**Kidentify Pte. Ltd.**
83 Keong Saik Road
02-01
Singapore 089168

**Public consultation on the Exposure Draft of the Privacy (Children's Online Privacy) Code 2026**

*Submitted to the Office of the Australian Information Commissioner*

4 June 2026

## Executive summary

1. k-ID welcomes the opportunity to comment on the Exposure Draft of the Privacy (Children's Online Privacy) Code 2026 (the Code) and the accompanying draft Explanatory Statement. This submission provides observations and suggestions drawn from k-ID's experience powering compliance infrastructure for online services that handle children's personal information across multiple jurisdictions, including in Australia.

2. k-ID supports the Code. Its privacy-first orientation, its alignment with the United Kingdom Information Commissioner's Office Age Appropriate Design Code, its adoption of the best interests of the child as a binding interpretive standard, and its risk-proportionate approach to age ascertainment are all well chosen and broadly consistent with international good practice.

3. This submission focuses on practical implementation. We have organised our comments around the provisions where, in our experience, deployment choices most directly affect how well the policy outcomes the Code seeks to achieve are realised in practice. Our comments are not directed at expanding or narrowing the Code's policy scope. They are intended to support the OAIC in giving operators clear and workable guidance for compliance.

4. In our experience, compliance with the Code is fundamentally an architecture problem. The Code creates space for an implementation approach that delivers reliable age signals alongside data minimisation: services know enough about their users to apply age-appropriate experiences, while collecting only what is needed to manage their risk. The Code is at its strongest where it steers operators toward this middle path: reliable, risk-proportionate, privacy-preserving age assurance and consent infrastructure.

5. The principal points in this submission are summarised below:

    - **Age ascertainment (s.8):** we support the risk-proportionate, technology-neutral standard, and recommend that the Explanatory Statement's data-minimised reuse principle be reflected in OAIC guidance. Guidance should also make clear that information collected to ascertain age is used only for that purpose, and not for profiling, tracking or any other use.
    - **Age assurance guidance:** the guidance on age assurance technologies foreshadowed in the Explanatory Statement is the natural home for recognising providers certified to recognised standards, on an open,

technology-neutral basis that names no provider and leaves every other obligation in force.

- **Privacy by default (s.9):** we support the strict-necessity standard. Interpretive guidance on how the test applies to processing performed by third-party compliance providers would help operators implement section 9 with confidence.
- **Parental responsibility verification (s.13(2)(b)):** the verification methods named in the Explanatory Statement are well chosen. We recommend the Code or guidance recognise that risk-proportionality applies to parental verification as well as to age ascertainment.
- **Child assent (s.20):** we support the principle, and recommend guidance on adequate assent and the interaction with the parental-controls exception described in the Explanatory Statement.
- **Privacy impact assessments (s.39):** the public PIA register would benefit from defined minimum fields that avoid requiring disclosure of security-sensitive or commercially confidential information flows.
- **Interoperability:** coordinated guidance from the OAIC and the eSafety Commissioner would help operators understand where the same age assurance event can satisfy overlapping obligations under the Code and the Online Safety Act 2021 (particularly Part 4A), while preserving each regulator's distinct statutory role.
- **Commencement:** the technology is not the barrier to implementation. Age assurance tooling can be technically integrated in days, so the Code's protections can commence promptly. Only the section 9 existing-accounts rollback warrants a short, defined transition.

6. k-ID is available as a technical resource to the OAIC as it develops ongoing guidance, particularly on age assurance technologies as foreshadowed in the Explanatory Statement. We have not made commercial recommendations in this submission, and we have not advocated for any particular method or vendor outcome. We have offered observations from our deployments that may inform OAIC's consideration.

## About k-ID

7. k-ID is a privacy-first compliance infrastructure provider. We help digital platforms, games, social media, and online services deliver age-adaptive experiences and meet their legal obligations relating to kids and teens. Our work spans age assurance, parental consent and verification, compliance orchestration, and region-specific implementation, all built on the principle that age assurance is an architecture problem, not an identity verification problem.

