Response to OAIC's Issues Paper on the development of its Children's Online Privacy Code - 31 July 2025

Introduction

Google welcomes the opportunity to provide feedback on the Office of the Australian Information Commissioner's (OAIC) development of the Children's Online Privacy Code (the Code). These are important and complex issues that merit thoughtful consideration and input from a wide range of stakeholders and we appreciate the OAIC's request for comment.

Google strives to maintain safe and positive online experiences for all of our users, and that is especially true for minors. We recognise the unique vulnerabilities of minors in the digital environment and support the OAIC's objective to enhance privacy protections for them.

We have consistently invested in research, policies and practices to offer age-appropriate ways for minors to explore, learn and participate in the online world as they grow. Such efforts are designed to prioritise our youngest users' wellbeing and to respect each family's unique relationship with technology. These efforts empower minors to be confident digital citizens and develop lifelong practices that will serve them well into adulthood. As part of our efforts, we support sustainable and smart regulation that respects users' privacy, access to information and rights to seek information and freedom of expression that can adapt over time as technology evolves.[1]

Our comments provide information on Google's approach and contain our recommendations for how the OAIC can best protect minors and families while also enabling access to the digital tools and experiences that are a foundational part of minors' everyday lives.

We have responded to the questions in the Issues Paper, grouping them by theme rather than chronologically. Where appropriate, our responses distinguish between children under the age of consent – for Australian users, 13 years of age (U13) – and minors above the age of consent

[1] We have led the industry by building and supporting the expansion of products like YouTube Kids—released in 2015 and used by families to access diverse, high-quality, playful and educational content from around the world—and Family Link—a parental controls app that allows parents to manage their child's privacy settings, among other things. We have invested heavily in programs like Designed for Families in the Play Store which helps ensure families have access to high-quality apps that protect children's privacy; and Search privacy and safety controls, which help users control their online footprint and blur unwanted explicit content, and School Time, which gives parents control over how and when their teens use Android devices. We also provide resources and guidelines for creators and developers, including programs that provide guidance on how to create great content for families.

but below 18 (teens). We use the terms “minors” or “U18” to refer to all users under the age of 18.

The following points are a high-level summary of our feedback to the Issues Paper and of our recommendations for the Code. In short, Google recommends that the Code should:

1. **Recognise that the “best interests of the child” is a dynamic concept**. This is most effectively addressed in each specific context by implementing privacy-by-design-and-default and privacy impact assessment processes. A risk-based approach can identify and enable protections for minors where and when they are most needed.

2. **Be principles-based, flexible and aligned with global standards** regarding the protection of minors and their privacy.

3. **Take into account minors’ full range of rights**, including the right to privacy, access to information, to express views freely on matters affecting them (where capable), and freedom of expression, and reflect an understanding that these rights must be applied fairly and proportionately, taking into account how they relate to each other.

4. **Reflect a risk-based and proportional approach**, especially in relation to age assurance, and should seek to ensure that the needs of minors of different maturity and capacity are appropriately considered in the context of different risks of harm. A one-size-fits-all approach will not protect minors’ privacy effectively. What works for children U13 does not necessarily apply to teens, especially older teens; what works for one family’s choices and circumstances may not be what works for another; and what makes sense for a high-risk service provider may not make sense for a lower-risk service provider.

5. **Recognise that age assurance is most effective and responsive to protecting privacy rights when conducted at the level of individual online services**, or parts of those services. Users should be protected where they are. Services should take reasonable action to understand the age of users, including a risk-based and proportionate approach to age estimation, and apply appropriate protections based on that age.

6. **Be consistent with the principles of data minimisation, purpose limitation, and retention**, in particular, by promoting the use of privacy-enhancing technologies (PETs). For example, requiring high levels of assurance in age verification may come at the expense of increased data collection and, depending on methods used, impact user privacy.

7. **Acknowledge the benefits of personalisation and, where appropriate, consider reasonable restrictions**. Personalisation, provided in the context of a service, is aligned with minors' 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 risks that minors 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 personalised advertising, and to enable the collection and use of data to support important functions, such as to deliver contextual advertising and improve the safety, performance and functionality of services, which benefits all users, including minors. Google supports regulations that prohibit personalised advertising for minors.

Additionally, Google encourages the OAIC to develop supplementary guidance on how the OAIC would interpret the Code, and provide examples of good practices.

Responses to Issues Paper questions

I. Scope and Application of a Children's Privacy Code

A. The Code should apply to services which are likely to be accessed by minors and allow APP entities to be flexible in their approach to protecting minors

Questions in Issues Paper addressed in this response
2.1 What threshold should determine when a service is considered 'likely to be accessed by children'
2.2 "Likely to be accessed by children" is the same standard as the UK's Age Assurance Design Code. Is there any evidence as to the practical effectiveness of the threshold in that context? (AU)
2.3 What steps should APP entities reasonably be expected to take to assess whether children are likely to access their services?
2.4 What role, if any, should age gating or other access control mechanisms play in meeting obligations under the Code?
2.5 Are there alternative approaches APP entities could take to meet their obligations under the Code, beyond age gating or age verification methods? If so, is there any evidence on the impact of such approaches on children's access to services or privacy outcomes?

2.6 Are there classes of APP entities, personal information, or activities of entities, for which different requirements under the Code may be appropriate? If so, what considerations should inform that approach?
2.7 How should the Code accommodate for the varying roles, functions and risk profiles of different kinds of services, activities or personal information?

The OAIC should adopt the "likely to be accessed by children" standard to determine what services are in scope of the Code

Service providers have the best understanding of the nature of their service, the data processing involved, types of content available and the risks that can arise, and should protect users wherever they are based on that understanding. To that end, Google is supportive of the Code applying to services which are "likely to be accessed by children", as used in the UK's Age Appropriate Design Code (AADC).[2] This standard is both clear and appropriate. Aligning with this approach would ensure consistency with developing global regulatory and industry standards, provide greater regulatory certainty, and reflect reasonable user expectations.

