Response to OAIC's Exposure Draft of Children's Online Privacy Code and Explanatory Statement
5 June 2026

Introduction

Google welcomes the opportunity to provide feedback on the Office of the Australian Information Commissioner's (**OAIC**)'s Exposure Draft of the Privacy (Children's Online Privacy) Code 2026 (**Code**) and Exposure Draft Explanatory Statement (**Explanatory Statement**).

Google recognises that the Code seeks to enhance privacy protection, increase transparency, and emphasise the best interests of the child as a primary principle in handling children's personal information. This aligns with Google's commitment to kids and families, which is guided by three essential pillars: protecting young people online, respecting families' unique relationships and preferences with technology, and empowering young people to safely learn and explore the digital world. While we support the OAIC's objective to enhance privacy protections for children, our guiding principle is that young people should be protected *in* the digital world, not *from* it. An effective framework should take a proportionate, risk-based approach, recognise evolving developmental stages and autonomy of teens, and adopt a holistic definition of the "best interests of the child" that balances safety with their fundamental right to access information, express themselves, and participate in society.

Google recommends that the Code should:

1. **Align with international frameworks**. Google recognises that the Code is intended to align with international frameworks such as the United Kingdom's Age Appropriate Design Code (**AADC**). We are supportive of international alignment to ensure consistency in global regulatory and industry standards, foster interoperability, and provide greater regulatory certainty. This allows service providers to build on established frameworks and best practices, so that users can benefit from a better experience which reflects user expectations.

2. **Be principles-based, flexible, and reflect a risk-based and proportionate approach**. Online services are diverse and provide varied but valuable benefits to users, including children. The Code should account for this diversity, both in the nature of the services, as well as the distinct developmental stages and evolving capacities of the children engaging with them. Service providers must have the flexibility to apply the standards in a way that reflects the service, the level of harm which it poses, and what is appropriate and technically feasible. A one-size-fits-all approach will not protect children's privacy effectively.

3. **Take into account children's full range of rights**. Google supports the promotion of children's rights and the protection of children, including the right to privacy. However, the Code should also recognise and facilitate the other rights of children, including the right to access information, freedom of expression and thought, and the right to play. It is also important to take into account the role of parental guidance in a way that recognises children's evolving capacities and agency.

4. **Recognise that the "best interests of the child" is a dynamic concept**. This is most effectively addressed by implementing privacy-by-default and privacy impact assessment processes. A

risk-based approach can identify and enable protections for children where and when they are most needed.

5. **Acknowledge the benefits of personalisation**. Personalisation, in the context of a service, is aligned with children's developmental needs and supports their ability to access and discover high-quality content and age-appropriate information online. It is also an important way to mitigate the risk that children may interact with content that is not age-appropriate. The Code should consider the nuances of personalisation, such as the distinction between content recommendation and targeted advertising, and enable the collection and use of data to support important functions, such as to deliver age-appropriate content and improve the safety and performance of services — which benefits all users, including children.

Taking these principles into account, we have set out our recommendations and comments on how the Code can enable a framework which best protects children while also providing access to the digital tools, information and experiences that are a foundational part of children's everyday lives.

Comments on the Code and Explanatory Statement

1. Scope and Application of the Code

We agree with the Code's application to services that are *likely to be accessed* by children. However, we recommend that the Code explicitly exclude cloud services, enterprise accounts or services, and business-to-business (B2B) services from its remit, as these are not likely to be accessed by children. Further, we are of the view that the Code should not apply to entities that are *primarily concerned with the activities of children*, for example, apps that track early childhood development, family photo sharing apps, online school management systems that monitor student performance, and internet-connected baby monitors. While we acknowledge that these types of services may present privacy risks to children, these services — which may also include educational institutions and educational technology (EdTech) services — raise different types of risks and should be considered separately from the Code in light of their unique context, roles and responsibilities. This would also be aligned with the approach taken in other international frameworks, such as the UK's AADC, which only applies to services likely to be accessed by children.