8. k-ID's product stack includes the Compliance Development Kit (a sessioned compliance integration covering age determination, consent, permissions, and verification), AgeKit+ (a standalone age assurance product for discrete age-decision use cases), Family Connect (parental engagement and consent), and Compliance Studio (server-side configuration of jurisdictional rules, permission catalogues, and verification preferences). k-ID, through the OpenAge Initiative, has also developed

AgeKeys, reusable passkey technology that allows a single, data-minimised age determination signal to be reused across services and platforms in a privacy-preserving manner, consistent with the cross-scheme reuse principle reflected in the Explanatory Statement.

9. k-ID is deployed in Australia and across multiple other jurisdictions including the European Union, the United Kingdom, Brazil, several US states, and Asia Pacific markets. Our architecture is designed to minimise the personal information collected to determine age, to limit data retention to what is necessary for the purpose, and to support purpose-limited consent with per-feature granularity.

10. This submission reflects observations from k-ID's deployment work and our engagement with regulators in multiple jurisdictions. We do not represent any specific operator or industry body, and we have not been engaged by any party to make this submission.

## General observations

### The Code's privacy-first orientation is well chosen

11. The Code is appropriately situated under the Privacy Act 1988 and made by the Australian Information Commissioner. We support this institutional location. Children's online privacy is an area where data minimisation, purpose limitation, transparency, and individual rights of access, correction, and destruction are the right organising principles. Provisions throughout the Code, including section 8(4) (destruction of sensitive information collected for age ascertainment), section 9 (high privacy by default), section 18 (specific consent), and section 32 (destruction on request), reflect a coherent, privacy-first design.

12. In our experience, child-safety outcomes and child-privacy outcomes are mutually reinforcing when the underlying architecture is privacy-first by design. Architectures that minimise collection, limit retention, and apply tight purpose-limitation reinforce both privacy and safety. Data minimisation is not a constraint on protecting children; it is foundational to it. The Code's structure encourages operators to build this kind of architecture from the outset.

### Rights of the child as the ethical anchor

13. We would encourage the OAIC to anchor the Code's best-interests standard (sections 10, 11 and 38) in the United Nations Convention on the Rights of the Child, with General Comment No. 25 (2021) as the authoritative framework for the digital environment. The Convention's protection rights (such as Article 19) sit alongside, not above, its participation rights: privacy (Article 16), freedom of expression and access to information (Articles 13 and 17), and rest, leisure and play (Article 31). A best-interests assessment grounded in the full Convention defaults to safe, age-appropriate participation rather than to exclusion, which is the outcome the Code's structure already supports.

### Alignment with the UK Age Appropriate Design Code is welcome

14. The Explanatory Statement notes alignment of section 8 with Standard 3, section 9 with Standard 7, and section 38 with Standard 2 of the UK Age Appropriate Design Code. We support this alignment. International coherence reduces fragmentation, improves operator certainty, and makes it easier for operators serving multiple markets to invest in compliant implementations rather than treating each market as a separate exception.

15. k-ID has worked with services that operate under the UK Age Appropriate Design Code as well as other similar international safety regimes. The drafting choices in the Australian Code are well informed by that operational experience and resolve some of the points of practical ambiguity that have surfaced in the UK over the years. The Australian Code's explicit attention to assent (section 20), to direct-marketing safeguards (section 11), and to the right of destruction (section 32) are constructive additions.

### Risk-proportionality is the right approach

16. Section 8(2) embeds risk-proportionality into the age ascertainment standard, and the Explanatory Statement extends similar reasoning to the choice of parental verification method (section 13). We strongly support this approach.

17. In our experience, different services benefit from different age assurance methods. A risk-proportionate approach lets lower-risk services use lighter-weight methods (such as age inference from indirect signals or self-declaration combined with downstream checks), and lets higher-risk services apply stronger methods (such as third-party identity verification or age estimation backed by an additional check). Layered approaches in which multiple lower-assurance signals combine to produce a defensible outcome work well in many service contexts. This is consistent with the position taken by international standards bodies and other regulators.