We also support the Code adopting the same tests and factors included in the UK AADC to determine whether the threshold is met. This promotes consistency, fosters interoperability, and provides greater legal clarity. Aligning with existing standards means service providers can benefit from, and build on, established frameworks and best practices.

For example, Google recommends that the Code should:[3]

- Enshrine the principle that the threshold is met where the possibility of a minor accessing the service is *more probable than not*.
- Require consideration of the ways in which the service is accessed and measures put in place to prevent minors' access, including reasonable age gating and age estimation.
- Encourage a "common sense approach" as to whether the "likely to be accessed" test is met.
- Seek to limit perverse outcomes, such as requiring providers of restricted services to make their services appropriate for minors or provide parental tools.

The Code should allow APP entities to determine appropriate protections in light of their services

[2] *See* UK Information Commissioner's Office, Age Appropriate Design: A Code of Practice for Online Services (2020), 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/.

[3] Ibid., see Services covered by this code | ICO.

Different APP entities should have the flexibility to engage with, and treat minors in different ways based on the nature of their service, their approach to understanding age, and their application of appropriate protections.

For services that are primarily targeted at children U13, all users of such services should be treated as minors. This is in line with other regulations like the US Children's Online Privacy Protection Act (COPPA).

Where services are intended for users above the age of 18, age-gating combined with appropriate age assurance provides an important protection to help mitigate the risk that minors gain access to services that are not designed for them and that are intended solely for adults. More data-intrusive methods (such as verification with "hard identifiers" such as government IDs) should be limited to high-risk services (e.g., pornography).

For services which are not primarily targeted at children under the age of consent nor intended only for adults, reasonable steps might include implementation of age estimation techniques and application of appropriate protections proportionate to the risks posed by the service. However, we encourage the OAIC in developing the Code to recognise that any method to estimate the age of users across services comes with tradeoffs, such as potentially unduly restricting access to important information and services. Implementation of age-estimation should be risk-based, preserve access to information and services, and respect privacy.

As estimation techniques are novel and evolving, any requirements should be flexible enough to evolve along with technological developments and be flexible enough to evolve along with technological developments and provide reasonable protection from liability for good-faith efforts to develop and implement improved solutions in this space. A flexible approach is better able to evolve with evolving customer interaction models than specific prescribed steps, which are impractical and potentially counterproductive.

Google also encourages the OAIC to ensure that the Code has the necessary flexibility to enable technological evolution and promote innovation in this space. The tests and factors listed above should naturally result in an APP entity being able to determine what methods would be considered "reasonable steps" in its ordinary course of business.

<u>Responsibility for age assurance should remain with the services that best know the potential risks posed by their content and features</u>

We do not agree with certain recent industry proposals that mobile app stores or device operating systems take on the obligation to verify all users' ages and share that information with all developers or websites. Minors access the Internet through many different ways, from mobile phones to desktop computers to gaming consoles. A focus on app stores alone fails to keep minors safer online - only restricting access to apps on mobile devices, which is just one

of many ways minors access information online. For example, minors would be able to continue to access and sign into social media via web browsers, sideloaded or pre-loaded apps and alternative pre-installed app stores, leaving them exposed to apps that have not invested in minors' safety. A focus on operating systems fails for similar reasons. This is why a multi-layered ecosystem-wide solution that continues to place responsibility on services is a better approach.

More worryingly, the current app store proposals being promoted by certain parts of the industry would require the sharing of granular age-band data with millions of developers who do not need it - and without user or parental consent. Similar risks are posed by some of the operating-system proposals. We have strong concerns about the risks of sharing such data (as envisaged by the proposal), especially the risks to minors.

In addition, age checks at the operating system or app store level often fail to protect minors on shared devices. Families frequently share devices, therefore relying on age assurance at app store or operating system level is insufficient for ensuring that a minor is actually protected when in an app or on a site if they are using a shared device. This also applies to hand-me-down device cases, as any app store age restriction will have likely been satisfied and a minor user would be able to simply use any app unrestricted.

B. All services that are likely to be accessed by minors should be covered by the Code

Questions in Issues Paper addressed in this response
1.1 Are there additional APP entities, or a class of entities, that should be covered by the Code? Please provide reasons or evidence to support your view.
1.2 Are there any APP entities, or a class of entities, that should be excluded from the Code's application? If so, on what basis?
1.3 Is there criteria that should be used to determine whether a particular APP entity, or class of entities, is appropriately included or excluded from the scope of the Code?

Google considers that all services that are likely to be accessed by minors should be covered by the Code, with the exception of those services discussed below as requiring exception (e.g., services provided by educational institutions, etc.). However, strict requirements should only apply where the risks and likelihood of harm merit their application.

It would be appropriate to exclude the following from the remit of the proposed Code: Cloud services; enterprise accounts or services; and business-to-business services. These are not

likely to be accessed by minors. Additionally, educational institutions and educational technology services should be considered separately from the Code given their unique context, roles and responsibilities.

II. Understanding and Respecting Minors' Capacity, Consent and Best Interests

A. The Code should reflect a nuanced and proportionate approach to consent and minors' capacity for consent

Question in Issues Paper addressed in this response
6.4 How can APP entities obtain genuine consent from children, or their parents or guardians, for the collection of sensitive information?
9.1 How can APP entities obtain genuine consent from children, or their parents or guardians, for the use or disclosure of their personal information, while ensuring that they comprehend the implications of such use or disclosure?

