Association for data-driven marketing & advertising

CHILDREN'S ONLINE PRIVACY CODE

OFFICE OF THE AUSTRALIAN INFORMATION COMMISSIONER

June 2026

Contents

Executive summary

- ADMA thanks the OAIC for the opportunity to make this submission.

Overarching concerns

- ADMA has a number of overarching concerns with the *Exposure Draft of the Privacy (Children's Online Privacy) Code 2026* (the Code). In summary:
  - The Code does not adopt a 'privacy by design approach built upon the bedrock principle of addressing the best interests of children. Instead, it translates a number of the 'privacy by design' principles of the UK AADC into prescriptive data-processing obligations. This approach is in direct contrast to the UK AADC, previous statements of intention of the Attorney-General's Department (AGD) and the OAIC, and Parliament's expression of intention in the Explanatory Memorandum.
  - The Code does not adopt the risk-based approach of the UK AADC which enables a regulated entity to apply overarching design standards in a manner that is proportionate to the risk of privacy harms that their service poses to children. Instead, the Code imposes obligations on a wide range of entities across the Australian economy and services that may be accessed by children, irrespective of the risk of privacy harms posed by those services. This will impose a significant new regulatory burden on a wide range of entities in relation to online services that do not pose significant risk of material privacy harms, directly contrary to the Government's objective (as also endorsed by the Productivity Commission)[1] of focussing regulation on areas where risks of material harms are significant.
  - The Code would likely lead to over-collection of personal information by regulated entities, inconsistent with other APP requirements and without focus on those services where risks of material privacy harms are significant. At the same time, the "strictly necessary" collection requirement risks preventing entities from using data in ways that benefit children, including for safety, integrity, and age-appropriate personalisation.
  - The age-assurance provision undermines the principle that individuals should be able to deal with entities anonymously.
  - The Code requires significant technical uplift and operational redesign that will not be possible for entities to achieve by December 2026 and risks encouraging entities to exclude children from their services, contrary to the OAIC's intention of creating safe online spaces for children within the digital environment. The proposed reforms would be particularly challenging for entities operating across the open web, services that interact with anonymous or non-logged in users, and smaller organisations that are not set up to undertake the extensive age-assurance and consent requirements set out in the Code.

Specific comments on Code

- ADMA also has the following specific comments:
  - The age-assurance obligations are highly onerous and should not apply to low-risk services. As drafted, they risk leading to over-collection of personal information by entities across the economy, creating more significant risks of privacy harm relative to the harm that the Code is intending to address. The Code should provide a

[1] For example, see the Productivity Commission's 2025 report, Creating a more dynamic and resilient economy, https://www.pc.gov.au/inquiries-and-research/resilient-economy/report/?ref=inflectionpoints.work; Danielle Wood, The Red Tape Impulse, 9 June 2026, https://inflectionpoints.work/articles/the-red-tape-impulse

regulated entity with flexibility to determine and document its reasoning a) if age-assurance is necessary and reasonably proportionate to the privacy harm posed by a service, b) whether the age-assurance method the entity adopts enables the entity to collect, use and disclose personal information in full compliance with the Privacy Act and APPs, evaluating both privacy risks that arise from both the service and from the age-assurance method adopted, and c) whether, if a service is 'likely to be accessed by children', the entity has ensured that the use of children's personal information in the context of provision of the service is 'consistent with the best interests of the child'.

- The scope of services regulated as 'likely to be accessed by children' should be stated in the Code itself, to provide certainty and reduce risk of overreach. An appropriate refocus would be that a service is 'likely to be accessed by children' if it is either targeted at children (as objectively ascertained), or manifestly attractive to children, for example, because a substantial number of children (stated as an objectively assessable measure) access the service. By such refocus, services such as general retail websites should not be captured. We note that if the scope of services 'likely to be accessed' by children is too broad and extends to services targeted to adults, then the 'best interests of the child' requirement may be more difficult to meet, given that the reasonable interests of adults can be quite different from the best interests of adults.
- The 'best interests of the child' requirement should be re-framed as an overarching requirement applied across the service, and not an obligation that entities are required to apply to each particular collection, use and disclosure of information. This reframing would be consistent with the 'safety by design' approach taken in the UK, EU, and advocated for by Sonia Livingstone.[2] The current approach is inconsistent with how the 'best interests of the child' test is intended to apply, as a holistic, balancing assessment, and risks discouraging processing that supports safety policies and age-appropriate personalisation.
- ADMA does not support the new 'strictly necessary' standard for data-processing activities. ADMA is concerned that 'strictly necessary' is a novel legal concept that creates legal uncertainty and therefore cost and regulatory burden for entities endeavouring to apply the standard. The combination of the now well-developed jurisprudence as to 'reasonably necessary' as applied having regard to the context of the service (not individual collections, etc.), combined with the overarching requirement to assess 'best interests of the child', provides a more manageable test, thereby reducing the regulatory burden on regulated entities while achieving the objects of the Code.
- The mandatory consent and assent provisions in the Bill are highly problematic to operationalise and therefore an excessive regulatory burden that should be removed from the Code. We recognise that the OAIC is endeavouring to empower children through agency and control as to whether and when personal information about them is collected or handled. However, this agency can be provided through clear transparency and age-appropriate notices. We have the following concerns in relation to over-extension of consent and assent provisions:
  - it risks acclimatising children and carers to click through consent and assent without careful evaluation of the service, engraining bad 'consent through fatigue' habits into a new generation of internet users;

[2] See section 3.5 of this submission.

- it is not aligned with a privacy by design approach;
- it is and inconsistent with the Privacy Act Review Report's recommendations;[3] and
- it will likely have significant unintended consequences for children wishing to access essential services on a confidential basis who may no longer be able, or choose, to do so. We note in this regard that if an overarching 'best interests of the child' requirement is introduced, consent and assent is not required, because the 'best interests' test provides for high provider responsibility, accountability and legal consequences.

- ADMA does not support introducing additional consent requirements for the collection of non-sensitive information for direct marketing purposes. We recognise that some products or services directly marketed to children today may be contrary to their best interests. However, for the reasons set out above, consent and assent are not the best tools to ensure that only products or services that are in the best interests of children are direct marketed to children: high provider responsibility, accountability and legal consequences for failure to self-assess the best interests of children are more appropriate tools. Also, imposition of consent and assent requirements on all direct marketing messages to children is likely to impede direct marketing which is in the best interests of children: for example, health and wellbeing initiatives, age-appropriate learning content and online safety messages. Direct marketing should continue to be governed by APP 7, subject to the 'best interests' test proposed in the Code for services 'likely to be accessed by children'.
- ADMA recommends that the requirement that personal information must be destroyed on request should either be removed from the Code or amended to be consistent with APP 11.2, to allow for de-identification as an alternative. Destruction will not always be technically feasible or practicable , and would limit the use of data for safety and integrity purposes, and legal processes. If there are concerns in relation to de-identification standards or processes, the OAIC Guidelines could be amended to clarify the OAIC's expectations in relation to de-identification, consistent with recommendation 21.5 of AGD's Privacy Act Review Report 2022.

[3] See section 2.1 below.

Summary of recommendations:

Overarching recommendations

That the Code:

1. Adopt a 'privacy by design' approach built on the bedrock principle of addressing the best interests of children, instead of translating privacy by design principles into prescriptive data-processing obligations.
2. Adopts a proportionate risk-based approach consistent with the UK's AADC.
3. Not include overly prescriptive requirements that lead to over-collection of personal information, potentially inconsistent with data-minimisation requirements in the APPs.
4. Retain the ability of individuals to deal with entities anonymously, in accordance with APP 2.
5. Take a consistent approach with any reforms that the Government introduces as part of the second tranche of reforms to the Privacy Act.
6. Provide entities with 24-36 months for implementation following registration.