18. We note the Explanatory Statement's definition of age assurance as an umbrella term covering age inference, age estimation, age verification, self-declaration, and parental attestation. This definition is helpful and consistent with the working definition in the IEEE 2089.1 standard and the United Kingdom regulatory framework.

## Specific comments on the draft Code

### Application of the Code (sections 5 to 7)

19. The scope of the Code is clearly drafted. Coverage of services likely to be accessed by children, plus the additional category of services primarily concerned with the activities of children, captures the practically relevant population without capturing unrelated services unnecessarily.

20. We note that the term "likely to be accessed by children" is not defined in the Code itself. Operators in our experience benefit from clear, factor-based guidance on this threshold (such as the indicators set out in the UK Information Commissioner's Office guidance on the Age Appropriate Design Code). We recommend the OAIC issue similar interpretive guidance.

**Recommendation 1.** Issue interpretive guidance on the meaning of "likely to be accessed by children" in section 7, with a non-exhaustive list of indicators (such as marketing channels, content style, content subject matter, prior user research data, app store classification, and observed user demographics). The factors provided by the US Federal Trade Commission under the Children's Online Privacy Protection Act (COPPA) offer a useful reference point.

## Age ascertainment (section 8)

21. Section 8 is the operationally pivotal provision of the Code for many services in scope. We support the drafting and the policy choices it reflects: a "reasonable steps" standard, risk-proportionality, minimal collection of personal information for the age check, and destruction of sensitive information after the check. Each of these reflects an important design principle. Age assurance, done well, is an architecture problem distinct from identity verification. An age check should establish whether a user is in the relevant age band; it does not need to establish, and generally should not establish, who the user is or otherwise be used to build a profile on them.

22. The Explanatory Statement makes two clarifications that we consider materially important to operator certainty. First, that age assurance is an umbrella term covering multiple methods. Second, that an entity that has already taken reasonable steps to ascertain age for another purpose (the Online Safety Act 2021 Part 4A example is given) may reuse that data-minimised age result for the Code's purposes, provided that compliance with the Code was a stated purpose of collection and the entity has taken reasonable steps to ensure the determination remains accurate, up to date, complete and relevant.

23. The reuse clarification matters because operators in scope will frequently be subject to multiple Australian regulatory frameworks that touch on age. A coordinated approach reduces the data flowing across schemes and supports operators in treating age as something to be established once, well, and reused. We support the reuse principle and recommend it be reflected explicitly either in the Code text or in OAIC guidance, including:

    1. the conditions under which a determination from one scheme can be reused for the Code's purposes (compliance with the Code being a stated purpose of the original collection, and the result remaining a data-minimised age result);
    2. the requirement that the determination remain accurate, current, and proportionate to the risk profile of the new use; and
    3. the role of metadata recording the basis on which an age determination was made (for example, the assurance level, the method used, and the original purpose), which supports both compliance assurance and operator due diligence.
    4. We would also encourage that any such reuse remain transparent to the end-user, consistent with the Code's privacy-first orientation.

24. The Explanatory Statement's discussion of age assurance technologies, together with the risk-based design of section 8, supports the use of appropriately governed third-party providers where this reduces direct collection of personal information by

the operator. A neutral intermediary that establishes age once, returns only what the operator needs to know (typically a binary outcome at the relevant threshold), and does not pass identity information through to the operator is more privacy-preserving than direct collection by the operator. We support drafting and guidance that recognise this model.

25. The Explanatory Statement foreshadows that the OAIC will maintain guidance on age assurance technologies. That guidance is the natural place to recognise providers that are certified to recognised technical standards for age assurance (such as ISO/IEC 27566), so that operators have a clear and open path to a compliant age-assurance method. Recognition of this kind would be open to any provider meeting the standard, would name no particular provider, and would leave every other obligation under the Code in force. It supports the Code's purpose by reducing the risk that operators, lacking a defined path, default to collecting more identity information than the situation requires.