Consent requirements should be limited to higher-risk processing and recognise risk of "consent-fatigue"

Google supports providing all users with meaningful information about, and control over, how their personal information is processed. However, the Code should recognise that consent is not suitable for all situations, especially if processing personal information is necessary to operate the service the user requested. We therefore support the OAIC's continued recognition of multiple legal bases for processing. Any consent requirements should focus on higher-risk processing (e.g., processing of precise geolocation information or biometric information for the purpose of uniquely identifying an individual) where it is most important for users to make informed choices.

Consent works best when it is used in a proportionate manner, and is informed and user-centred. This means that consent is relied upon only where appropriate, considering the relevant circumstances. In the context of minors, this will often depend on whether minors have the capacity to exercise real choice and control, and if it is appropriate for such minors to exercise such control.

This proportionate and risk-based approach also helps avoid the perverse effect of "consent fatigue". Consent fatigue would be a particularly troubling outcome for minors who are learning how to engage and use technology, and to manage their privacy and online safety sustainably as they become adults.

In presenting consent requests to minors, the core processing purposes or objectives should be made clear, without overwhelming the user with a granular list of individual actions. The Code should recognise that - if and where consent is required - APP entities can simplify consents, and present purpose-based consents for similar processing with similar risks, to help ensure both minors and parents (i) easily understand the purpose(s) for which the consent is being sought; (ii) are not faced with repetitive and disruptive requests for consent; and (iii) can engage in holistic consideration of data processing and their choices.

Ensuring minors' consent is "genuine" requires a contextual approach

Where consent is required, organisations should provide meaningful, easy-to-use mechanisms that allow users to easily determine how their personal information is collected and used, in a manner that is appropriate for the context. The method and format of consent should also take account of relevant circumstances of the service and processing, and applicable safeguards.

Genuine consent will be helped by:

- **Audience-Appropriate Information**: Meaningful transparency is key. Information about data practices should be presented in clear, concise and age-appropriate language, potentially utilising visual aids or interactive elements that may make the information more friendly for minors (or indeed, any user).
- **Avoiding Deceptive Practices**: practices designed to trick or coerce minors into providing personal information should be explicitly prohibited. This is an area in particular where the OAIC could highlight positive examples of notice and, where appropriate, consent practices.

Consent requirements should acknowledge differences in minors' maturity and capacity, and the different risks they face online

Teens from age of consent to 18 should generally be considered to have capacity to consent and should not require parental consents. When parental consent is appropriate and required, such as for children under the age of consent, it should be done in a technology-neutral, flexible way to allow for technological innovation.

There is also a range of differences in maturity, capacity and risks of harm between children below the age of consent and teens. As a result, there are important differences in how to support the best interests of children U13 and teens. Google recommends that the Code should guide services to provide protections for minors in a way that respects their development and the ability of families to make choices about how they use technology. Teens have increased developmental capacity and agency and it is important for them to access information as they continue learning.

This approach would also reflect the UN Convention on the Rights of the Child (UNCRC), which Australia ratified in 1990. In particular, Article 12 of the UNCRC enshrines the right of minors, who are capable of forming their own views, to express those views freely in all matters:

> *"States Parties shall assure to the child who is capable of forming his or her own views* ***the right to express those views freely*** *in all matters affecting the child, the views of the child being given due weight in accordance with the age and maturity of the child"* (Article 12(1), UNCRC, emphasis added).

Considerations around consent should reflect these distinctions and be grounded in a risk-based, proportional approach. Such an approach would also support teens' need for access to high-quality digital tools that help them learn and develop, exercise their rights, flourish in the global economy, and connect with friends and family.

Consent requirements should be considered against the impact on minors' rights, including to access information online

In considering issues related to consent and parental supervision, we also encourage the OAIC to consider the full spectrum of minors, the range of familial relationships, and how to support minors' best interests, including within contexts that may be important for the minor's development.

In particular, Google encourages the OAIC to recognise the importance of minors to have the freedom to seek, receive, and impart information, and to have the freedom to manifest their own beliefs. The Code should acknowledge the importance of facilitating and balancing the rights of a minor, especially the right to freedom of expression (Article 13, UNCRC),[4] and freedom of thought, conscience and religion (Article 14, UNCRC).[5]

For example, minors may live in unsupportive households or simply seek privacy as they safely explore issues around identity, religion, politics, or issues that are important for their development. This can be particularly relevant for underrepresented or vulnerable communities. For example, leading LGTBQ+ advocacy organisations have noted that parental consent requirements could prevent minors from accessing important mental health and

[4] Article 13(1), UNCRC: "*The child shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of the child's choice.*"
[5] Article 14(1) UNCRC: *"States Parties shall respect the right of the child to freedom of thought, conscience and religion."*

suicide prevention information and community-specific resources and expose minors to mental and physical harm.[6]

The Code should provide clear guidance on mechanisms for obtaining and verifying parental consent, acknowledging the practical challenges without creating requirements that hinder access to beneficial services.

Parental consent requirements can also be challenging for parents. It is not always feasible for parents to provide timely consents (for example when parents are at work or are otherwise not able to meaningfully engage with the consent request). As such, relying too heavily on parental consent may disproportionately delay or restrict a minor's access to online services. Parental consent requirements should be developed considering such practical challenges, and the need to ensure that minors' access to age-appropriate services (and ability to exercise their rights, including to expression and to express a view freely on matters affecting them) is not unreasonably curtailed as a result of inappropriate and unnecessarily disruptive parental consent requirements.

B. Approach to parental consent should be considered in light of the best interests of the child and implications on minors' rights to privacy and to access their personal information

Question in Issues Paper addressed in this response
14.3 In what circumstances should a parent or guardian be able to make an access request on their child's behalf and receive a copy of their child's personal information? How should the balance be struck between a parent's right to protect the best interests of their child and the child's right to privacy, when APP entities are dealing with access requests for a child's personal information?
15.3 In what circumstances should a parent or guardian be able to make a correction request on their child's behalf?