In this respect, we ask that the OAIC consider the exemption regime which Indian law provides under the Digital Personal Data Protection Act, 2023 (DPDP Act) and its corresponding DPDP Rules. In particular, the Indian approach explicitly recognises that a one-size-fits-all approach stifles beneficial services. To address this, the DPDP Act expressly provides exemptions for:

- **"Verifiably Safe" Platform Exemptions:** The government is empowered to exempt specific platforms from the parental consent obligation and the prohibitions on tracking and advertising if the data fiduciary can conclusively demonstrate that its data processing practices are "verifiably safe" for children.
- **Entity-Based Exemptions (Class-Based):** The DPDP Rules establish conditional exemptions for specific classes of entities, including educational institutions and schools. Provided they adhere to the conditions of necessity, data minimisation and technical safeguards, these entities are relieved from the parental consent requirements and the absolute ban on tracking. This acknowledges that their core operations (such as monitoring student academic progress) are inherently for the child's benefit.

Providing for similar exemptions in Australia would allow platforms — particularly EdTech and educational institutions — to continue delivering personalised, data-driven learning outcomes without being hindered by rigid prohibitions that are primarily designed to regulate commercial social media platforms.

2. Age of Consent

While Google understands the OAIC's intent to provide regulatory clarity by codifying its existing guidance, we consider that hardcoding a rigid digital age of consent — particularly at a high baseline of 15 years — is not the most effective way to protect children online. A more effective way to protect children while ensuring that their rights are upheld is to focus on feature and functionality controls, enabling age-appropriate experiences while allowing children to enjoy all the benefits that technology brings.

Protections for children should be applied in such a way that respects their development and the ability of families to make choices about how they use technology. Teenagers have increased developmental capacity and agency, and it is important for them to access information as they continue learning.

Setting the threshold at 15, especially when paired with the Code's proposed parental verification mechanisms, can inadvertently harm teenagers who have legitimate needs to access online resources, but might not be able to get consent or may want privacy from their parents. For example, it may not be feasible for individuals under 15 to seek parental consent before accessing each educational or occupational resource online that relies on consent for any aspect of their data processing. Alternatively, their parents may not be able or appropriately placed to provide consent, for example if they are absent, incapacitated, abusive, or not technologically savvy.

A rigid digital age of consent of 15 could have wider implications that may affect vulnerable populations. In particular, locking children out of online services may have a disproportionate impact on those from marginalised groups, restricting their access to helpful services and age-appropriate information they depend upon to learn, grow, civically engage, and stay in touch with friends and family. In short: not all people have engaged parents; not all people have parents at all; and not all parents do right by their kids.

Research shows that 77% of referrals to *akt*, a youth homelessness charity based in the United Kingdom, cited rejection and abuse from family members based on the identity of the young person as the driving force behind their homelessness. Parents or guardians in those cases may not act in the best interests of their children, and barring these teenagers from accessing online services and communication tools absent parental consent will only further the digital divide for those children.

According to *The Trevor Project*, a leading youth suicide prevention and crisis intervention organisation for LGBTIQA+ young people:

> "Parental consent requirements prevent young people from being able to access information regarding mental health support, suicide prevention, [and] community resources. … Requiring parental consent to access information risks exposing young people to family rejection, violence, homelessness, and harms to their mental health."

In this way, introducing rigid parental consent requirements risks unnecessarily burdening children's rights to freedom of expression and access to information — rights which are enshrined in the UN Convention on the Rights of the Child.

Adopting a more flexible framework which does not set a rigid age for consent does not prevent any parent from making decisions about when their children can or cannot access online services. Moreover,

strict requirements do not do anything to protect children from any risks that may arise after their parent grants consent, once they actually start using the service. True protection is better achieved through continuous, age-appropriate product design and default privacy controls.

Nevertheless, if a hardcoded digital age of consent needs to be introduced, our view is that **13 years** would be the appropriate threshold, as this aligns with global benchmarks in the United Kingdom, United States and Singapore. This helps to ensure consistency in global regulatory and industry standards, foster interoperability, and most importantly, to align user expectations.

3. Age Assurance

Google supports the approach to age assurance outlined in the Explanatory Statement, where the nature and frequency of checks is risk-based and balanced alongside privacy and other rights. We also agree that a risk-based approach may include age inference, age estimation, age verification, self-declaration and parental attestation, depending on the context in which providers are seeking to ascertain an end user's age.