26. A natural complement to recognising certified providers is a narrow, process-specific compliance presumption. An operator that ascertains age in good faith through a provider in the recognised category would be presumed to have taken reasonable steps to ascertain age for the purposes of section 8(2). The presumption would be scoped to the section 8(2) accuracy obligation alone; every other duty under the Code (privacy by default, best interests, transparency, destruction, monitoring notification, and privacy impact assessments) would remain in full force. A mechanism of this kind is process-specific and open by certification, and is structurally similar to long-standing models such as the ESRB's COPPA safe harbour, GDPR Article 40 codes of conduct, and financial-services know-your-customer frameworks, each of which leaves broader duties intact. It gives operators a defined compliance path for the one obligation where certainty most reduces the temptation to over-collect.

27. Section 8(4) requires destruction of sensitive information collected for age ascertainment, which we support. We suggest the OAIC go one step further in guidance and make explicit that personal information collected to ascertain age — whether or not it is sensitive information — should be used only for that purpose, and not for profiling, tracking, tracing, advertising, or any purpose other than age assurance. A clear purpose-limitation expectation prevents age-check data from becoming a back-door source of profiling data, which would undercut the privacy-first intent of section 8.

28. Three observations on section 8 that we consider important to its successful operation:

    1. **Method neutrality.** OAIC guidance can usefully remain method-neutral and outcomes-based, recognising that different age assurance methods suit different services, risk levels, age bands, and family contexts. Guidance that names methods illustratively rather than prescriptively leaves room for innovation as age assurance techniques continue to mature.
    2. **Supporting proportionate data collection.** The Code is at its strongest where it supports operators in choosing the lightest-weight age assurance method that satisfies the relevant risk threshold. Where a less data-intensive method is sufficient to meet the reasonable-steps standard for a given service

and risk profile, that method is the right choice. We encourage the OAIC to make this principle explicit in guidance.

3. **Portability of the age signal.** Where a provider has made a successful age determination, we recommend the OAIC encourage that the result be made available to the end-user in a portable, interoperable format, so the user can present it in other appropriate contexts rather than repeating an age check and the data collection that entails. Correspondingly, the OAIC could encourage operators to be able to accept such a signal where it carries reasonable proof of reliability. For example the assurance level, method, and original purpose recorded in its metadata (paragraph 24). Portability of this kind advances data minimisation: an age established once, well, need not be re-collected and re-verified.

**Recommendation 2.** Reflect the Explanatory Statement's data-minimised reuse language in OAIC guidance, including the conditions for reuse, the role of accuracy, and the value of metadata recording the basis of an age determination. Confirm that operators may rely on third-party age assurance providers consistent with section 8, and that the foreshadowed age assurance guidance may recognise providers certified to recognised standards on an open, non-naming basis. Make explicit that information collected to ascertain age is to be used only for age assurance and not for profiling, tracking, or other purposes. Encourage that a successful age determination be made available to the end-user in a portable, interoperable format, and that operators be able to accept such a signal where it carries reasonable proof of reliability.

**Recommendation 3.** Consider pairing recognition of certified providers with a narrow, process-specific compliance presumption for the section 8(2) accuracy obligation: an operator that ascertains age in good faith through a provider in the recognised category is presumed to have taken reasonable steps to ascertain age. The presumption is scoped to that obligation only; all other duties under the Code remain in full force. This is consistent with established models such as the ESRB COPPA safe harbour and GDPR Article 40 codes of conduct.

## Privacy by default (section 9)

29. We support section 9. The strict-necessity standard, the high-privacy-by-default obligation, and the requirement to provide accessible, child-usable controls for not-strictly-necessary processing are well drafted. Privacy by default, properly implemented, is a design discipline that runs through the whole product, not a setting that is configured at the end. The Explanatory Statement's clarification that strict necessity is narrower than reasonably necessary supports operators in applying that discipline at the right point in the design process.