Recommendations on specific aspects of the Code:

Age-assurance

7. Section 8 should be amended to provide for a risk-based, proportionate approach to age assurance and to recognise a range of age assurance methods, consistent with the OAIC's March 2026 age assurance guidance and data minimisation principles.
8. The Code should provide entities with flexibility to undertake their own assessment of the privacy risks posed by their service and make a decision accordingly about whether their service should be subject to age assurance measures to mitigate significant risk of material privacy harm to children within age ranges likely to access the service.

'Likely to be accessed'

9. Services 'likely to be accessed' by children should be clarified in the Code to mean 'services which are either targeted at or manifestly attractive to children'. This Code will need to be considered and potentially applied by most businesses and other entities providing websites and otherwise providing services over the internet. The Code will create a substantial regulatory burden and cost of doing business across the Australian economy which can and should be partly mitigated by the Code being clear, definitive, stable and predictable as to the criteria to be used to determine whether a service is likely to be accessed by children. The criteria should be stated within the Code, not left to guidance. 'Manifestly attractive to children' should be based on an objectively assessable measure of a substantial number of children likely to access a service, or accessing a service over a specified period.
10. The Explanatory Statement should clarify that the intention of the Code is that entities should make an assessment of 'likely to be accessed' based on the circumstances of the entity.
11. Subject to 7. above, the OAIC should issue guidance setting out non-exhaustive factors that entities may take into account in determining whether their service(s) are 'likely to be accessed by children'.

Best interests of the Child

12. The 'best interests of the child' requirement should:

- Be reframed as an overarching principle rather than an additional prescriptive requirement that applies to specific data-handling activities;
- Require a holistic assessment of the various rights that children hold, consistent with the approach to the test in the UK;
- Allow organisations to have flexibility to determine how the standard is best met and how these rights are appropriately balanced. in the circumstances of the organisation's business.

Strictly necessary

13. The standard for data-handling should continue to be 'reasonably necessary'.
14. Section 9 should be removed from the Code.
15. If there are concerns that the 'reasonably necessary' standard is unclear in the context of services targeted at or manifestly attractive to children, the OAIC could provide additional clarification in guidance material, noting that in the event of conflict between the 'reasonably necessary' and 'best interests of the child' tests, the latter should take precedence.

Consent/assent

16. The proposed consent and assent obligations should be removed from the Code.
17. Consent should not be required for use or disclosure of non-sensitive personal information, including for secondary purposes.

Direct marketing

18. 'Direct marketing' should continue to involve 'the use or disclosure of personal information to communicate directly with an individual to promote goods or services' as is the case under existing law. Consistent with the Privacy Law Review Report 2022, it should not capture targeted advertising more broadly, or communications which are not 'directed at an individual'.

Destruction

19. The requirement that personal information must be destroyed on request should be removed from the Code.

1. Introduction

ADMA recognises the importance of strengthening privacy protections for children in the digital environment. ADMA supports the policy goals of an overarching test of 'the best interests of the child' as a primary principle to consider when handling personal information,[4] and aligning the Code with the approach taken in the UK's Age Appropriate Design Code.[5] The Code should also align with the existing Australian privacy law framework and the stated object of the Privacy Act 1988 of ensuring that the privacy of individuals is balanced with the interests of entities in carrying out their function or activities.[6]

We are concerned that the Code as drafted does not achieve these goals. The Code as drafted is likely to create unintended consequences, including: over-collection of personal information by entities across the economy (in a manner that is disproportionate to any privacy harms to children and which creates new privacy and security risks); inability of children and adults to deal with entities anonymously (inconsistent with APP 2); extreme consent fatigue (which will likely discourage online engagement and lead to children developing bad habits of 'clicking through' or exploring pathways to circumvent restrictions); barriers to entities using data in ways that benefit children, for example for safety, integrity, and age-appropriate personalisation; potential exclusion of children from digital services where entities determine it is not feasible to comply with the obligations set out in the Code; and risks of inconsistency with tranche 2 reforms and existing privacy law obligations.

We think an alternative approach is needed, modelled on UK AADC privacy by design approach, and based on the 'best interests of the child' assessment, to enable entities to undertake the balancing of considerations that is required to achieve the policy intent of the Code. Prescriptive age assurance, consent and data-handling obligations should be removed and should instead be subject to an entity's self-assessment of how best to implement the 'best interests of the child' framework in the context of the entity's businesses and whether those mechanisms are necessary and proportionate to the privacy risks to children in the circumstances. In other words, ADMA's view is that the Code should facilitate multiple implementation paths to give effect to its intended objectives, rather than prescribing the specific procedures that must always be followed regardless of whether they affect the required outcomes.

These concerns are addressed in detail below, structured in three key parts:

- Overarching concerns.
- Proposed alternative approach.
- Specific concerns in relation to the provisions of the Code as currently drafted.

[4] Exposure Draft Explanatory Statement, 2.

[5] Privacy Law Review Report, Proposal 16.5.

[6] Privacy Act 1988, s 2A.

2. Overarching concerns

2.1 Code is out of step with intended purpose and objects of Privacy Act

The Attorney-General's Department's Privacy Act Review Report,[7] recommended that a Children's Online Privacy Code be developed and that it be modelled on the UK Age-Appropriate Design Code (**UK AADC**).

In implementing this recommendation, the *Privacy and Other Legislation Amendment Bill 2024* amended the Privacy Act requiring that a Children's Online Privacy Code (**Code**) be developed, that it 'must set out how one or more of the Australian Privacy Principles are to be applied or complied with in relation to the privacy of children', and that it may also 'impose additional requirements to those imposed by one or more of the APPs, so long as the additional requirements are not contrary to, or inconsistent with, the APPs'.[8]

In addition, the Code is required to be consistent with the objects of the Privacy Act, which include *'to recognise that the protection of the privacy of individuals is balanced with the interests of entities in carrying out their function or activities'*.[9]

In our view, the Code is not consistent with the intended purpose set out in AGD's Privacy Act Review Report, imposes obligations that are inconsistent with the existing APPs, and does not sufficiently balance the interests of entities in carrying out their functions.

We set out our reasoning in relation to these overarching concerns in sections 2.2-2.7 below.

2.2 Code should align with the 'privacy by design' approach of the UK AADC

ADMA notes that the Code is developed in the context of the Australian legal framework and therefore should complement the APPs and provide guidance to entities on how the APPs should be applied to protect the privacy of children. However, drafting for the Australian legal context does not require a fundamentally different approach to that taken in the UK AADC, also noting that the UK AADC was endorsed by the Australian Parliament as the model for this Code.

The UK AADC provides 15 design standards which must be taken into account when designing online services. Organisations must be able to show how they have ensured that the standards have been applied in the design process: subject to this requirement for objective self-assessment, the UK AADC allows regulated organisations flexibility as to how they meet the 15 standards. The UK AADC allows for compliance based on documented risk-assessments undertaken by entities, to address their specific businesses. This approach enables organisations to balance commercial considerations with privacy risks, and to implement practices which are best suited to the particular circumstances of their businesses.[10] For example, ICO guidance on the 'best interests of the child' standard specifically provides that 'taking into account of the best interests of the child does not mean that you cannot pursue your own commercial or other interests'.[11]

---

[7] Attorney-General's Department, Privacy Law Review Report, 2022, Proposal 16.5.

[8] Privacy Act 1988, s 26C(2)(a) and s 26(3)(a). See also https://ministers.ag.gov.au/media-centre/draft-childrens-online-privacy-code-released-31-03-2026

[9] Privacy Act, Section 2A(1)(b).

[10] 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/about-this-code/

[11] 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/1-best-interests-of-the-child/

By contrast, the proposed Australian Code does not adopt a principles-based, 'privacy by design', risk-based approach. It does not provide design standards to be considered, which may then lead to a finding that the APPs have not been complied with. Rather, the Code sets out specific requirements to be met, a number of which operate separately from and in addition to the APPs.[12] It is not clear from the drafting of the Code that these requirements provide organisations with any flexibility to balance commercial considerations based on objective self-assessment of risks of privacy harms or the requirement to act in the best interests of children.