<u>The Code should provide clear framework to help APP entities navigate competing rights and interests, which is sufficiently flexible and focused on the best interests of the child</u>

[6] *See* The Trevor Project, *Mental Health Care Access and Use among LGBTQ+ Young People* (2024), https://www.thetrevorproject.org/research-briefs/mental-health-care-access-and-use-among-lgbtq-young-people/ ; *see also* Carlos Gutierrez, *The Dangers of Legislative Parental Consent Requirements*, LGBT Tech (Oct. 11, 2023), https://www.lgbttech.org/post/legislative-parental-consent-requirement.

Google supports all our users' ability to access, correct, delete and port the data they have provided to Google; these are foundational user rights and practices that support user control and trust. Google offers users a range of user-friendly and accessible tools to manage their information, including, for example, the ability to delete their entire account, or activity from particular services. These tools are extended to supervised Google Accounts that Google enables parents to set up and manage for their children through Family Link.

However, like any right, these are not absolute. Google encourages the OAIC to implement a clear framework under which competing rights and interests can be evaluated once a user has made an access request, or to enable APP entities to ensure that a user requesting information has the right to receive that information. We also encourage the OAIC to enable service providers to take reasonable and proportionate steps to verify the request prior to responding, including to avoid unauthorised disclosure.

It is important to ground rights in the Privacy Act (such as access and correction rights) in the best interests of children. It is therefore important to consider how to implement appropriate protections for such rights considering the best interests of the child. In particular, to recognise and seek to prevent the infringement of minors' rights by third parties who seek or request to gain access to their personal information (including by the minor's parents and family members in certain circumstances), in particular where the minor has capacity.

For example, for children U13, it is typically appropriate for parents to exercise these rights on the child's behalf. However, for minors over the age of consent (and who are not in a supervised account experience), there are very limited circumstances where a parent should be able to exercise these rights on behalf of a minor, such as where the minor lacks the legal capacity or the minor is deceased, provided those are subject to a court order.

C. The Best Interests of the Child (BIOC) principle should be a key component of the Code and integrated into privacy-by-design-and-default

Question in Issues Paper addressed in this response
14.1 What mechanisms are needed to ensure children can easily access their own personal information?
14.6 Do you have any specific views on how APP 12 should be applied or complied with in relation to the privacy of children?

<u>The best interests of the child should be a key component of the Code</u>

Long-standing consensus among child development experts is that when considering a minor's best interests, it is important to holistically consider all relevant aspects of the minor's experience and circumstance, including their safety, physical and mental wellbeing, privacy, agency, access to information and freedom of participation in society.

Google agrees that online services used by children U13 and teens should be required to assess the collective best interests of minors within comparable developmental stages, based on expert research and best practices. This is to ensure that products and services are age-appropriate, and developed, designed and offered considering the collective best interests of children U13 and teens.

Google encourages the OAIC to highlight positive examples of child-centred design in the Code, which reflect on the different components of a minor's best interests. This would ensure that the best interests of the child principle forms a key component of the Code, and will be an effective incentive for service providers.

Privacy-protective default settings for minor accounts should be encouraged; restricting access to services should be avoided

In certain circumstances, for example where services or features are designed for and intended to be used only by users above the age of 18, it is in a minor's best interest for their access to be restricted by service providers.

However, in all other cases, the most effective approach to balance (and allow the minor to exercise) the rights available to them is to focus on providing privacy-protective settings *by default* (designed using a risk-based approach) especially for minor accounts, and ensuring data minimisation and limited visibility *by default*.

Google considers that all default privacy settings provided to minors by the online service, product or feature should generally be configured to settings that offer a high level of privacy. However, there may be occasions where the underlying processing objectively enhances minors' experience of the applicable service, product, or feature. In such cases, it may be appropriate instead for the APP entity to offer the option to change the setting.

The Code should promote privacy standards that allow minors to enjoy more age-appropriate, inclusive and relevant online experiences that meet the needs or requirements of such users and their parents.

The Code should reflect the benefits of personalisation to minors and their use of online services

Google recommends that the Code recognises the distinction between personalisation and personalised advertising, and acknowledges that personalisation provides a range of benefits to minors.

For example, personalisation provided in the context of a service, aligns with minors' developmental needs and supports their ability to access and discover high-quality content and age-appropriate information online. Content recommendation is also an important means to identify and mitigate risks that minors may interact with content that is not age-appropriate.

The Code should provide guidance to enable the collection and use of personal information to support important functions, such as to deliver contextual advertising and improve the safety, performance and functionality of services, which benefits all users, including minors.

Google therefore encourages the recognition that a contextual approach is necessary (to avoid a one-size-fits-all approach) to personalisation, in order to consider the full range of benefits that minors experience (e.g., online safety, educational material, and digital and media literacy).

<u>The Code should integrate the BIOC principle into the design of services and Privacy Impact Assessment (PIA) process</u>

Google's goal is to build with child-centric considerations from the outset. We believe PIAs are critical tools for identifying and mitigating risks to the privacy of minors.

The Code should take a principles-led approach to the PIA process, to ensure a meaningful exercise in assessing and mitigating risk for minors.

Google also encourages the OAIC to recognise the value in interoperability, and that service providers will be undertaking impact assessments related to rights of minors in the digital environment for a range of regulatory reasons.

The Code should therefore provide clear guidance on how to effectively integrate child-centric considerations into existing PIA frameworks. This would enable a greater focus on the substance of risks and mitigations, rather than the format and manner of different assessments.