30. Operators may encounter uncertainty around how the strict-necessity test in section 9 applies to processing carried out by third-party providers engaged to support compliance functions, such as age ascertainment, parental verification, consent management, and data-subject-rights orchestration. The test applies most directly to the operator's own processing for service delivery; its application to

compliance-provider processing is a question on which interpretive guidance from the OAIC would be useful, particularly given the Explanatory Statement's discussion of age assurance technologies and the role they may play in supporting Code compliance.

31. **Existing accounts.** Section 9 applies to both new and existing accounts on commencement. In our experience, applying high privacy by default to existing accounts requires operational resources: some services will need to inventory existing accounts of likely or known minors, identify which optional elements are currently enabled, and roll back default settings to comply. This is the one part of the Code that genuinely warrants transition lead time, and we address it under Commencement below.

**Recommendation 4.** Provide interpretive guidance on the application of the strict-necessity test to processing performed by third-party compliance providers, confirming that processing undertaken solely to enable the operator's Code compliance is consistent with the strict-necessity standard.

## Parental responsibility verification (section 13)

32. Section 13 is operationally consequential. The 15-year-old self-consent threshold is well chosen and consistent with existing OAIC guidance and the Australian Law Reform Commission's earlier review. The requirement that consent for under-15s come from a person with parental responsibility, accompanied by reasonable steps to confirm parental responsibility, is the right approach.

33. The Explanatory Statement helpfully names a non-exhaustive set of verification methods: parent account email confirmation; vouching tokens from banks, schools, or telecommunications providers; customer service video conference; and government digital ID. These reflect deployable practice. We suggest the following observations be reflected in OAIC guidance:

    1. **Risk-proportionality applies to parental verification.** What is reasonable depends on the sensitivity of the information being collected from the child and the purposes for which it will be used. A simple email confirmation may be reasonable for low-risk processing of contact details. Stronger methods (such as credentialed vouching, government digital ID, or video conference) are appropriate for sensitive information or high-risk uses. The OAIC's guidance should affirm this proportionality.
    2. **Federation reduces fresh collection of parent data.** Where a parent has already established their identity and parental responsibility through a trusted credential issuer (a bank, a school administration system, a telecommunications operator's account, or a government digital ID), it is preferable from a privacy perspective for the operator to verify via that credential rather than collect parental identity information directly. This reduces the parental data footprint and supports purpose-limitation. We recommend the OAIC's guidance encourages federation where it is available and suitable to the risk.
    3. **Notice to the child (section 13(3)).** The age-appropriate notice to the child after parental consent is given is a thoughtful inclusion. It supports the child's

developing privacy literacy and avoids treating parental consent as a closed transaction between the operator and the parent. Operators may benefit from sample notice templates with the prescribed section 13(3) content.

**Recommendation 5.** Affirm in guidance that risk-proportionality applies to parental responsibility verification, and that federation through trusted credential issuers (banks, schools, telecommunications providers, government digital ID schemes) is encouraged where suitable to the risk. Provide sample age-appropriate notice templates for section 13(3).

## Consent quality and currency (sections 14 to 19)

34. The consent quality standards in sections 14 through 19 (voluntary, informed, current, specific, unambiguous, no coercion, no bundling, no inference from omission) align with international good practice and with the Privacy Act's general consent framework. We support them.

35. **Currency and reconsent (sections 15(4) and 16).** The 12-month maximum consent period is a reasonable upper bound. Implementation of reconsent has a particular feature for under-15s that we draw to OAIC's attention: when the original consent was given by a person with parental responsibility, reconsent at the 12-month point requires fresh parental verification. If the original verification was, for example, a vouching token, the operator will need either a fresh vouching event, or a sustainable mechanism for reverifying without collecting fresh parental identity data. This is a legitimate case for federation and for credential reuse with proper data minimisation.