In ADMA's view, this fundamental difference means that the proposed Code in Australia is much more complex than the UK Code and therefore more difficult (and expensive) for regulated entities to interpret as well as impractical for entities to apply and operationalise. We are concerned that the complexity of the Code and its multi-layered requirements will translate into legal and compliance costs for regulated entities and disadvantage entities that are less well-resourced, without any clear evidence that these additional layers of requirements are reasonably required to ensure the best interests of children. We therefore advocate an alternative approach to achieve consistent objectives: that is, an outcomes-based Code that facilitates multiple implementation paths to affect the required outcomes, rather than prescription of specific procedures that must always be followed, regardless of their proportionality or effectiveness to affect the required outcomes.

The UK AADC's flexible and risk-based approach enables that Code to apply in a proportionate way to services, based on the level of risk of privacy harms posed by a service, and implemented in a way that is tailored to a business' business model and consumer interface. It also enables businesses to balance privacy and safety obligations in a way that achieves these conflicting policy goals without needing to compromise one or the other because regulatory obligations are rigidly framed.

For example, under the UK AADC, when considering the best interests of the child, organisations are required to take into account interests including privacy risk, online safety, freedom of expression, participation rights, business functions and proportionality in designing and developing their service.[13] By contrast, as set out below, the Code is more specific in its drafting and appears to require the best interests of the child test to be met in relation to every collection, use and disclosure of personal information. This approach is restrictive and cumbersome to apply and would not allow competing interests to be considered in the same way as under the UK AADC.

Recommendation:

1. **That the Code adopt a 'privacy by design' approach built on the bedrock principle of addressing the best interests of children, instead of translating privacy by design principles into prescriptive data-processing obligations.**

2.3 Code should apply to services proportionately to the privacy harm posed to children

In ADMA's view, adopting a privacy by design approach would enable the Code to focus on entity accountability for reasonable, objective and documented self-assessment of application of the overarching requirements of 'best interests of the child', consistently with the OAIC's focus on ensuring APP entities undertake and document privacy threshold assessments and privacy risk assessments, but applying the new overarching test and associated design requirements to

[12] For example, additional consent requirements and additional data-handling requirements.

[13] 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/1-best-interests-of-the-child/?q=data+subject

regulated services. This approach would also reduce the regulatory burden by ensuring greater consistency between the Code and the existing legal framework. The Code, by contrast, introduces additional obligations to be applied alongside the APPs, which will likely create uncertainty and confusion in practice.

If the OAIC does not favour adopting a privacy-by-design approach similar to the UK AADC, but instead wishes to adopt more prescriptive obligations, our view is that it is particularly important that the application of the Code is

a) substantially narrowed to services that are either targeted towards children, or that are likely to be accessed by children because they are manifestly attractive to children (and evidenced by a substantial number of children accessing the service(s)); and

b) sufficiently flexible so that entities can apply the provisions of the Code (for example age-assurance requirements) in a manner proportionate to the privacy risk that their data-processing poses to children.

We set out our views on 'likely to be accessed by children' in more detail in section 3.2 below.

Recommendation:

2. **That the Code adopts a proportionate risk-based approach consistent with the UK's AADC.**

2.4 Code obligations should not include overly prescriptive requirements that lead to over-collection of personal information

Data minimisation is a foundational concept woven throughout the APPs. The OAIC has indicated that a key concern it has in relation to children's personal information is that online platforms are 'routinely collecting and using large volumes of personal information about children' and that a key goal of the Code is to minimise unnecessary data collection and ensure that entities collect children's personal information only where required.[14]

ADMA agrees this should be a key goal of the Code, consistent with the APPs. However, we are concerned that provisions in the Code require additional collection of personal information without a clear privacy benefit. In particular, provisions requiring age-assurance and implementation of consent/assent mechanisms are inconsistent with data minimisation.

ADMA considers that the Code could better balance data minimisation goals and child privacy safety goals.

Recommendation:

3. **That the Code not include overly prescriptive requirements that lead to over-collection of personal information, potentially inconsistent with data-minimisation requirements in the APPs.**

[14] Exposure Draft Explanatory Statement, 1.

2.5 Code obligations should retain the ability of individuals to deal with entities anonymously, in accordance with APP 2

APP 2 provides that individuals must have the option of dealing anonymously or pseudonymously when dealing with an APP entity. As noted in the OAIC's guidance,[15] the ability to deal with an entity anonymously or pseudonymously has numerous benefits. Some of these include:

- promoting autonomy and dignity;
- minimising of unnecessary data collection;
- promoting access to sensitive services and information;
- promoting freedom of expression;
- minimising risk of identity fraud;
- promoting meaningful privacy choices and privacy self-management.

The proposals in the Code, particularly on age-assurance and consent/assent, practically undermines this APP. Age-assurance gives rise to privacy risks that children and parents may not be comfortable with. For example, age-assurance can involve collection of sensitive personal information such as biometric information, and age-estimation or behavioural age inferencing can involve analysing browsing patterns, app usage, language and typing style, purchase behaviour and facial analysis and engagement times. This type of monitoring and profiling of users itself gives rise to privacy risks, can lead to online platforms collecting more personal information than is reasonably necessary. ADMA submits that a proportionate approach is appropriate in order to avoid unnecessary privacy intrusions and inconsistency with the principles of data minimisation and facilitating anonymous or pseudonymous interactions.

ADMA has similar concerns about the consent/assent provisions. Division 2 sets out a detailed and complex consent process that requires organisations to collect additional personal information which may include age/date of birth, evidence of parental relationship (or other relationship with parental responsibilities), parent contact details, identify verification information and records of consent and assent. Some of this information may be highly sensitive and not information that many children and caregivers will want to share online. ADMA submits that the provisions are disproportionate, having regard to the controls proposed through overarching obligations of risk assessment and mitigation and best interests of children, and that the provisions create unnecessary privacy intrusion and are inconsistent with the principles of data minimisation and facilitating anonymous or pseudonymous interactions ADMA has a number of concerns with these provisions (see – section 3.5 below), including that they are inconsistent with APP 2 – they effectively prevent people from engaging with entities anonymously.

Recommendation:

4. **That the Code retain the ability of individuals to deal with entities anonymously, in accordance with APP2.**

2.6 Code should be consistent with Privacy Act and any proposed Tranche 2 reforms and avoid duplication with other laws

In our view, the Code should take an approach that is consistent with any reforms that the Government introduces as part of the second tranche of reforms to the Privacy Act. We think the approach the Code is taking risks creating inconsistencies. By adopting a new legal standard for data-processing ('strictly necessary') and a novel approach to consent (albeit derived from a New

[15] OAIC – APP Guidelines, Chapter 2: APP 2 – Anonymity and pseudonymity, 2014.

York statute), before an appropriate new framework for notice and consent provisions is addressed in tranche 2 reforms, the Code is creating a high risk that the Code requirements, and those of tranche 2, will be inconsistent. The highly prescriptive nature of the Code increases this risk.

For example,

- If the tranche 2 reforms move away from a consent-centric approach to privacy to reduce consent fatigue, as was recommended in the Privacy Act Review Report 2022, it would be inconsistent for the Code to create significantly more consent requirements for children and carers.
- If as part of any move away from a consent-centric approach to privacy, the proposed reforms introduce an overarching requirement that applies to the collection, use and disclosure of personal information; as currently drafted, entities will be required to satisfy two overlapping but different tests in respect of the same data-handling processes.
- If the APPs are simplified in line with the Productivity Commission's recent recommendation,[16] this may directly impact the Code, for example the direct marketing provisions. This important topic has not yet been the subject of consultations between the Attorney-General's Department and relevant stakeholders, although such consultations were foreshadowed to occur before tranche 2 changes to direct marketing provisions were further developed.

