clear guidance would support consistent implementation while ensuring transparency obligations do not inadvertently disrupt gameplay or impose unnecessary technical burdens.
- Minimising disruption: To ensure notification requirements are workable across diverse game environments and compatible with the immersive nature of gameplay, we recommend that section 33(3)(c) be amended as follows:

  The notification must: … be given in a way that reasonably ensures the child is aware of the use of the mechanism ***while minimising disruption to the primary use of the service****.*
- Family and household contexts: The OAIC should clarify how notification requirements under section 33 apply in family or household account contexts, including where parental controls are enabled and children are using services under parental supervision. Guidance should recognise that additional child-facing notifications may not be necessary where they would be redundant or unduly disruptive.
- Scope of geolocation data: The OAIC should also clarify the scope of "geolocation" for the purposes of section 33, including whether this is intended to capture only precise geolocation tracking, as opposed to incidental or functional data (e.g. IP addresses) processed as part of standard service delivery.

17. Child-friendly information and complaints mechanisms

Sections 35 and 36 of the Code require entities to provide clear age-appropriate information about children's privacy rights, and to establish child-friendly inquiry and complaints processes.

While the objective of ensuring accessible and child-centred privacy information is supported, these requirements raise significant practical considerations for the games industry, particularly for smaller studios.

Requiring studios to design, implement and maintain a standalone child-specific inquiry and complaints process (separate from general customer support) risks imposing a disproportionate administrative burden in the absence of clear guidance on scalability or

proportionality. This burden is amplified where studios have limited direct interaction with users and rely on platform-managed identity, messaging and reporting systems.

Section 36(4) also requires a complaints and inquiries process that caters for anonymous complaints, presenting particular challenges in this context. For example, where a studio has no direct relationship with a child user and interactions are mediated entirely through a platform's account and identity systems, it may not be technically feasible for the studio to authenticate, receive, and act on anonymous complaints independently of the platform.

Without clear guidance, compliance efforts risk focusing on duplicative or formalistic processes rather than on mechanisms that are genuinely accessible and effective for children. For instance, recognising platform-level systems as a valid means of compliance in appropriate circumstances would support the policy objective of child accessibility while reflecting the structural realities of how games are distributed and supported.

Recommendation:

The OAIC should clarify what constitutes a proportionate and compliant child-friendly inquiry and complaints mechanism for the purposes of sections 35 and 36 of the Code, having regard to the size, resources and business models of different game developers.

18. Mandatory privacy impact assessments

Sections 38 and 39 of the Code impose mandatory privacy impact assessments (PIAs) for high privacy risk activities relating to services likely to be accessed by children, including prior to the launch of new services or material changes to data handling practices, alongside a requirement to maintain a public register of PIAs.

In a game development context, PIAs may reasonably be triggered by game releases, new game modes, features or mechanics, or live service updates that involve changes to the collection, use or disclosure of children's personal information.

For studios that release multiple games or substantial updates each year, this creates a recurring pre-launch compliance requirement that sits alongside existing obligations such as classification, platform certification, safety assessments and quality assurance.

The burden is further compounded by the requirement that PIAs assess whether data handling practices are in the "best interests of the child". This increases compliance complexity and potential legal uncertainty, particularly for services operating across diverse age groups and jurisdictions.

The requirement in section 39 to maintain a public register of all PIAs raises additional concerns. While transparency is an important accountability mechanism, a public register of PIAs in the games sector risks exposing commercially sensitive information. Game development is highly competitive and innovation driven. Disclosure of this information goes beyond transparency and may create unintended commercial disadvantages, particularly for smaller businesses.

Public disclosure may also create unintended security risks, where PIAs contain detailed descriptions of system design, risk mitigation strategies or known limitations that could be exploited to undermine safety mechanisms or platform integrity.

Requiring PIAs to be completed prior to a game launch, for example, creates a potential gating requirement that risks introducing regulatory delay into development timelines already constrained by platform submission processes, content classification and coordinated global release schedules. Delays at this stage can have disproportionate commercial consequences, particularly where releases are tied to fixed publishing windows.