To make minimum age checks effective and workable, we encourage consideration of the following:

- **Risk-Based Approach:** Regulatory requirements should avoid imposing arbitrary friction and excessive collection of data. Age restrictions and assurance mechanisms must adopt a risk-based approach, carefully balancing the nature and frequency of checks against user privacy and other fundamental rights enshrined in the UN Convention on the Rights of the Child, such as freedom of expression and access to information. This ensures that interventions treat children like children and adults like adults, without broadly suppressing access to vital age-appropriate information and services and excluding marginalised and vulnerable groups.
- **Proportionate Expectations:** Age assurance mandates should avoid a "one-size-fits-all" approach that treats all platforms, services, or functionalities identically regardless of their actual risk profile. The processing of personal data required for age assurance should remain necessary, proportionate and effective, balancing the privacy risks of widespread data collection against the objective of protecting children. The higher the risk of a service or feature, the more confidence a provider should have in its chosen age assurance method.
- **Graduated Experiences:** Legal frameworks should recognise developmental needs and the reality that a teenager's cognitive capacity and need for autonomy differ from those of a younger child. Platforms should be permitted to provide a spectrum of experiences that evolve alongside child users. This facilitates a staged approach to digital participation, offering a safe, gradual transition from heavily supervised exploration to mature digital independence.
- **Implementation at the Point of Risk:** Rather than imposing blanket, front-end friction through hard age verification requirements that degrade the experience for all users and may pose elevated privacy risks, hard age checks should be targeted at the point of risk. Where a safe, age-appropriate experience can be provided with effective frictionless age estimation, this should not only be permitted but encouraged. This approach helps ensure that hard verification requests and associated friction remain focused on specific, high-risk circumstances.

Age verification methods requiring government IDs, facial recognition, or banking details could create new privacy and security risks. This is why we consider age verification for all users as a sole tool to be disproportionate, higher risk and potentially less effective than a more nuanced combination of a number of tools. The same protections can effectively be achieved with less privacy invasive methods. For

example, Google's age estimation model analyses user activity patterns to determine the likelihood of a user being over or under 18, and only requires them to provide more information in specific circumstances (for example, to prove they are above 18 if we estimate they are under 18). In this context, conducting additional age assurance, where a user has already established their age with sufficient certainty through this estimation process, may exacerbate privacy risks while also degrading user experience.

More broadly, a greater number of checks does not necessarily equal a safer experience online. A reliance on frequent and intrusive checks risks driving users away from services that have heavily invested in safety by design, and onto riskier, less scrutinised platforms that lack robust safeguards. Imposing excessive friction may also incentivise users to adopt methods to bypass age checks, making it more difficult to monitor risks, provide timely interventions, and ultimately protect children.

Age assurance technologies are rapidly evolving. To make age assurance as effective as possible going forward, policymakers should preserve flexibility for providers to innovate and deploy proportionate, privacy-preserving approaches (such as age inference) rather than locking the ecosystem into high-friction verification requirements for lower-risk functionalities.

4. Privacy-by-Default and the "Strictly Necessary" Test

Google supports the principle of privacy-by-default and has implemented measures consistent with that principle, including by conducting impact assessments to determine appropriate mitigations.

However, Google has concerns about the "strictly necessary" requirement, which goes beyond the test in international frameworks including the AADC, and does not take into account other relevant considerations. For example, under the AADC, settings must be "high privacy" by default, unless the entity can demonstrate a *compelling reason* for a different default setting, taking into account the *best interests of the child*.

Google recommends that the Code adopt alternative language modelled on the AADC's "compelling reasons" test, which allows a risk-based approach subject always to the best interests of the child. This approach would preserve the protective intent of proposed section 9 of the Code to provide an enhanced level of protection for children beyond the "reasonably necessary" standard, while still accommodating other functions that, whilst not *strictly necessary* to deliver a core service, are clearly in the best interests of the child, such as providing age-appropriate content and information.