In addition to Tranche 2 privacy reforms, there are a number of laws as well as law reform processes underway, which overlap with the Code and which could therefore give rise to inconsistent obligations or regulatory tensions. These include:

- The Online Safety Act, associated Codes and Basic Online Safety Expectations;
- Online Safety Amendment (Social Media Minimum Age) Act 2024;
- Competition and Consumer Amendment (Unfair Trading Practices) Bill 2026;[17]
- Digital Duty of Care consultation.[18]

We also note advertising in Australia is currently comprehensively regulated under a framework of technology neutral provisions that regulate the content of advertising to address potential harms from that content, including to children. For example, Australian Consumer Law, Commonwealth and State legislation regulating specific products such as gambling and alcohol advertising restrictions, medium specific laws, for example the Broadcasting Services Act and associated Australian Content and Children's Television Standards, industry specific laws for example the Therapeutic Goods Administration Code, Banking Code of Practice and many others, and the AANA framework of advertising Codes including the Code of Ethics as well as specific codes to address advertising to children, food & beverage advertising, environmental claims and wagering advertising.

This comprehensive regulatory framework minimises the risk of a range of different harms arising from advertising and marketing content and business practices, while also recognising that advertising is key to communicating information, including about products and services, to the Australian community. In ADMA's views, this framework provides a strong foundation for ensuring children have access to safe spaces online, while also balancing competing considerations such as privacy, freedom of expression and enabling online participation.

[16] Productivity Commission, Harnessing Data and Digital Technology, 2025-26, Recommendation 4.1.

[17] https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/bd/bd2526/26bd058

[18] https://www.infrastructure.gov.au/department/media/publications/digital-duty-care-australia-developing-duty-care-framework-online-services-used-australians

The approach of creating overlapping obligations goes against the Productivity Commission's recent recommendations in relation to avoiding over-regulation. In our view adopting a principles-based privacy by design approach (as proposed in detail in section 3) will reduce the risk of inconsistency with existing Privacy Act provisions, any Tranche 2 reforms, as well as other laws and law reform processes that are underway.

Adopting a privacy by design approach would enable the Code to complement the existing framework of regulations rather than altering or bringing into question existing policy settings that have been achieved through other consultation processes.

Recommendation:

5. **That the Code take an approach that is consistent with any reforms that the Government introduces as part of the second tranche of reforms to the Privacy Act.**

2.7 Technical feasibility

ADMA has significant concerns regarding the ability of entities to transition their technical capabilities to comply with the obligations in the Code as drafted. Even if the issues outlined in this submission are addressed, ADMA's feedback from members is that, subject to the final provisions of the Code, it will likely require substantial technical uplift and operational redesign by the entities that are required to comply with it.

At a high level, the additional requirements that organisations would be required to undertake may include:

- Creating a way to recognise users across site and app visits, for example, through use of cookies, device identifiers, browser fingerprinting, temporary tokens or federated login systems.
- Introducing or purchasing an age estimation or verification system, for example by integrating third-party age assurance providers, deploying facial recognition technology, or purchasing or developing software to verify identity documents or infer age from behaviour or usage patterns.
- Developing data mapping and governance systems so that entities understand what child data is collected, where it flows, which vendors receive it and which processing activities depend on age.
- Building new user journeys and parental consent flows, for example by building systems that are able to pause data collection until consent is obtained, contacting parents, authenticating parents, obtaining consent, storing evidence of consent and managing revocation.
- Re-engineering advertising and analytics systems if child and adult traffic needs to be segmented, personalised ads need to be suppressed for children, or if data-sharing needs to be restricted;
- Further to the point above, this re-engineering would also require upgrades to programmatic real-time bidding protocols which underpin online advertising, to enable advertisers and their technology partners to identify children and continue advertising;
- For entities with global businesses, they may need to consider geolocation systems.
- Upgrading cybersecurity infrastructure due to the increased risks from holding more and more sensitive PI and working through how to minimise the privacy risks associated with

privacy intrusive practices that organisations may not have the infrastructure necessary to securely support.

- Engaging staff.
- Testing and auditing.

The Code would require all entities providing regulated services (regardless of risk of material privacy harm) to develop and implement entirely new technical systems, governance processes, consent architectures, and age assurance capabilities that do not currently exist within their services or business models. These changes will require significant lead time for design, procurement, testing, deployment, and organisational implementation.

The proposed reforms would be particularly challenging for entities operating across the open web and services that interact with anonymous or non-logged-in users. These entities will not have access to personal information collected through existing subscriber relationships and so will need to develop one or more of the technological methods to recognise and age-assure users listed above. All of these options would carry their own privacy risks due to the additional personal information being collected. Each method has trade-offs in terms of privacy, accuracy, cost, accessibility and bias or discrimination.

Many smaller entities will not currently have identity systems, internal technical staff or compliance lawyers, or arrangements with third party vendors in place to manage complex data systems and regulatory obligations on their behalf. For much of the SME sector, these obligations will be disproportionately expensive to their size, and for those that are not targeting their services to children, or whose services are not manifestly attractive to children, they will also be disproportionate to the privacy risk to children arising from their services (and may in fact be creating more serious privacy risks from the additional collection of data required by the Code).

All entities will need to consider whether they can comply with these requirements, and if they cannot, whether they should exclude children from their online spaces entirely to avoid non-compliance. A transition period of 24-36 months will assist entities in this regard, though some may still ultimately consider that implementing the provisions of the Code is not feasible for them and that locking under-18s out is more cost-effective or more consistent with their risk appetite.

These issues highlight the critical importance ensuring that the Code is appropriately targeted to services where there is a significant risk of material privacy harm to children, and that the Code's provisions are technically feasible and operationally manageable.

Recommendations:

6. **A minimum 24–36-month implementation period following finalisation of the Code to enable as many entities to comply as possible.**

3. Proposed alternative approach

In our view, the Code should be risk-based and proportionate and facilitate multiple implementation paths to affect the Code's intended objectives, rather than prescribe the specific procedures that must always be followed regardless of proportionality or effectiveness to affect the required outcomes.

ADMA favours an alternative approach whereby entities that are providing services reasonably likely to be regulated by the Code, undertake a threshold assessment as to whether their services are within the scope of the Code.

If an entity's threshold assessment is that the entity is reasonably likely to be providing a regulated service within the scope of the Code, the Code could require the entity to undertake a structured assessment of risk of privacy harms and 'consistency with the best interests of children' reasonably likely to access the service (applying a holistic assessment as set out in section 3.3 of this submission)

A structured assessment by a regulated entity of whether a service is 'consistent with the best interests of the child' could include consideration of factors such as:

- the degree of transparency to children, carers and others as to why and how personal information is collected and shared,
- whether children are afforded reasonable agency (and therefore control) as to collection and handling of personal information, and
- any other competing interests which the entity has taken into account in the assessment,

having regard to the nature of the service and proportionality of the collection and handling.

An entity might elect to implement age assurance, consent, or other access limitation features if the entity determines such steps are proportionate and reasonable in the circumstances to mitigate risks of privacy harms to children to the point that residual risks of privacy harms are low, as well as ensuring that collection and handling of personal information related to the service is consistent with the best interests of children likely to access the service.

The assessment could be documented in writing held by the regulated entity and made available to the OAIC upon request.

We do not support the requirement in clause 36 in the Code that entities publish a list of privacy impact assessments conducted to comply with the requirements of the Code. If those requirements are clearly stated in a Code that adopts the alternative approach advocated above, OAIC could reasonably assume that regulated entities will conduct those assessments and hold documentation of them, or face the very substantial penalties and other sanctions that OAIC can now impose. A public record of privacy impact assessments - but one aspect of assessments that entities should be conducting to ensure compliance with the Code – is potentially misleading as to the range of activities that an entity should be undertaking, and simply unnecessary.