III. Transparency and Communication Strategies

A. Transparency requirements should consider different age ranges and capacities, taking into account the nature and context of the service

Questions in Issues Paper addressed in this response

3.1 Would age-based guidance be appropriate and assist APP entities in tailoring protections and interfaces appropriately and effectively?
3.2 In terms of providing guidance for the processing of children's personal information by APP entities covered by the Code, how appropriate do you consider the above age ranges would be?
3.3 Please provide any views or evidence you have on children's development needs, in an online context in each or any of the above age ranges.

<u>While taking age into account for developing regulatory guidance is appropriate, defining strict requirements according to age-ranges will result in practical difficulties for compliance and over-collection of personal information</u>

Google welcomes the OAIC's acknowledgement that the range of development needs among minors (including due to age, neurodiversity and learning difference, among other factors) requires a contextual approach to age-based guidance as opposed to a "one-size-fits-all" approach.

Google therefore encourages the OAIC to ensure that the Code reflects this acknowledgement and recognises that there will often be exceptions and contexts that require different approaches.

For example, on this basis, Google does not support using age-ranges to define strict requirements. Exceptions will always exist to the relevant assumptions (used for such age-ranges), and there are technical and practical complexities in estimating ages of children U18. There is therefore a concern that, to ensure compliance with age-based obligations, services could be forced to use more intrusive age-assurance measures. This prescriptive approach also fails to recognize and support families in making their own decisions as to what is appropriate for their child.

As a result, Google encourages the OAIC to draft guidance that is consistent with approaches in other jurisdictions, which reflects the need to consider the broader context when imposing restrictions on minors' participation in the digital environment. For example:

- The UK AADC (which includes age-ranges as a guide, but does not prescribe specific requirements which services must meet for each age-range), states: "*Children are*

individuals, and ***age ranges are not a perfect guide*** *to the interests, needs and evolving capacity of each child*" (emphasis added)[7]

- UNICEF's report on best interests in the digital environment points out the need for a holistic interpretation and the importance of youth participation in the online sphere, noting in particular that a blanket application of child safety obligations (such as age-range based obligations), could "*be a measure that may simultaneously infringe on other rights, such as right of access to information or right to participation*".[8]

- UNICEF also published a policy note in April 2025 specifically on an age-based social media ban, which identifies possible unintended consequences of blanketly applying age-based rules.[9] The policy note indicates that UNICEF considers efforts to make social media platforms safer is more important and more likely to be effective than restricting access to them.[10]

- The Irish Data Protection Commission also emphasises the importance of taking a holistic approach when applying the best interests of the child principle in the context of making decisions as to the processing of personal information of minors and references to the UN Committee's statement that the best interests principle "*is aimed at ensuring both the full and effective enjoyment of all the rights recognised in the*

[7] ICO, Age Appropriate Design Code, 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/.

[8] The report notes, for example, that: "The best interests of the child principle and the proportionality principle are two fundamental concepts, particularly when making decisions that affect children. These principles, while seemingly distinct, often intersect and inform each other in various legal contexts. The proportionality principle serves as a crucial tool for resolving conflicts between competing interests, particularly when a state seeks to limit or interfere with human rights that are related to those competing interests. The best interests of the child is one of the rights within a proportionality test. States have the duty to protect children online and businesses have the responsibility to respect children's rights. However, a policy aimed at enhancing child safety online such as blanket bans on social media access, for example, can be a measure that may simultaneously infringe on other rights, such as right of access to information or right to participation." Didem Özkul, Steven Vosloo & Bella Baghdasaryan, UNICEF, Best Interests of the Child in Relation to the Digital Environment 14 (2025), https://www.unicef.org/innocenti/media/10571/file/UNICEF-Innocenti-Best-interests-child-digital-environment-brief-2025.pdf.

[9] *See* UNICEF, Drawing a Line in Digital Spaces: Age-Based Restriction of Social Media 2 (2025), https://www.unicef.org/media/170666/file/Policy%20note_age%20restrictions%20social%20media-new.pdf.pdf.

[10] *See Social Media Ban*, UNICEF, https://www.unicef.org.au/unicef-youth/staying-safe-online/social-media-ban-explainer?srsltid=AfmBOoq6wcC8arD5A82iTFNW9IBgL_oljlUxbJpwbNUmCVK1Cidi7mw6 (last visited July 29, 2025).

[UNCRC] and the holistic development of the child.[11]

B. The Code should encourage a multi-layered approach to transparency and communicating information

Questions in Issues Paper addressed in this response
4.1 What communication methods should APP entities use to ensure privacy policies are meaningfully understood by children of different ages, abilities and backgrounds?
4.2 How should APP entities ensure APP1 obligations are met when their services are used by both adults and children, particularly when children are not the intended primary users?
8.1 What methods can be employed by APP entities to effectively notify or ensure children are aware of data collection practices in a manner that is age-appropriate and can be easily understood by children?
8.2 How can APP entities ensure that notifications are accessible to children with diverse needs, including those from culturally and linguistically diverse backgrounds, or living with disability?
8.3 Are there circumstances in which an APP entity would be justified in taking no steps to notify or ensure children are aware about data collection practices? How can we minimise these instances to ensure that APP entities are adopting a best practice approach when it comes to notification and awareness?
11.2 What steps should APP entities take to communicate with children (or their parents or guardians) about the risks of cross-border data transfers?

Service providers are best placed to understand their audiences and how best to tailor transparency information – the Code should not be overly prescriptive

[11] *See* Ireland Data Protection Comm'n, Fundamentals for a Child-Oriented Approach to Data Processing 18-20 (2021), https://www.dataprotection.ie/sites/default/files/uploads/2021-12/Fundamentals%20for%20a%20Child-Oriented%20Approach%20to%20Data%20Processing_FINAL_EN.pdf.