A "compelling reasons" approach is necessary to provide services and experiences that are in children's best interests. In particular, this recognises that personalisation provides a range of benefits to children, including in relation to online safety, provision of educational materials, and enhancing digital and media literacy. Accordingly, a platform should have the ability to enable personalisation by default if it has conducted the necessary impact assessments, implemented appropriate risk mitigations and determined it is in fact in the best interests of the child by enhancing the child's experience and safety.

5. Best Interests of the Child (BIOC)

Google supports the BIOC principle as a key component of the Code and welcomes the Explanatory Statement's clarification that collecting, using or disclosing personal information in ways that are consistent with BIOC does not mean that an entity cannot pursue its own commercial or other interests, and that an entity's commercial interests may be compatible with BIOC.

However, Google recommends that the BIOC assessment is to be considered as a primary consideration which should be taken into account as part of the privacy-by-default design principle and privacy impact assessment (**PIA**) process, rather than at each point of collection, use and disclosure. Accordingly, we would recommend clarification that the BIOC assessment is not required on a "per transaction" (i.e. per collection, use or disclosure) basis, but rather should be considered as part of building privacy-by-default into the design of online services, and the PIA process. This would allow organisations to take a risk-based approach based on the specific service, product or feature, while taking into account the expected audience (which could be of mixed ages) and potential risks.

6. Verifiable Parental Consent

Google acknowledges the importance of involving parents and guardians in decisions relating to children's privacy. When parental consent is appropriate and required, it should be done in a technology-neutral, flexible way to allow for technological innovation.

However, Google has significant concerns about the requirement to take "reasonable steps to confirm that the person who gives consent is a person with parental responsibility for the child". Examples of methods suggested in the draft Explanatory Statement include email communication, vouching via a token provided by a bank, school or telecommunications provider, a video conference with a customer service agent, or a form of government digital ID. Several of these methods raise serious practical and privacy concerns. For example, requiring service providers to examine documents or engage in verification processes that expose sensitive personal information about parents and children creates its own privacy risks and is not consistent with principles of data minimisation.

In any case, establishing the parent-child relationship is not always straightforward. Take, for example, the case of a child whose parents are divorced or disagree about parental permission.

Such requirements also place an unnecessary burden on those parents who may want to grant their child or teenager increased, age-appropriate autonomy. The better approach is to adopt a scalable standard that enables platforms to more efficiently support families in creating supervised accounts for their children.

Moreover, requiring proof of parentage could prevent children from accessing important information and services, particularly for children or families who may not have access to certain documentation to prove parentage, or for children who live in unsupportive households or seek information on sensitive matters, such as issues around identity, religion, mental health and wellbeing. LGBTIQA+ advocacy organisations have noted that parental consent requirements could prevent children from accessing important mental health and suicide prevention information and community-specific resources, which may expose children to mental and physical harm.

To address these practical challenges, we encourage the OAIC to look to international frameworks that have adopted more pragmatic, privacy-preserving mechanisms. For example, under the Indian DPDP Act, the regulatory approach to children's data prioritises securing verifiable consent from an identifiable adult, rather than mandating strict documentary proof of the legal parent-child relationship (i.e. verification is of the parent's identity only, not of parentage). Similarly, the upcoming amendment to Japan's Act on the Protection of Personal Information — while formally introducing parental consent protocols for children under 16 — codifies a flexible and business-friendly approach. The framework explicitly directs that flexible verification methods shall be permitted to avoid imposing an excessive burden on both consumers and businesses. By explicitly guarding against operational friction, Japan's model demonstrates how a major

digital economy can protect children without choking user onboarding or forcing businesses to build invasive, over-engineered identity verification technology.

Furthermore, this standard of "identifiability" can frequently be satisfied using data already available with the platform. Rather than forcing users to submit new, sensitive documentation — which goes against the principle of data minimisation — platforms should be able to leverage existing, privacy-preserving data points to reasonably verify that the consenting user is an adult. For instance, a platform might assess established account tenure, historical usage and interaction patterns, the presence of verified payment instruments, or previously completed age-assurance checks.