Recommendations:

- Proportionate and scalable approach: The OAIC should adopt a proportionate and scalable approach to PIAs under sections 38 and 39 of the Code, including the use of standardised or simplified PIA templates and scaled assessment requirements for small and mid-sized businesses, having regard to the nature, scale and risk profile of the service.
- Scope and operation of PIAs: The OAIC should clarify: (1) the threshold of "significant change" that triggers a new PIA obligation under sections 38 and 39 (including confirming that this refers to materially new or higher-risk features rather than incremental or iterative updates); (2) how the "best interests of the child" standard should be applied in practice; and (3) how any requirement to maintain a register of PIAs can be implemented in a manner that promotes transparency and accountability, without requiring disclosure of commercially sensitive or security-relevant information.
- Register of PIAs: The OAIC should reconsider the requirement in section 39(2) to maintain a public register of PIAs. Consideration should be given to alternative approaches that preserve regulatory oversight, while mitigating unintended risks and burdens, such as maintaining an internal register of PIAs that can be made available to the OAIC on request, or permitting appropriate redactions of commercially sensitive or security-relevant information prior to publication. A public register may create unintended incentives to limit the scope or documentation of PIAs and could expose information that undermines system integrity or safety controls.

19. Review of privacy practices and staff training

We support the objective of ensuring that entities handling children's personal information maintain strong governance processes, including regular review of privacy practices (section 25 of the Code) and staff privacy education and training (section 40). As outlined in our previous submission, the video games industry already invests significantly in safety systems, parental controls, moderation processes and platform-level protections that support responsible data handling.

However, the implementation of sections 25 and 40 must remain proportionate and reflect the diversity of the Australian games sector. Many emerging and independent studios

operate with limited administrative capacity and lack dedicated compliance teams. As we have previously emphasised, regulatory obligations should scale with risk and avoid imposing unnecessary red tape that diverts resources away from core development activities without delivering meaningful privacy benefits.

19.1. Review of privacy practices

While regular review is important, a rigid annual requirement for all studios (regardless of size, risk profile or the nature of the game) may impose disproportionate burdens. A more flexible, risk-based approach would better reflect the realities of game development and ensure that reviews occur when they are most relevant.

Recommendation:

To reduce unnecessary administrative burden for smaller businesses, while maintaining accountability, section 25(1) of the Code should be amended as follows:

> *An entity must review and update, at least **biennially**, the practices, procedures and systems required by Australian Privacy Principle 1.2 to ensure that they comply with the Australian Privacy Principles and this Code.*

19.2. Privacy education and training

We support the importance of ensuring that staff who handle children's personal information understand their obligations. However, mandatory annual training for all staff with regular or frequent access may be burdensome for smaller businesses.

To reduce compliance burden while maintaining high standards, the OAIC should provide standardised training modules that studios can adopt or adapt. This would ensure consistency across the sector and support smaller businesses who may not have the capacity to design bespoke training programs.

Recommendations:

- Proportionate and flexible approach: To avoid unnecessary repetition, while ensuring training remains relevant, section 40(2)(c)(ii) of the Code should be amended as follows:

  *at least **biennially** thereafter**, and additionally where there is a significant change to the entity's privacy practices**.*

- Sector-specific guidance: The OAIC should provide sector-specific guidance on privacy training obligations in the games sector.
- Standardised privacy training: To support proportionate compliance, particularly for smaller businesses, the OAIC should develop standardised privacy training modules that entities can adopt or adapt, reducing the need for bespoke training programs while supporting consistent understanding of obligations across the sector.

IGEA supports strong children's privacy protections and believes the industry is well-placed to comply where obligations are clear and proportionate. We welcome ongoing engagement with the OAIC as it finalises the Code.

For further questions or information about our submission, please contact us at policy@igea.net.

About IGEA

IGEA is the industry association representing and advocating for the video games industry in Australia and New Zealand. Our industry includes the developers, publishers, and distributors of video games, as well as the makers of the most popular video game platforms, consoles and devices.

IGEA has over a hundred members, from emerging independent studios to some of the largest technology companies in the world.

Among our various activities, IGEA also organises the annual Games Connect Asia Pacific (GCAP) conference for Australian game developers and the Australian Game Developer Awards (AGDAs), which celebrate the best Australian-made games each year.

Find out more: www.igea.net

Acknowledgement of Country

IGEA acknowledges and pays respect to the past and present Traditional Custodians and Elders of this land and the continuation of cultural, spiritual and educational practices of Aboriginal and Torres Strait Islander peoples. We would like to extend our acknowledgments to the indigenous people from countries overseas and recognise their strength, wisdom and creativity.

IGEA

interactive games & entertainment association