Google recommends that the Code should encourage a multi-tiered approach to transparency and communicating information, including through the use of written notices, images, videos and just-in-time notices.

To ensure the Code is practical, it should also encourage the tailoring of communication strategies to different audiences without being overly prescriptive, noting that services will be best-placed to understand how audiences interact with their services and what combination of communication strategies, content and settings will be most effective at conveying required transparency information. This highlights the need for a flexible, risk-based, and proportionate approach to the Code's requirements regarding presentation of information to relevant audiences. This is especially relevant for services with mixed-age audiences.

It would be helpful for the Code to acknowledge that different audiences have different needs and interests when it comes to transparency information. For example, information available to parents would not be appropriate for, would not be understandable by, and should not be required to be made available to, children U13. Where children U13 are concerned, parents should generally determine the relevant settings, including to decide whether (and in what circumstances) their child should have the ability to change certain settings. This is because parents generally understand, and are best placed to gauge the developmental needs of the child.

Google encourages the OAIC to consider and align with well-established approaches to transparency in other jurisdictions, which typically require a clear and concise (and age-appropriate) description of:

- the categories of minors' information that may be processed and categories of sources of that information;
- the purposes for which minors' information may be used;
- the types of entities with which minors' information may be disclosed and the purposes for doing so;
- any options or controls available for minors and/or their parents to manage minors' privacy settings, information and activity;
- how minors and/or their parents can access, update, export, remove, delete and restrict processing of minors' information;
- contact information for questions and feedback.

IV. Data Practices: Collection, Use, Disclosure, Quality and Retention

A. Principles of necessity, fairness and lawfulness should be applied contextually and consider the full range of factors that APP entities must balance in the context of processing personal information of minors

Questions in Issues Paper addressed in this response
6.1 What criteria should define what is 'reasonably necessary' for an APP entity's functions or activities when collecting children's personal information, and how can APP entities ensure they adhere to this?
6.2 What does 'lawful 'and 'fair' mean in the context of children's personal information? How should these terms be applied specifically for children, given their evolving developmental and digital engagement stages?
6.3 Are there cases in which the collection of children's personal information would not be considered fair in any circumstances?
7.1 What processes should APP entities implement to identify and appropriately handle unsolicited personal information related to children?

<u>The criteria for what is "reasonably necessary" should be principles-led, proportionate, and reflect the nature of the service; it should enable APP entities to consider competing considerations in different contexts and be consistent with other jurisdictions</u>

By definition, what constitutes "reasonably necessary" depends on the context. It is an *objective* standard applied to different circumstances, as reflected in jurisprudence both in Australia and across the world.

The OAIC itself recognises this in its existing guidance, which emphasises that the test of what is "reasonably necessary" is objective, and that the APP entity - in justifying its actions - is best placed to determine what is in fact *reasonably necessary* in the context of their activities (see below). Google therefore encourages the OAIC to apply a consistent interpretation, including in the context of minors.

> *"The 'reasonably necessary' test is an objective test: whether a reasonable person who is properly informed would agree that the collection, use or disclosure is necessary. It is the responsibility of an APP entity to be able to justify that the particular collection, use or disclosure is reasonably necessary."*[12]

This is also consistent with other regulatory approaches, and reflects a global alignment on appropriate standards. For example, the Singaporean privacy regulator, the Personal Data Protection Commission (PDPC), has provided guidance on the concept of "reasonableness"

[12] OAIC, "Chapter B: Key concepts | OAIC", see "Reasonably necessary and necessary" (B.117).

within their Personal Data Protection Act (**PDPA**). We provide an excerpt below (emphasis added):

> *The PDPA recognises that a **balance needs to be struck** between the need to protect individuals' personal data and the need of organisations to collect, use or disclose personal data. The PDPA seeks to provide such a balance by allowing organisations to collect, use and disclose personal data for purposes **which a reasonable person would consider appropriate** in the circumstances and similarly requires organisations to act based on this standard of reasonableness."*
>
> *"In determining what a reasonable person would consider appropriate in the circumstances, an organisation should consider the particular circumstance it is facing. Taking those circumstances into consideration, **the organisation should determine what would be the appropriate course of action to take** in order to comply with its obligations under the PDPA based on what a reasonable person would consider appropriate."*
>
> *"A 'reasonable person' is judged based on an objective standard and can be said to be a person who exercises the appropriate care and judgement in the particular circumstance. **The Commission notes that the standard of reasonableness is expected to be evolutionary**. Organisations should expect to take some time and exercise reasonable effort to determine what is reasonable in their circumstances. As being reasonable is not a black and white issue, organisations and individuals may find that there will be different expectations about what is reasonable. In assessing what is reasonable, a possible step that an organisation could take is to view the situation from the perspective of the individual and consider what the individual would think as fair."*

Since the concept of "reasonably necessary" is inherently an evolutionary, fact-specific and objective assessment, the Code should empower APP entities to demonstrate compliance with the Code by taking proportionate and justifiable steps tailored to their specific functions and services. For example, considering the nature of the information collected, and the benefits for and foreseeable impact on minors. This approach encourages ongoing diligence and innovation in privacy-preserving practices, fostering a more effective and adaptable framework for protecting minors' privacy online.

This also reflects the diversity of services, each with different characteristics, and ways in which users (including minors) engage with such services. As a result, a case-by-case approach is necessary.

In practice, the purposes for collecting data about minors will also overlap to a large degree with users of *all* ages. For example, the APP entity's internal operations, maintenance of systems, product functionality, safety and security, and fraud prevention. These are core and

vital functions that are in the interests of all users. As a result, there should therefore not be a different test for what is "reasonably necessary" for these purposes with respect to minors and adults.