By allowing platforms to rely on existing contextual data to reasonably confirm they are interacting with an adult, this approach successfully balances the need for protective oversight with the principle of data minimisation. Adopting a similar standard in Australia would prevent the disproportionate privacy risks associated with collecting sensitive (and sometimes unavailable) familial records, while ensuring that vulnerable children are not arbitrarily cut off from vital online resources and communication tools due to a lack of formal legal documentation.

7. Consent for Use and Disclosure

Consent being the sole legal basis for processing children's data

Google has significant concerns on the practical implications of the proposed section 11(1)(a) of the Code, which requires that organisations must obtain consent in order to use or disclose a child's personal information. This means that organisations would no longer be able to rely on the "reasonable expectations" test under APP 6.2(a), which permits the secondary use or disclosure of personal information where the individual would reasonably expect such use or disclosure, and it is related (or, for sensitive information, directly related) to the primary purpose of collection. This deviates from a fundamental principle in the *Privacy Act 1988* (Cth) (**Privacy Act**) and the Australian Privacy Principles, which recognises that consent is not always required or appropriate. This is also significantly out-of-step with international frameworks such as the European General Data Protection Regulation (**GDPR**) and Singapore's Personal Data Protection Act (**PDPA**), which recognise legal bases other than consent. For instance, Singapore allows organisations to process a child's personal data without express consent for safety-critical functions that a reasonable person would consider appropriate, such as age assurance or protecting children from harmful content.

By strictly mandating consent for any secondary use or disclosure, the proposed section 11(1)(a) could inadvertently restrict organisations from relying on reasonable expectations to proactively process data in ways that are necessary to protect the safety and well-being of children in the digital environment.

Bundled consent

Read together, the proposed sections 14, 15 and 18, would require organisations to obtain separate consent (and notice) for each purpose or instance of collection, use or disclosure of personal information. The practical effect of such a requirement, borne out in countries with similar laws, is that every interaction with a service will begin with multiple screens of checkboxes to fill out. It is a fallacy that the more checkboxes a user checks, the better the comprehension — rather, overwhelming the user with a granular list of individual actions is more likely to undermine meaningful consent. When children and their parents are faced with repetitive and disruptive consent requests for every single data action, they become overwhelmed and are less likely to meaningfully read or evaluate the implications of their choices.

Google believes that clear, plain-language notices explaining routine, non-sensitive data processing give users a far better understanding of what they are agreeing to, even when a single "consent action" encompasses multiple related processing purposes. A proportionate, risk-based framework should reserve explicit, granular consent for high-risk operations — such as precise geolocation or biometric data collection — while recognising that simplified, purpose-based bundled consent is significantly more effective at helping users seamlessly comprehend and manage their everyday data. Furthermore, regulatory frameworks must account for the reality that every service provider maintains a distinct set of "essential processing purposes" critical to delivering their core service. Forcing separate consent mechanics for these essential operations when mandated by law provides little practical utility and risks rendering the consent process transactional rather than meaningful.

Requirement to refresh consent every twelve (12) months

The requirement for consent to be refreshed annually is particularly unusual and may cause children to be repeatedly interrupted by consent prompts they do not meaningfully engage with, or have children's access to services interrupted when consent lapses.

This framework, especially when coupled with onerous parental consent requirements, a consideration of BIOC on each use and disclosure, and a heightened consent standard, is not aligned with international benchmark legislation, and does not meaningfully increase privacy protections for children.

Accordingly, we recommend that:

(a) **Consent should not be the sole legal basis.** Rather, consent should be reserved for higher-risk processing where it is most important for users to make informed choices. Alternatively, if this requirement needs to remain, we recommend clarifying that purpose-based consents for similar processing with similar risks may be grouped within a single consent request. For example, the Singapore regulator provides that organisations do not need to specify every activity they will undertake when notifying individuals — rather, organisations just need to state their purposes at an appropriate level of detail for the individual to determine the reasons and manner in which the organisation will be processing personal data, in order to make an informed decision. Furthermore, we recommend expressly recognising that consent can be inferred where the use or disclosure of personal data is required for safety-critical functions such as protecting children from harmful content.