36. **Threshold transitions.** When a child crosses the 15-year-old threshold during a service relationship, the legal basis for consent shifts from parental to direct. The Code does not address this transition explicitly. We suggest OAIC guidance address this scenario, including timing expectations and any retention implications for the original parental-consent record.

**Recommendation 6.** Address in guidance the practical implications of consent currency for under-15s, including reconsent flows requiring fresh parental verification, and threshold-transition flows when a child reaches age 15 during the service relationship.

## Child assent (section 20)

37. Section 20 is a thoughtful provision. Maintaining parental consent as the legal basis for sensitive uses while requiring child assent supports both child agency and parental responsibility. We support it.

38. Implementation of section 20 raises practical questions on which OAIC guidance would be valuable:

    1. The relationship between the assent step and the parental-consent step: the Code requires the child's assent (including to the entity contacting a person with parental responsibility), but the precise sequencing and notice content for each step would benefit from clarification;

2. What constitutes adequate evidence of assent: an active affirmative action by the child, age-appropriate notice, and a record of the assent are reasonable expectations, but operators would benefit from concrete examples of compliant flows; and
3. The interaction with the parental-controls exception described in the Explanatory Statement (under which a child's assent is not required where a person with parental responsibility has already consented for that purpose, including through parental controls applied on the child's account). We note this exception is described in the Explanatory Statement rather than stated in section 20 itself; a worked example, and confirmation of where the exception sits in the Code, would assist operators.

**Recommendation 7.** Provide a worked example or design-pattern guidance for section 20 assent flows, including the sequencing of child assent and parental consent, the form of evidence of assent, and the boundary with the parental-controls exception described in the Explanatory Statement. Confirm whether that exception is intended to be reflected in the Code text.

## Destruction of personal information (section 32)

39. We support section 32. The right of children, and persons with parental responsibility for under-15s, to request destruction of specified personal information is a meaningful enforcement of the underlying privacy principles. The express position that de-identification is not sufficient to comply (in light of re-identification risks) is the right call.

40. Two implementation observations:

    1. **Destruction across the data ecosystem.** An operator subject to a destruction request will frequently hold the relevant personal information across its own systems, third-party processors, archival backups, and analytics environments. Compliant destruction within 30 to 60 days requires either a clear data inventory or a managed orchestration capability. This is a practical reason to consolidate child-data handling on a smaller number of well-governed processors.
    2. **Interaction with consent and processing records.** Where the operator has relied on consent (under section 13) to process personal information, destruction of that information should also include destruction of any associated consent record, save where retention is independently required by law. The Code does not address this directly but the implication is consistent with the destruction obligation. Guidance on the treatment of consent records would help operators avoid retaining residual identifiers.

## Notification of parental controls and geolocation monitoring (section 33)

41. We support section 33. The principle that children should be informed when their use of a service is being monitored, controlled, or geolocated, including in the peer-to-peer context, supports both privacy and child agency.

42. Implementation observations:

    1. **Persistent in-product indicators for ongoing monitoring.** We read subsection 33(2)'s "throughout the period" requirement as confined to

genuinely continuous monitoring by another end-user, principally live peer-to-peer location sharing, rather than to the one-off notification appropriate to parental controls under subsection 33(1). A persistent indicator is proportionate in that narrow case and is already common in live-location features; a single clear, age-appropriate notice is sufficient where a control is simply in place. We would caution against extending a persistent-notification expectation across all parental-control mechanisms, which would add UI burden without a commensurate privacy gain.

2. **Differentiating monitoring types.** Operators implement a range of mechanisms covered by section 33, including content filters, in-app purchase restrictions, time limits, communication controls, and geolocation sharing. Age-appropriate notification will, in practice, vary by mechanism. Guidance on the level of specificity required would help operators avoid either generic over-notifying or under-notifying for some controls.

3. **Coexistence with parental rights and child best interests.** Parental controls support parental responsibility, which is itself a UNCRC principle. The notification obligation under section 33 supports the child's developing autonomy and right to a private space, also a UNCRC principle. In our experience these can coexist by design. The notification does not need to allow the child to disable a parental control; rather, it must inform the child that one is in place. We agree with the policy approach in section 33 and consider the drafting workable.