The concept of "fairness" in the context of collecting minors' personal information should be interpreted contextually, considering the purposes of processing, and the benefits for, and risks of harm to, minors

In the same vein as "reasonably necessary", the concept of "fairness" in the context of collecting minors' personal information is inherently a dynamic and context-dependent assessment.

For example, it requires an assessment of what minors expect and anticipate, considering - among other things - their reasonable expectations and the information provided to them. The OAIC also recognises (in its Question 6.2) that the concept of "fairness" (and its application in practice) will change depending on the evolving developmental and digital engagement stages of minors, and the specific service.

This means that certain practices may always be considered "unfair", due to the minor's limited capacity to understand the benefits and risks of the service, and to exercise effective control. For example, in the context of employing dark patterns in games to encourage minors to disclose more personal information than is reasonably necessary.

However, Google encourages the OAIC to acknowledge the importance of taking a principles-based and case-by-case assessment, to ensure that the Code does not encourage the placement of unfair limits on minors' development and digital engagement.

In particular, it is important that the Code reflect all relevant circumstances in determining how APP entities can engage with minors, including how minors themselves engage with the online service (and between different services), and any changes in minors' reasonable expectations (and understanding) of the service and how it operates. A good example of this is as the U13 becomes a teen.

The OAIC itself recognises that what can be deemed fair may change depending on the context.

> *"Whether a collection uses* ***unfair means will depend on the circumstances****. For example, it would usually be unfair to collect personal information covertly without the knowledge of the individual. However, this may be a fair means of collection if undertaken in connection with a fraud investigation*" (OAIC guidance on APP 3, emphasis added).[13]

[13] OAIC, Chapter 3: APP 3 Collection of solicited personal information | OAIC, see Para 3.62.

For example, OAIC notes that whether covert collection of personal information would be considered fair depends on the circumstances. This is particularly relevant in the context of parental oversight and child protection. For example, where a parent has intentionally enabled parental monitoring or parental control features on a child U13's supervised device for safety reasons (without the supervised child U13's explicit knowledge). It would be contrary to public policy, and APPs, to consider that such activities were unfair, in relation to supervised children who lack sufficient maturity or capacity.

Google notes that the OAIC has provided examples of general practices considered "unfair" (as outlined above). If the OAIC includes additional examples in the Code or supplementary guidance, Google encourages the OAIC to consider the range of relevant circumstances, to avoid an inadvertently restrictive approach.

For example, Google considers that personalised advertising may be considered unfair for minors. However, Google encourages the OAIC to recognise the distinction between personalised advertising and other personalisation: not all personalisation is inherently unfair in the context of minors. It is vital to consider the legitimate and fair use of data to enhance the safety, performance, and functionality of services. Such uses genuinely benefit all users, including minors.

For example, personalised recommendations, when implemented responsibly, can be invaluable in helping children U13 and teens discover content that is genuinely well-suited to their individual needs, developmental stage, and interests. Without such personalisation, minors are more likely to encounter content that is less relevant, less helpful, and consequently, less potentially age-appropriate. Such processing can be fair, and is likely to be both within the reasonable expectations, and in the best interests, of the minor.

B. The Code and associated guidance should promote a holistic assessment to safeguarding minors and protecting their personal information from misuse, focusing on privacy enhancing technologies and examples of good practice

Questions in Issues Paper addressed in this response
9.1 What safeguards should APP entities put in place to prevent the misuse of children's personal information for secondary purposes without appropriate consent or where other exceptions apply?
9.2 What secondary uses or disclosures of personal information could be reasonably expected by children, and how should these expectations vary by age and stage of development?

10.1 Can an APP entity ensure that it creates a 'reasonable expectation' that it may use or disclose children's personal information for the purposes of direct marketing? And if so, how?

The Code should provide examples of the kinds of safeguards that can be implemented to prevent the misuse of minors' personal information, whilst recognising a case-by-case assessment is required. Service providers should be encouraged to undertake a holistic assessment of how to keep minors safe online and protect their privacy, balancing these considerations against other factors that are relevant to the best interests of the child.

Google also encourages the OAIC to incentivise the use of Privacy Enhancing Technologies (PETs). When used responsibly, PETs play an increasingly important role in protecting people and their data and preventing harm.

Google considers that PETs create a safer ecosystem for all online users, and is thoughtful about where and how it uses PETs. As a result, Google provides more detail about how entities (such as the OAIC) could advance the use of PETs online.[14] For example, incentives could come from public support of the use of PETs (e.g., language encouraging use, where feasible, in the Code), encouraging industry or technical standards, providing guidance that identifies specific risks to privacy and expectations about appropriate protections or thresholds, and legally codifying the value of PETs in data subject rights requirements.

D. The Code should favour privacy-preserving measures over strict retention or deletion requirements

Questions in Issues Paper addressed in this response
13.3 How can APP entities ensure their data retention policies are appropriate for children's data, including timely deletion or de-identification when the information is no longer needed?

APP entities should be encouraged to consider data retention of minors' data in the design process of their services, in line with the best interests of the child by design principle. The Code should encourage the use of privacy-preserving settings that provide meaningful ability to understand and control over the retention and deletion of their personal information, without restricting an APP entity's ability to retain data necessary for their legitimate purposes and legal obligations.

[14] Google, Responsible Development and Use of Privacy Enhancing Technologies: How Governments Can Help (2025), https://services.google.com/fh/files/misc/pets_whitepaper.pdf.

V. Protecting Personal Information and Preventing Harmful Practices

A. The Code should not be prescriptive as to specific technical security requirements to safeguard minors' personal information over and above existing requirements

Questions in Issues Paper addressed in this response
13.1 Are there any additional or specific technical measures that APP entities should adopt to safeguard children's personal information from security risks, considering their heightened vulnerability?
13.2 Are there any additional or specific organisational measures that APP entities should adopt to safeguard children's personal information from security risks, considering their heightened vulnerability?