4. Specific concerns

3.1 Age assurance

Part 3, Div 1, s 8 of the Exposure Draft provides that, 'subject to subsection (3), before an entity collects personal information about an end-user of the entity's service, **the entity must take steps that are reasonable in the circumstances to ascertain the age of the end-user**'. Subsection (3) provides that 'the entity may collect personal information about an end-user of the entity's service before ascertaining the end-user's age only to the extent that the information is necessary for the entity to comply with subsection (1)'.

Section 26GC(5) of the Privacy Act provides that, 'Subject to subsection (7), an APP entity is bound by the Children's Online Privacy Code if:

(a) all of the following apply:

(i) the entity is a provider of a social media service, relevant electronic service or designated internet service (all within the meaning of the *Online Safety Act 2021*);

(ii) the service is likely to be accessed by children;

(iii) the entity is not providing a health service; or

(b) the entity is an APP entity, or an APP entity in a class of entities, specified in the code for the purposes of this paragraph.

ADMA is concerned that these provisions read together raise significant proportionality and implementation concerns. They appear to require all providers of social media services, relevant electronic services and designated internet services (i.e. potentially any entity with a website), to undertake age-assurance of their customers/site users, where the relevant service is "likely to be accessed by children". The Code and Explanatory Statement do not currently provide any indication of what the OAIC will consider to be 'steps that are reasonable in the circumstances' or how these age assurance obligations will be calibrated according to the actual risk of privacy harm to children.

This creates a significant risk that the Code a) imposes highly onerous age-assurance obligations on entities beyond what is currently required under the APP framework, and/or b) that the Code will be read by entities in this way and therefore lead to over-collection of personal information for the purposes of undertaking age-assurance, thereby creating much more significant risks of privacy harm relative to the harm that the Code is intending to address.

In addition to the significant technical difficulties set out in section 2.7 above, these requirements necessarily give rise to significant privacy risks from over-collection of personal information for the purposes of conducting age-assurance. While some methods, for example, self-declaration methods, would minimise this risk, they would also be easily be bypassed and create unnecessary friction at the consumer interface for all customers to the site. Other methods involve either extensive profiling/behavioural inferencing, facial recognition, or collection of identity documentation, all of which give rise to privacy risks including over-collection and can be costly for entities to implement.

In practice, even if there is a risk that a child may access any website or online service across the open web, most of these services will not be targeted at or attractive to children, and most will not know or reliably know whether a visitor to their site is a child (unless the child is logged-in to the service, or self-declares age, or the site uses some form of age-assurance or tracking technology, as set out in section 2.7 above).

From a public policy perspective, ADMA is not convinced that this is something that entities should be required to do if their service is not targeted at children or manifestly attractive to children. General websites may be accessed by children from time to time, however, in our view, the potential harm from over-collection from these websites outweighs the benefit of any harm-minimisation that age-assurance of these types of websites would provide. For example, a retail store which provides clothing, homewares, beauty products and children's clothing and toys, may be accessed by children from time to time: however, the store is not targeting children or promoting its online store as a service for children. While a significant number of children may from time to time access the website, having regard to regulatory burden and proportionality to significant risk of material privacy harm to children, we suggest that it is inappropriate to require the store to identify and profile its users to determine exactly who they are and how many children are accessing the website, or to partition the website.

We recommend against requiring formal verification across all services. This would risk creating large stores of sensitive identity and behavioural data, which will itself create heightened privacy and security risks for children, be inconsistent with the Code's broader data minimisation objectives, and create costly and consumer unfriendly technical barriers to accessing online services that children generally have little interest in.

For all services, regardless of whether they are targeted at or manifestly attractive to children or not, age-assurance will pose risks significant implementation challenges. We have set out some examples of the challenges, and our members' concerns, in **Table 1 below**. These challenges highlight why entities should be given flexibility to consider the proportionality of age-assurance as a mechanism to meet the privacy objectives of the Code. ADMA's view is that the Code should not require or incentivise APP entities to adopt privacy intrusive age-assurance methods that are not proportionate to the privacy harms that their services pose.

Recommendations:

7. **Section 8 should be amended to provide for a risk-based, proportionate approach to age assurance and a range of age assurance methods, consistent with the OAIC's March 2026 age assurance guidance and data minimisation principles.**
8. **The Code should provide entities with flexibility to undertake their own assessment of the privacy risks posed by their service and make a decision accordingly about whether their service should be subject to age assurance measures to mitigate significant risk of material privacy harm to children within age ranges likely to access the service. For example, verifiably reliable age assurance measures may be necessary to be deployed to enable a regulated service provider to objectively determine that a service is only likely to be accessed by children within a particular age range, because those measures are appropriate to mitigate significant risk of material privacy harm to children that are not within that particular target range.**

Table 1. Examples of unintended consequences of age-assurance provision

Identity documentation	Child A would like to access educational information on the Zoo's website for a school assignment. The Zoo considers its website caught by the Code and as a result has implemented age-verification software that requires him to upload his ID. Child A is 13 and doesn't have any ID other than his birth certificate which is with his mum. He lives with his dad and won't see his mum for another month. Child A is effectively unable to have access to the information for the purposes of the school assignment.

Freely accessible services (non-subscription) and services that allow anonymous users	Small publisher X provides freely accessible information and news for all Australians. Its philosophy is to keep information open and in the public domain, and to enable users to research sensitive topics anonymously, so its business model is based on not requiring visitors to create accounts in order to access its website, which is accessed by people from all demographics. While it is not interested in collecting personal information that it does not need, it collects some personal information as part of operating the site including IP addresses, information collected via cookies and tracking technologies for purposes of site functionality, security and analytics, and technical logs for security, abuse prevention and site administration. Small publisher X has the options of either - changing its entire business by requiring users to set up accounts and setting up its business to collect significantly more personal information, and implementing the provisions of the Code in relation to its child users - or complying with the provisions of Code in respect of all of its users which effectively means it needs to actively identify its child users and their parents anyhow, for the purposes of the mandatory consent provisions.
Loyalty programs	Supermarket Z operates a loyalty scheme linked to a household account which allows purchasing from multiple people in the same household to be associated with a single account, so rewards and benefits accumulate together. Supermarket Z sees activity associated with the account but does not necessarily see the identity of the individual family member making each purchase. When a member of the household uses the account, the supermarket collects a range of basic details and information about shopping behaviour which may include name, email address, pages viewed, details of children in the household, personal information from cookies and payment information. The supermarket has no reliable way to determine who the end user is at any particular time. The supermarket's only practical option is to treat the account holder as the customer. It is unclear whether this would be sufficient to comply with the law or whether the Code requires the supermarket to undertake more detailed behavioural inferencing or biometric analysis to determine who the customer is at any particular time.

3.2 'Likely to be accessed'

Services 'likely to be accessed' by children should be clarified in the Code to mean 'services which are either targeted at or manifestly attractive to children'.

This Code will need to be considered and potentially applied by most businesses and other entities providing websites and otherwise providing services over the internet. The Code will create a substantial regulatory burden and cost of doing business across the Australian economy which can and should be partly mitigated by the Code being clear, definitive, stable and predictable as to the criteria to be used to determine whether a service is likely to be accessed by children. The criteria should be stated within the Code, not left to guidance.

'Manifestly attractive to children' should be based upon a quantitative or other objectively assessable measure of a substantial number of children likely to access a service, or accessing a service over a specified period, stated in the Code as that quantitative or other objectively assessable measure. This approach is taken in other codes, for example, the ABAC Responsible

Alcohol Marketing Code provides that alcohol marketing may only be placed where the audience is reasonably expected to be at least 80% adults.[19]

The Explanatory Statement and later guidance material might then expand upon the application of the criteria as should be stated in the Code. It should not be necessary for most entities and their advisers to work through secondary sources such as guidance to work out the circumstances in which this Code applies.