**Recommendation 8.** Provide design-pattern guidance for section 33, including a worked example of persistent in-product notification for ongoing peer-to-peer geolocation sharing, and examples of age-appropriate notification for the principal categories of parental-control mechanism.

## Privacy impact assessments (sections 38 and 39)

43. We support section 38 and the related register requirement (section 39). PIAs that genuinely engage with information flows, strict necessity, the best interests of the child, and the risk of harm are a useful discipline for operators.

44. The three core components identified in the Explanatory Statement (information flows mapping, compliance check, risk assessment) are the right structure. We suggest two refinements that may strengthen consistent practice:

    1. **Treatment of third-party processors in the information flows.** Where an operator relies on third-party providers for age ascertainment, parental verification, or consent management, the PIA should map the data flows to and from those providers, the basis on which they process the data (typically as a processor for the operator), and how purpose-limitation is enforced. This applies symmetrically to providers of analytics, recommendation, and content-moderation services that process children's data.

    2. **Best-interests assessment as a documented exercise.** Section 38(2)(d) requires the PIA to record the best-interests assessment and the reasoning on which it is based. In our experience, this is the part of a children's PIA where structured guidance has the largest effect on the quality of the assessment. We recommend OAIC guidance set out a structure for the

best-interests assessment, including the factors named in the Explanatory Statement (developmental impact, identity development, freedom of association, vulnerable groups, evolving capacities), so the assessment becomes a substantive analytical exercise that meaningfully informs design decisions.

45. **Public register (section 39(2)).** Section 39(2) requires entities to publish their register of privacy impact assessments online. We support transparency. We note, however, that the Code does not specify what the published register must contain. Without defined minimum fields, operators face uncertainty and a risk of disclosing security-sensitive information flows or commercially confidential detail through the act of publication. We recommend OAIC guidance specify the minimum published fields for the register and confirm that the obligation does not require disclosure of information whose publication would itself create a privacy or security risk. This is a further area, alongside age assurance technologies, where structured OAIC guidance would materially improve consistency.

**Recommendation 9.** Specify in guidance the minimum fields for the published section 39 register of privacy impact assessments, and confirm that publication is not required where it would itself create a privacy or security risk or disclose commercially confidential information flows.

## Implementation considerations

### Interoperability with the Online Safety Act and other domestic frameworks

46. Operators in scope of the Code will frequently be in scope of one or more other Australian frameworks that touch on age, including Part 4A of the Online Safety Act 2021 (social media minimum age), the eSafety Industry Codes and Standards, and the new Online Safety Act registration scheme for designated service categories. International operators serving Australia will also be navigating the EU, UK, US, and other regional frameworks.

47. A coordinated interpretive note from the OAIC and the eSafety Commissioner on the interaction between the Code and the Online Safety Act would be highly valuable, while preserving each regulator's distinct statutory role. Specific points where coordination would help operators understand where the same age assurance event can satisfy overlapping obligations:

    1. The relationship between the Code's section 8 age ascertainment standard and the Part 4A age verification standard, including the conditions under which a determination meeting one standard can also be relied upon for the other;
    2. The treatment of operators who are within Part 4A scope but outside the Code (or vice versa);
    3. The consistency of expectations on parental verification between the two regimes; and
    4. The alignment of enforcement posture and the avoidance of inconsistent guidance from the two regulators.

48. We recognise this is partly a question for the OAIC and partly a question for the eSafety Commissioner. We would value the opportunity to discuss this with the OAIC and to support coordination with eSafety where helpful. A useful international reference point is the joint statement on age assurance issued by the UK Information Commissioner's Office and Ofcom, which set a shared framing without altering either regulator's statutory role.

**Recommendation 10.** Coordinate with the eSafety Commissioner on regulatory coherence between the Code and the Online Safety Act, particularly Part 4A, so that operators understand where the same age assurance event can satisfy overlapping obligations, while preserving each regulator's distinct statutory role.