(b) **Consent should not need to be refreshed every 12 months.** Rather, consent should only need to be refreshed if there is a material change to the nature of processing or the purposes for which consent was given. Alternatively, if this requirement needs to remain, we recommend the following options:
    (i) Clarifying that consent can be deemed to have been validly refreshed if there have been no material changes to the processing.
    (ii) Recognising that the "current" consent requirement can be satisfied through the provision of persistent, easy-to-use privacy controls paired with periodic reminders. Meaningful privacy comes from empowering users with continuous control over their data, rather than imposing transactional blocks. For example, Google provides robust privacy controls within account settings and Family Link that users can adjust at any time, and sends regular, proactive reminders to users to complete a Privacy Check-Up. By maintaining these continuous account controls and sending periodic prompts to review privacy settings, platforms can actively engage children and parents in their data choices and satisfy the

policy goal of ensuring consent remains valid and current, without causing unnecessary service disruptions.

(iii) If any explicit requirement to refresh consent is codified, it should focus on the continued use of services across the age of consent threshold. For example, when a teenager reaches the applicable age of consent and elects to manage their account independently, Google requires the teenager to actively review and agree to Google's Privacy Policy and Terms of Service before the transition is complete.

This approach recognises the importance of maintaining flexible lawful bases for processing, and helps to avoid consent fatigue. Requiring separate consent requests for every use or disclosure may overwhelm children and their parents, which may paradoxically undermine the quality and genuineness of consent. This may also interfere with children's rights to access information and services if they or their parents do not engage.

8. Assent of Child

Google recognises the OAIC's deliberate intention to involve children in the consent process and supports the underlying objective of promoting digital literacy and a sense of autonomy for children. However, we disagree with the proposed approach.

Firstly, it is unclear what additional meaningful protection this "assent" requirement introduces in addition to parental consent, especially when the premise is that it is being obtained from a child who inherently lacks the legal capacity to provide valid consent in the first place.

Secondly, the Code introduces an unprecedented concept into privacy law. "Assent" as a distinct statutory prerequisite does not exist in the Privacy Act or international frameworks like the UK AADC. This means that new jurisprudence needs to be built to provide clarity on what this actually means for regulated entities.

Finally, it is likely to make little practical difference because companies will simply treat it as consent. Differentiating between "consent" and assent will be extremely difficult to implement at scale across services with large and varied user bases. To operationalise this at scale, platforms will likely comply by adding interfaces with an "I agree" button. As explained above, having more checkboxes does not lead to better comprehension, ultimately providing only the illusion of privacy.

We believe that meaningful, risk-adjusted and age-appropriate notices, complemented by appropriate default privacy settings, are the way to empower children to be more actively involved and informed about how their personal information is handled. Google already puts this into practice by providing privacy policies and "bite-sized" notices that are explicitly designed to be age-appropriate for children.

Furthermore, we deploy transparency tools tailored to new technologies, such as a U18-specific user notice in AI Mode — developed based on research with child development experts — which advises younger users to double-check important information and provides tips on how to do that. We also feature youth-specific onboarding flows, including a Teen GenAI Literacy Guide and accompanying videos, to actively support teens on their learning journeys and help them understand what the technology can and cannot do.

In addition, we offer easy-to-use tools that respect the preferences of families by providing the flexibility to manage their unique relationships with technology in line with the child's evolving developmental capacity. For instance, Family Link allows parents to set up supervised accounts for their children, set

screen time limits, and more. Teens can also opt to continue parental supervision through Family Link after they turn 13.

We believe that the use of these existing, context-rich tools and protections allow children to be meaningfully informed and empowered, and take into account the evolving capabilities of the child, while reducing unnecessary transactional friction and burden which would inevitably arise from the assent requirement.

Accordingly, Google recommends clarification that the use of such tools would be sufficient, without the need for a separate children assent step.

9. Transparency

Google supports the principle of enabling children to make informed decisions, but is of the view that entities are best placed to understand their audiences and how best to tailor transparency information. On this basis, the proposed transparency sections should not be overly prescriptive and should afford entities with flexibility in how those obligations are met, particularly for services with mixed-age audiences.