In ADMA's view, the risks and unintended consequences of not narrowing the scope of section 26GC(5)(a)(ii) would be significant, and provide an example of exactly the sort of regulation that the Productivity Commission has warned would risk dampening productivity in the Australian economy due to lack of being appropriately targeted.[20] To address this risk, the provisions of the Code should clarify exactly which services are 'likely to be accessed by children', and be sufficiently clear so that entities can confidently assess whether their service falls within scope.

Recommendations:

9. **Services 'likely to be accessed' by children should be clarified in the Code to mean 'services which are either targeted at or manifestly attractive to children'. This Code will need to be considered and potentially applied by most businesses and other entities providing websites and otherwise providing services over the internet. The Code will create a substantial regulatory burden and cost of doing business across the Australian economy which can and should be partly mitigated by the Code being clear, definitive, stable and predictable as to the criteria to be used to determine whether a service is likely to be accessed by children. The criteria should be stated within the Code, not left to guidance. 'Manifestly attractive to children' should be based on a quantitative or other objectively assessable measure of a substantial number of children likely to access a service, or accessing a service over a specified period.**
10. **The Explanatory Statement should clarify that the intention of the Code is that entities should make an assessment of 'likely to be accessed' based on the circumstances of the entity.**
11. **Subject to the above, the OAIC should issue guidance setting out non-exhaustive factors that entities may take into account in determining whether their service(s) are 'likely to be accessed by children'.**

Table 2. Examples of 'likely to be accessed by children'

Department store	**Department store D sells a broad range of everyday products including clothing, footwear, books, baby products, beauty items, sporting goods and family focussed products such as toys, school supplies and kids' apparel. These are all available from its publicly accessible website.** **Department Store D is not targeted at children or manifestly attractive to children. While it sells children's products, and these products are available on a separate webpage to its other products, the products are targeted at and primarily purchased by adults and**

[19] https://abac.org.au/

[20] https://www.pc.gov.au/media-speeches/speeches/growth-mindset/

carers. There is no evidence that the webpage has a substantial number of child visitors.

Department Store D should not fall within the scope of the Code.

3.3 Best interests of the child

Part 3 Div 1 Sections 10 and 11 of the Code set out requirements that entities cannot collect, use or disclose personal information about a child unless the specific collection, use or disclosure 'is consistent with the best interests of the child'.

This approach in the Code appears to deviate from the AADC, the work of Sonia Livingstone and the framing of Proposal 16.4 of the Attorney-General's Department's Privacy Act Review Report 2022.

Under the AADC, the 'best interests of the child' is required to be a primary consideration *when designing and developing online services*. As part of this consideration, ICO guidance provides that organisations are required to consider the range of rights that children hold, including in relation to safety, health, wellbeing, family relationships, physical, psychological and emotional development, identity, freedom of expression, privacy and agency to form their own views and have them heard.[21] Organisations have some flexibility to determine how the standard is best met, and how these rights are appropriately balanced, in the circumstances of the organisation's business.

The European Digital Services Act takes a similar approach. Regulation (EU) 2022/2065 DSA provides: *Providers of very large online platforms and of very large online search engines should take into account the best interests of minors in taking measures such as adapting the design of their service and their online interface, especially when their services are aimed at minors or predominantly used by them." (para. 89)*[22]

This is consistent with Sonia Livingstone's approach, which supports "safety by design" and ensuring that child-rights or best-interests impact assessments are undertaken when designing products. Her work with the Digital Futures Commission stated that the 'best interests concept must be applied holistically', and expressed concern that the ICO's framework could be read as implying that each right can be addressed separately. It was recommended that 'given the complexities and contingencies of children's lives, rights appear to clash… the "best interests of the child" requires that a holistic judgement is reached through careful consideration… so that, on balance, talking all things into account, the best interests of the child prevail'. [23]

The Attorney-General's Department's Privacy Act Review Report 2022 similarly proposed to 'Require entities to have regard to the best interests of the child as part of considering whether a collection, use or disclosure is fair and reasonable in the circumstances',[24] and that 'The substantive requirements of the Code could address how the best interests of child users should be supported in the design of an online service'.[25]

The approach taken in the Code requires a best interests of the child assessment to be undertaken in relation to specific data-handling activities, regardless of the broader context.

[21] 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/1-best-interests-of-the-child/

[22] https://eur-lex.europa.eu/eli/reg/2022/2065/oj/eng

[23] https://researchonline.lse.ac.uk/id/eprint/119557/1/Digital_Futures_Commission_data_protection_and_the_best_interests_of_the_children_published.pdf

[24] Proposal 16.4.

[25] Proposal 16.5.

ADMA would support 'the best interests of the child' obligation being re-framed as a design principle rather than relating specifically to collections, uses and disclosures of personal information. The approach taken in the Code deviates from other jurisdictions and is inconsistent with the Digital Futures Commission's recommendations to the ICO in relation to the operation of the test under the AADC, in particular, that the test should consider all of the circumstances and rights of the child holistically.

In ADMA's view, reframing the "best interests of the child" requirement as an overarching interpretive principle relevant to the design and operation of a service, would better align with comparable international frameworks, including the UK AADC, while requiring entities to appropriately consider and mitigate risks to children in the context of their services more broadly. It would better align with the APPs. In our view, it would also lead to better outcomes for children if the test informs what is 'reasonable' or 'fair' in the context of children's vulnerability, rather than introduced as a further, additional test in relation to specific data handling activities.

The approach taken in the Code risks creating practical and interpretive challenges for entities attempting to operationalise the obligation. ADMA is concerned that the current approach could lead to unintended consequences, including:

- it risks discouraging routine data processing, for example, to support safe, age-appropriate experiences;
- it could be interpreted as imposing a de facto ban or severe restriction on advertising and marketing activities, well beyond the restrictions that exist in relation to advertising to children in the offline environment;[26]
- it could potentially lead to confusion in relation to how it applies to personalisation of content.

For example, is collection of personal information for the purposes of direct marketing 'consistent with the best interests of the child' if the direct marketing content is not inappropriate for the age demographic that the service attracts? If a parent provides their child with a loyalty card or debit card to pay for a product and in the course of payment personal information is collected from the child, will that be considered 'consistent with the best interests of the child'?

Recommendation:

12. **The 'best interests of the child' requirement should:**
    - **Be reframed as an overarching principle rather than an additional prescriptive requirement that applies to specific data-handling activities.**
    - **Require a holistic assessment of the various rights that children hold, consistent with the approach to the test in the UK,**
    - **Allow organisations to have flexibility to determine how the standard is best met and how these rights are appropriately balanced. in the circumstances of the organisation's business.**

Table 3. Example of concerns with 'consistent with the best interests of the child' test.

Online safety	**Company Y uses automated tools to detect risks of grooming or abuse on its service. The tools monitor behavioural patterns, and Company Y retains logs so that it can investigate conduct that is high risk according to the automated tool.**

[26] For example, see the *Broadcasting Services (Australian Content and Children's Television) Standards 2020*.

Company Y is unsure if it meets the 'best interests of the child' test because the Code requires every collection, use and disclosure of personal information to be in the best interests of the child rather than an overall assessment. Company Y is unsure how the best interests test should be applied to every individual data-handling activity, or whether collection and use of personal information for the purposes of a broad risk-mitigation strategy using automated tools would meet the test, given the intrusion on the child's private communications. Company Y has no option other than to obtain detailed external legal advice given the complexity of the multiple 'best interests' tests' and overlapping obligations that apply to data-handling, despite the fact that Company Y has conducted a detailed assessment of the automated tool to ensure that any privacy risks associated with the tool, data collection and behavioural monitoring are minimised.