## Commencement timing

49. The Explanatory Statement notes that the commencement date is to be drafted and expressly invites views. We note at the outset that the Exposure Draft currently contains no transition or grace mechanism of any kind; the commencement provision is left blank. We therefore offer the following observations on how commencement can best serve the Code's purpose.

50. Technology is not the limiting factor. Age assurance and consent infrastructure of the kind the Code contemplates can be integrated into a live, internationally operating platform in a matter of days — in some cases in as little as a week. In one recent case, k-ID completed such an integration for a global platform in three days. Build and integration time is therefore not, in our experience, a reason to delay the point at which children begin to receive the Code's protections.

51. A prolonged commencement runway carries a real cost: it postpones the protections the Code is designed to deliver, and it gives operators under no time pressure little reason to act. We would caution against a long, general transition period on the assumption that implementation is technically slow. It is not.

52. The one obligation that genuinely warrants transition lead time is the section 9 existing-accounts requirement. Applying high privacy by default to an existing user base involves inventorying accounts of likely or known minors, communicating with users (and where appropriate persons with parental responsibility), and rolling back default settings without service disruption. This is operational rather than technical work, and it can be managed with a short, defined transition applied specifically to existing accounts, rather than a long delay applied to the Code as a whole.

53. On balance, we suggest the OAIC commence the Code promptly, so that new protections take effect without unnecessary delay, and apply a short, clearly defined transition window only to the section 9 existing-accounts obligation. This approach serves the quality of implementation while ensuring that speed of protection for children is not sacrificed to a runway that the technology does not require.

**Recommendation 11.** Commence the Code promptly so that its protections take effect without unnecessary delay. The technical implementation of age assurance is not the limiting factor. Apply a short, clearly defined transition window only to the section 9 existing-accounts obligation, rather than a long general transition period.

## Closing

54. k-ID welcomes the OAIC's leadership in developing the Code and acknowledges the depth of consultation that has informed it. The Code is well drafted, well aligned with international practice, and grounded in a coherent privacy-first design. Australia is now one of the most clearly defined age assurance markets globally.

55. The work ahead is operational. The Code's success will depend on how operators implement age ascertainment, parental verification, default settings, and consent flows in practice. We are available as a technical resource to support the OAIC's development of ongoing guidance on age assurance technologies, as foreshadowed in the Explanatory Statement, and would welcome the opportunity to engage further during the remainder of the consultation period and as the Code progresses to finalisation.

56. Please direct any questions or follow-up to the contact details below.

**Contact**

[redacted]

Chief Corporate Affairs Officer, k-ID

## Annex A — Drafting and cross-reference observations

The following are minor drafting and cross-reference observations offered solely to assist the OAIC's drafting team. They do not bear on the substance of our submission and can be disregarded if the OAIC prefers. They are gathered here, rather than in the body, for that reason.

1. Section 4 (definitions note): the paragraph lettering of the terms drawn from section 6 of the Act appears to run (a), (b), (c), (b), (c), duplicating (b) and (c).
2. Section 11(6): the sub-numbering appears to run "(a) … (ii)", which looks incomplete.
3. Section 15(4): the 12-month maximum is expressed by reference to "paragraph (3)(b)", but the reliance period that the cap is intended to govern appears to sit in paragraph (3)(c) (consistent with the reference in section 16(2)(c)(i)). This looks like a cross-reference that may need correcting.
4. Section 18(2): two paragraphs appear to be lettered "(a)"; the second is presumably intended to be "(b)".
5. Section 20(4): two paragraphs appear to be lettered "(a)"; the second is presumably intended to be "(b)".
6. Section 29(4): the sub-numbering appears to run "(a) … (ii)", which looks incomplete.
7. Explanatory Statement: the discussion of section 10 appears to move from subsection 10(3) to 10(5) and 10(6) without a 10(4); and a reference to "subsection 26(3)(3)" appears to contain a typographical error.