Overly prescriptive requirements inherently limit an organisation's ability to design privacy notices in a manner that is most appropriate and accessible for its users. When regulations mandate exhaustive, itemised descriptions or rigid structural formats, organisations are forced to provide verbose notices that quickly devolve into complex "legalese". This approach is counterproductive — rather than fostering transparency, such technical and lengthy disclosures overwhelm the average user and actively reduce the notice's overall comprehensibility and effectiveness. For younger audiences already navigating complex digital environments, avoiding this kind of forced cognitive overload is essential to preserving their ability to actually understand and control their data. Instead, the transparency requirements should focus on the "why", and not the "what", by explaining the core reasons for data processing. By providing a concise objective rather than prescriptive details, the notice reduces cognitive load and ensures users feel informed and in control without being bogged down by excessive detail.

While Google agrees with the principle that child-facing privacy policies should be clear, concise, transparent and easily accessible, there should not be prescriptive requirements in relation to the content which goes beyond the existing APP 1 and APP 5 requirements, or specific requirements in relation to position, font size and type, and so on. In particular, we note that section 23(6) requires specific disclosures about anonymous and pseudonymous dealings, and h*ow the organisation manages personal information linked to pseudonyms*. This goes well beyond existing transparency requirements of APP 1.3 and 1.4 and would require organisations to provide technical disclosures that are unlikely to be fully understood by children — thereby undermining clear communication and causing confusion for children who are trying to make meaningful choices about their privacy.

Further, there should not be multiple notice requirements which mandate disclosure of different types of information. For example, in addition to the transparency requirements in Division 3 of the Code:

(a) When seeking a child's *assent* (as discussed above), the proposed section 20(5)(b) requires organisations to notify the child of certain information such as the period for which parental consent would be relied upon, and the consequences of assenting or not assenting — which differs from the information usually required under APP 5.

(b) The proposed section 35 also imposes a separate obligation which requires organisations to provide end users with information about the kinds of personal information the organisation

processes, the kinds of inquiries and complaints that end users can make and the potential outcomes of those inquiries or complaints.

These various requirements, alongside existing privacy policy and collection notice requirements in APPs 1 and 5, create confusion and notice fatigue for users, as well as operational challenges for service providers. Accordingly, we recommend that the Code should not introduce new notice or transparency requirements, and instead should focus on ensuring that organisations satisfy the existing APP 1 and APP 5 requirements in a child-friendly way.

10. Individual Rights; Complaints

Google acknowledges the importance of children's control over their personal information. However, we would urge the OAIC to consider:

(a) Recognising that complete data destruction is not the only — or always the most appropriate — mechanism to give individuals agency and autonomy over their own information, reduce the risk of unauthorised disclosures or other similar goals. The same can be achieved if the entity has applied robust de-identification techniques such that the remaining data can no longer identify any particular individual. This approach aligns with established global privacy frameworks, which widely recognise that de-identified data falls safely outside the scope of deletion mandates. By recognising de-identification as a form of "deletion", organisations can simultaneously uphold user privacy, maintain resilient digital infrastructure, and retain aggregated, non-personal data that is vital for service improvements and research. Accordingly, a right to de-identification is already sufficient.

(b) Qualifying that the right to deletion is not absolute, and, like other activities of processing, must be fundamentally anchored to the principle of purpose limitation. Companies should be able to retain personal information as long as at least one of the purposes for its collection remains valid. It is important to remember that companies need to process personal information for purposes that extend beyond mere front-end service provision. For example, certain critical secondary business functions — such as optimising cybersecurity models or improving service safety — may require retention of historical data containing some personal information to be effective. Such purposes can continue to be valid after the individual has discontinued their relationship with the company or requested deletion.

(c) Recognising that a very prescriptive mandatory destruction obligation creates significant operational complexity for large-scale services, where personal information is distributed across multiple systems and may be embedded in technical logs and backups.