3.4 Strictly necessary

Part 3, Division 1, s 9 provides that "an entity must implement technical and organisational measures that ensure that, by default, the entity only collects, uses or discloses personal information about a child that is strictly necessary to provide the entity's service'; and that such measures must 'enable an end-user... who is a child... to control whether personal information about the child is collected, used or disclosed if that information is not strictly necessary for the provision of the entity's service'.

'Strictly necessary' data handling vs default settings as a design principle

ADMA understands that this is intended to align with the UK AADC's Standards. However, as with the 'best interests of the child' standard, under the UK AADC, the requirement to have 'high privacy' default settings is imposed as an overarching design principle as part of the 'best interests of the child' framework and subject to a Privacy Impact Assessment, rather than an obligation that is evaluated for individual data-handling activities.

As part of the UK AADC framework, the default settings standard requires 'high privacy' by default unless a compelling reason for different default setting can be demonstrated. The guidance on this standard provides that

> '*it is not necessary... for you to provide a privacy setting for any personal data that you have to process in order to provide your core or most basic service. This is because without their essential processing there is no core service for you to offer. In this circumstance, if the child wishes to access the core service, you cannot offer them a choice over whether their personal data is processed or not. In order to give children control over when and how their personal data is used, you should provide privacy settings for any processing that is needed to provide additional elements of the service that go beyond the core service'*. [27]

It also provides for an exception to 'high privacy' default settings:

> '*if you can demonstrate that there is a compelling reason for different default setting taking into account the best interests of the child'*.

[27] 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/7-default-settings/

In other words, under the UK AADC the overarching best interests principle is the primary consideration: provided privacy settings are consistent with the child's best interests, entities will still be complying with the law, even where they do not have the highest privacy default settings.

By contrast, the Explanatory Statement provides that

> '*the strictly necessary requirement means that the collection, use or disclosure of that information should be essential to provide the service to which the Code applies, rather than reasonably necessary. In other words, an entity needs to collect, use and disclose personal information in that way in order to actually deliver the elements of the service the child has signed up for. For example, this does not include the collection, use or disclosure of personal information for broader business purposes (e.g. for marketing, service improvement or as part of an indirect funding model). The 'strictly necessary' test establishes a narrower and more protective threshold than 'reasonably necessary'*. [28]

This paragraph of the EM essentially provides that this obligation goes beyond the regulation of default settings and requires each collection, use and disclosure of PI to be assessed in accordance with a new standard, 'strictly necessary', for which there is no precedent under our exiting law, rather than the existing 'reasonably necessary' standard.

ADMA has the following key concerns with this:

- It is inconsistent with the privacy by design approach taken in the UK AADC, where the provision relates to high privacy default settings rather than a standard for data-handling activities.[29]
- It introduces a new standard into Australian privacy law that does not have a clear meaning and will lead to regulatory complexity and uncertainty.
- It isn't necessary to change the legal standard for data collection given that, as provided in OAIC guidance:
    - *"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."*

  and

  > *".. a collection, use or disclosure of personal information will not usually be considered reasonably necessary if there are reasonable alternatives available, for example, if de-identified information would be sufficient for the function or activity.*[30]

For these reasons, while conceptually we support the idea that entities should not be collecting, using or disclosing data that they do not need for the provision of the service that the child is requesting, the existing APPs already require this.[31]

In addition, if the 'best interests of the child' test is incorporated into the Code as an overarching principle rather than a data-handling obligation (as we understand was the OAIC's intention),[32] then that would impose an additional obligation on entities, over and above the requirements in

---

[28] Exposure Draft Explanatory Statement, 8.

[29] 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/7-default-settings/

[30] https://www.oaic.gov.au/privacy/australian-privacy-principles/australian-privacy-principles-guidelines/chapter-b-key-concepts

[31] https://www.oaic.gov.au/privacy/australian-privacy-principles/australian-privacy-principles-guidelines/chapter-b-key-concepts

[32] OAIC Roundtable, 29 April 2026.

the APPs, to ensure that all of their dealings with children and their data is 'consistent with the best interests of the child'. Collecting more personal information than what is reasonably necessary will not be in the best interests of the child unless the circumstances are such that that data is used in the child's best interests. An additional 'strictly necessary' test would be superfluous and risks overcomplicating the law and confusing entities.

Activities that should be considered acceptable

The introduction of the 'strictly necessary' standard suggests that there is concern that certain data-handling practices are not sufficiently restricted under existing law. ADMA members would like to understand which data-handling practices the OAIC is concerned about.

As currently drafted, there is uncertainty as to whether the provisions are intended to capture activities such as personalisation and recommender systems, which are integral to many digital services and business models, including online retail, content platforms, and safety systems. These systems are commonly used not only for commercial purposes, but also for important functions such as serving age-appropriate content, online safety, fraud prevention, service integrity, and service improvement. Restricting these activities would be disproportionate and inconsistent with consumer expectations regarding how digital services operate.

Our members have expressed some concern that ordinary business activities including use of recommender systems and personalisation of content should not be viewed as somehow outside of the 'strictly necessary' standard. All ordinary business activities required to provide a consumer with a service that they have requested should be viewed as (strictly) necessary to provide the service. This should also include activities necessary for internal business operations or for security or verification purposes.

Businesses require certainty that ordinary day-to-day activities such as these can continue where appropriate safeguards are in place.

Conflict with other regulatory settings

There is also potential for conflict between the proposed "strictly necessary" standard and obligations arising under other regulatory frameworks, including the Online Safety Act. For example, services may be required to undertake behavioural analysis, safety monitoring, or age estimation activities to identify self-harm risks, prevent harmful interactions, or comply with online safety obligations, even where those activities may not be characterised as "strictly necessary" to provide the core service itself.

Technical feasibility of implementing two standards

There are also concerns regarding the technical feasibility and operational complexity of implementing and maintaining two separate data handling standards across services, particularly where systems and algorithms operate holistically rather than in discrete categories of "strictly necessary" and non-essential processing.

Recommendations:

13. **The standard for data-handling should continue to be 'reasonably necessary'.**
14. **Section 9 should be removed from the Code.**
15. **If there are concerns that the 'reasonably necessary' standard is unclear in the context of services targeted at or manifestly attractive to children, the OAIC could provide additional clarification in guidance material, noting that in the event of conflict between the 'reasonably necessary' and 'best interests of the child' tests, the latter should take precedence.**

Table 4 – Examples of issues with 'strictly necessary' threshold

'Strictly necessary ' and loyalty or rewards programs	**Convenience Store X has obtained legal advice that the new 'strictly necessary' threshold means that the store can only collect the minimum amount of personal information necessary from customers who are children in order to provide them with the basic service. Teenager Z is 15 and would like to sign up for Store X's loyalty program to be able to obtain loyalty rewards and discounts. However, Convenience Store X's interpretation of their legal advice is that it is unable to collect any personal information from children for the purpose of signing up under 18s to its loyalty program which they do not consider to be part of their 'basic service'. Convenience Store X ceases providing rewards and discounts to under 18s.**

3.5 Consent requirements

Part 3 Division 2 of the Code, sets out the requirements for consent to the collection, use or disclosure of personal information about a child, including the requirement for parental consent where the child is less than 15 years of age, as well as the child's assent where the personal information is sensitive information, where an entity wishes to use or disclose the personal information for a purpose other than the purpose for which it was collected or where an entity wishes to use or disclose the personal information for direct marketing.

ADMA is concerned about operational feasibility of the consent/assent requirements in the Code for reasons which we set out below. We question whether what is being proposed will achieve the outcome that the OAIC intends.

Unintended consequences of shifting the burden of privacy back onto children and their parents

Firstly, the approach put forward is completely inconsistent with the approach put forward in the Attorney-General's Privacy Law Review report which identifies consent fatigue as a serious issue to be addressed,[33] and proposes shifting the burden of consent from consumers onto organisations.[34] The proposed consent framework instead shifts an increased burden back onto consumers, including children.