APP entities should be required to establish, implement and maintain reasonable administrative, technical and physical measures to protect minors' personal information from unauthorised access, disclosure, modification and destruction.

However, these measures should be proportionate to the risk of harm to the individuals whose personal information is being processed, taking into account the sensitivity and volume of the personal information at issue, the context and purposes of the processing of the personal information and the cost of available security measures.

The Code should be principles-led as to the measures that APP entities should implement to safeguard minors' personal information, reflecting that the nature of such measures will need to reflect the specific service.

VI. Enabling Children's Privacy Rights (Access, Correction, Anonymity, Opt-Out)

A. APP entities should be empowered to provide age-appropriate tools, in a format that best reflects the nature of the service, for minors and parents to access and correct personal information

Questions in Issues Paper addressed in this response
14.1 What mechanisms are needed to ensure children can easily access their own personal information?

14.4 What timeframe should be considered a 'reasonable period' for responding to a child's access request?
14.5 In what manner or format should personal information be provided to a child when an access request is made, so that it is both practicable for APP entities and developmentally appropriate for children of different ages and capacities?
15.1 What does 'accurate, 'up-to-date', 'complete', 'relevant' and 'not misleading' mean, in the context of children's personal information, given their evolving developmental and digital engagement stages?
15.2 What processes or mechanisms should be established to allow children to request corrections of their personal information easily?
15.4 What timeframe should be considered a 'reasonable period' for responding to a child's correction request?

Minors should have tools to access and correct their personal information, in a manner that is appropriate to their ages and capacities. For supervised children U13, parents should be the primary avenue for accessing and correcting a minor's personal information. Teens should have greater autonomy and control over their access to and correction of their personal information.

Service providers are best-placed to understand what tools are appropriate for different audiences, depending on the nature of their services. For example, Google sends a minor an email when they turn 13 in Australia (or the applicable age in their country) to inform them that they are eligible to update their account and end parental supervision. This gives a user, who has reached the age of consent, access to more features of Google services, control over resetting their password and creating a secure passkey to access their Google Account, the ability to manage and correct their personal information and the option to export a copy of content in their account to back it up or use it with a service outside of Google.

The Code should be principles-led and not be prescriptive as to the level of detail, response times and format of responses to access requests. This should be assessed by service providers in light of the nature of their services and understanding of their audiences.

C. Anonymity and pseudonymity promote minors' rights to privacy, freedom of expression and access to information, which should not unduly curtailed

Questions in Issues Paper addressed in this response
5.1 How can APP entities provide children with meaningful options to use services anonymously or under pseudonyms, considering their developmental stages at different ages?
5.2 In what scenarios would it be justifiable to require children to identify themselves in order to access an APP entity's service? How can these instances be minimised to protect their privacy?
5.3 Are there instances where age assurance technologies conflict with an individual's right to remain anonymous or pseudonymous, and what evidence supports this, or suggests otherwise?

Anonymity and pseudonymity are important components to users' ability to exercise their privacy rights online and access information and services. Anonymous or pseudonymous spaces provide an important environment for minors - and all users - to explore potentially sensitive information or aspects of their identity such as politics, religion, gender and sexuality, and seek support on mental and physical health, bullying, difficult family situations, even with strong privacy and security controls. They can also provide minors a way to access appropriate information and services without pressure to curate their online persona which can enable authentic self-expression and genuine engagement with ideas and communities. The potential for anonymous or pseudonymous experiences should be preserved.

Implementing a risk-based and proportional approach centred on the best interests of children will also guard against unintended consequences for rights to privacy, freedom of expression, and access to information, including those of minors. For example, signed-out users on Google Search have Safe Search Blur enabled by default, which helps protect signed out users from inadvertently encountering explicit imagery on Google Search. With Safe Search Blur, explicit imagery – such as sexually explicit or graphic violent content – is blurred by default when it appears in Search results.

D. Opt-out mechanisms should be simple and accessible without prohibiting functions that pose low risks of harm to minors

Questions in Issues Paper addressed in this response

10.2 How can APP entities ensure mechanisms are in place for children to opt-out of receiving direct marketing communications, in a simple and accessible way?

APP entities should provide simple and accessible mechanisms for minors to opt-out of receiving direct marketing communications. These mechanisms should be designed to be easily understood and used by minors, taking into account their age and developmental stage. While supporting these opt-out rights, it is important that the approach does not prohibit key advertising and marketing functions that pose minimal privacy risks, such as the delivery of contextual advertising and advertising reporting and measurement. These functions are important for the viability of many online services and pose a low risk of harm.

Please also refer to our comments in Section III (Transparency and Communication Strategies) of our response, above.

VII. General Considerations and Implementation Challenges

Questions in Issues Paper addressed in this response
4.3 What should be considered under the 'reasonable steps' test when implementing internal practices, procedures and systems for managing children's personal information?
4.4 What steps should APP entities take to ensure children, and their parents, can easily make privacy-related inquiries or complaints, and how should APP entities respond in a child-appropriate way?

<u>There is no one-size fits all approach</u>

Online services are diverse and provide varied but valuable benefits to users, including minors. The Code should account for this diversity, both in the nature of the services, as well as how users (including minors) engage with such services.

In practice, this requires a case-by-case (or service-by-service) approach, to ensure that the reasonable steps accurately reflect the specific service, and what is appropriate and technically feasible.

<u>Reasonable steps should reflect the risks posed</u>

It is also important that any “reasonable steps” consider the specific risks posed by the service. The Code would benefit from a recognition of the importance of proportionality, and the relevance of risk-based and principle-led measures. The Code should not be prescriptive as to specific steps that APP entities should implement, as such measures will invariably need to reflect the risks (and benefits) of the service.