(d) The requirement to provide information about an organisation's information handling practices is overly onerous. In particular, the requirement to provide information about automated decision-making (**ADM**) compels organisations to provide meaningful information about the existence of ADM, *the logic involved*, the consequences of such decisions, and whether profiling has been used. This ADM disclosure obligation represents a materially higher compliance burden as compared with existing and incoming APP obligations, including the new APPs 1.7-1.9 (which do not require disclosure of information about the logic involved). This means that organisations would need to provide technical, potentially commercially sensitive information to children — which does not even need to be provided to adult users, and may not be understood by children. This would also require organisations to develop separate processes and dedicate resources to respond to

such requests from children, which creates an additional operational burden that does not necessarily result in enhanced privacy protections.

Further, the mandated timelines to respond to access, correction and destruction requests are too prescriptive and represent a significant operational burden. We believe that the current approach of requiring organisations to respond within a "reasonable period" is sufficient. While we agree it is important for organisations to respond to requests within a reasonable time, data protection laws should not prescribe arbitrary response timeframes as each individual request or exercise of a right is unique and of varying complexity. Timelines should remain flexible to account for legitimate operational challenges that organisations may face when responding to requests, such as the need to verify the individual's identity, locate personal data across multiple systems, assess whether exemptions or limitations apply, consult with legal advisers on complex or novel issues, redact third-party information and coordinate responses where multiple organisations are involved. Accordingly, the existing formulation is sufficient, supported with OAIC *guidance* that this should generally be within 30 days.

If timelines need to be included, the Code should consider the timelines in benchmark international legislation such as Article 12(3) of the GDPR, which provides controllers with 1 month to respond to rights requests, extendable by a *further* 2 months where necessary, taking into account the complexity and number of requests. This approach recognises that whilst straightforward requests may be resolved quickly, more complex requests require additional time for thorough and compliant responses.

Similarly, Google supports the objective of accessible, child-friendly inquiry and complaints processes. However, as noted in relation to individual requests, the introduction of specific statutory timeframes for responding to inquiries and complaints is a significant new compliance commitment which does not cater for inquiries or complaints of varying complexity. Accordingly, there should not be hard-coded timelines, and organisations should only be required to respond within a "reasonable period". Alternatively, if timelines must be introduced, there must be a regime that allows for appropriate extensions as discussed above, and these should be considered alongside the timeframes for responding to individual requests, to ensure a coherent and workable scheme of response obligations.

11. Privacy Impact Assessments (PIAs) and Privacy Reviews

Google builds with child-centric design principles from the outset and strongly supports PIAs as critical tools for mitigating risks to children. While we endorse the PIA requirement in principle, we recommend a flexible, principles-based approach rather than mandating specific formats or rigid content requirements. If an organisation already conducts thorough PIAs as a core part of its privacy compliance program, forcing standalone, Australia-specific, and child-specific PIAs in addition to that creates a highly duplicative compliance burden that is unlikely to deliver measurable enhancements to children's privacy.

It is difficult to see how the requirement to maintain an online register of PIAs yields meaningful privacy benefits. If platforms are required to publish the PIAs in their entirety, it creates serious risks to commercial confidentiality and operational security. Alternatively, if the requirement is restricted to disclosing merely the titles and dates of assessments to protect that confidentiality, the mandate devolves into an empty administrative hurdle that delivers zero practical transparency or safety benefits for children. Because neither approach yields a positive privacy outcome, the Code should focus on ensuring that organisations conduct appropriate PIAs in order to assess and mitigate risks to children, without creating an additional layer of bureaucracy through specific formats, content and maintenance of a public register.

Similarly, the requirement to review privacy practices, procedures and systems on an annual basis is unnecessary. The 12-month review cycle is arbitrary and does not reflect how privacy practices and risks actually evolve in practice. For organisations operating multiple services with varied user bases, an annual review requirement, irrespective of whether there has been any material change to information handling practices, will result in compliance exercises conducted for their own sake, rather than exercises that add genuine privacy value. Rather, the review obligation should be linked to material changes in the organisation's services, information handling practices, or the applicable legal and technical landscape. If an organisation undergoes multiple material changes within a 12-month period, each change would trigger a review — which may in fact be conducted more frequently than once every 12 months. On the other hand, a mandatory annual review would force businesses to allocate significant resources to formulaic compliance exercises which may not enhance privacy protections.