ADMA has previously supported the concept of shifting the responsibility for consent away from consumers onto organisations. Research referenced by the ACCC has estimated that it would take consumers 46 hours per month if they were to read all of the privacy policies they encounter online.[35] The same study found that even though users are constantly reminded to read privacy policies, one in three Australians still does not look at any legal information online. In other words, it is not practical for most adults to read every privacy notice presented to them online. ADMA does not support an approach that seeks to increase this burden for parents and place a similar burden on children. The proposed approach is particularly impractical given the requirements as drafted apply broadly to entities across the economy, therefore creating an unworkable volume of consent requirements for both consumers as well as entities. Most parents will not have the capacity to be constantly consenting to privacy notices for their children, on top of the notices that they are already required to read and consent to for themselves.

In addition, the friction that is created from the constant requirement for multiple consents suggests that accessing online services is an inherently risky or negative activity and in ADMA's

[33] Privacy Act Review Report 2022, for example see chapter 11.

[34] Ibid.

[35] https://www.unsw.edu.au/newsroom/news/2024/05/Worried-address-birth-date-health-data-being-sold

view, would create a false impression that the risk of children engaging in online spaces is higher than what it actually is and discourage parents from letting their children access these spaces. This is highly problematic in light of the fact that online spaces can have significant benefits for youth well-being. There are multiple studies that illustrate how online services accessed via apps, web-based platforms, and online benefit users' emotional, social, cognitive, and behavioural well-being.[36] Online services are often seen as preferred to in-person services because of concerns about privacy and the stigma of accessing similar programs in-person. Requiring adult consent will effectively remove the ability of children to independently access these services and so will act as a deterrent to accessing critical well-being services in cases where they may be able to provide essential assistance in areas including health, sexual health, and psychological services.[37]

We are therefore concerned that this proposal will be counter-productive and lead to children simply being locked out of online spaces. It risks leaving children in a position where they are more reliant on their parents to access online spaces and services and assumes that that is a positive outcome. Inherent in placing this burden on parents are a number of assumptions, including that a) children are comfortable requesting the parent's consent, b) parents will turn their minds to each and every privacy notice each and every time their child wishes to access an online service, c) they will do so in a timely manner and d) parents will discharge that burden in a way that is either in the child's best interests and/or takes the child's views into account. We submit that it is not realistic to expect that parents will do this every time a child wishes to use a different online service. Further, the impact of parents not engaging is likely to be disproportionately felt by children from non-traditional family structures where parental relationships may be more difficult to verify. In any event, we submit that this requirement should not apply in circumstances where the risk of any privacy harm from a service the child is trying to access is low.

Borrowing from COPPA, the NY Child Data Protection Act and the SAFE for Kids Act not the preferred model and not aligned with AADC

We understand that the consent and assent provisions in the Code draw from a combination of US frameworks, including the federal Children's Online Privacy Protection Act (COPPA), the New York Child Data Protection Act (NYCPDA), and the New York Stop Addictive Feeds Exploitation (SAFE) for Kids Act which we understand is not yet in effect.[38]

Our general understanding is that:

- COPPA is a longstanding US federal notice-and-consent framework, introduced in 1998, designed to protect children under 13.[39] It imposes certain requirements on operators of websites or online services directed to children under 13 years of age, and on operators of other websites or online services that have actual knowledge that they are collecting personal information online from a child under 13 years of age. These operators are only permitted to process a child's data after mandatory parental consent. There is no concept of the child's own assent.
- The NYCDPA, which is designed to protect teens aged 13-17, shifted away from COPPA's mandatory notice and consent approach to requiring either consent or restricted data processing based on what is "strictly necessary".[40] The approach in the NYCPDA was taken as a move away from the outdated approach in COPPA towards a privacy-by-design

[36] For example see: https://pmc.ncbi.nlm.nih.gov/articles/PMC12665752/?utm_source=chatgpt.com

[37] https://www.jmir.org/2022/8/e39094/

[38] https://ag.ny.gov/sites/default/files/regulatory-documents/safe-for-kids-act-nprm.pdf

[39] https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-312

[40] https://uk.practicallaw.thomsonreuters.com/w-043-6862?transitionType=Default&contextData=(sc.Default)&firstPage=true

approach focussed on collecting less data. Like COPPA, however, the NYCDPA's informed consent/data minimisation framework for 13-17 year olds applies far more narrowly than the Code – both as to the range of services covered and the circumstances in which the NYCDA operates. [41]

- Specifically, the NYCPDA only applies to online operators that *control the purposes and means of processing personal data* for *covered users*, where the operator either *knows* that the user is under 18; or the operator's service is *primarily directed* to users under 18.[42] In those cases, it requires entities to apply data minimisation requirements *or* obtain informed consent from 13-17 year olds. The rules that apply to 13-17 year olds are otherwise the same as those that apply to the broader population.
- The SAFE for Kids Act is not a privacy law but rather an online safety law aimed at restricting children's access to personalised social media feeds and other features that are 'designed to maximise engagement'.[43] It is the only one of these three frameworks that pairs a child-assent step with parental consent. It is not yet in force, and accordingly the operative detail has not yet been finalised. [44] In its current form, parental consent is required for certain specific functions such as providing algorithmically curated feeds to under 18s or to deliver overnight notifications.[45] Minor assent is proposed only for the limited purposes of permitting the platform to contact the parent to seek the required consent; not for assent to detailed and complicated data-handling practices (as covered in requirements of Part 3 Div 2 Section 2(2)(a) of the Code).

ADMA is concerned that the approach proposed in relation to consent in the Code appears to be a combination of the most restrictive requirements from these US frameworks without regard for the context or narrower scope in which they operate, and in a manner that appears to be inconsistent with subsequent developments to move away from mandatory consent in the US, as well as the privacy by design approach in the UK AADC and recommended in the Privacy Law Review Report.

We note that mandatory consent frameworks such as the consent framework under COPPA for under 13s in the US have been widely criticised as 'outdated', 'creating significant friction for online users' and 'actively discouraging companies from building open digital public spaces'.[46] These are issues that can be avoided by opting for a privacy by design approach such as the approach taken in the UK AADC, instead of adopting highly prescriptive obligations from legal frameworks that are based on traditional notice and consent style approaches. We recommend against adopting outdated mandatory consent requirements into Australian law and instead aligning more closely with the approach in the UK AADC.

Implementation issues

In addition to concerns outlined above about the proposed approach that the Code is taking, and the impact on children and parents, ADMA is also concerned that the mandatory consent provisions would give rise to significant practical implementation difficulties for APP entities in addition to those mentioned above, including:

- Verifying the parent is actually a parent
- Verifying the child's age
- Preventing children from circumventing the system

[41] https://uk.practicallaw.thomsonreuters.com/w-043-6862?transitionType=Default&contextData=(sc.Default)&firstPage=true
[42] https://uk.practicallaw.thomsonreuters.com/w-043-6862?transitionType=Default&contextData=(sc.Default)&firstPage=true
[43] https://www.privo.com/blog/new-yorks-safe-for-kids-act-what-the-proposed-rules-mean-and-what-to-do-now
[44] https://ag.ny.gov/sites/default/files/regulatory-documents/safe-for-kids-act-nprm.pdf
[45] Ibid.
[46] For example see https://texaslawreview.org/childrens-digital-privacy-and-the-case-against-parental-consent/

- Managing changing family circumstances
- Building and maintaining consent infrastructure
- Ongoing consent and data lifecycle management
- Record keeping and auditing
- Customer support requirements

Critically, in practice, operationalising these requirements is likely to result in significantly increased collection of personal information to verify age and parental relationships, therefore undermining the broader data minimisation objectives of the Code and placing entities at greater risk of data breaches.

ADMA therefore recommends that the proposed consent and assent obligations be removed from the Code.

Recommendation:

16. **The proposed consent and assent obligations should be removed from the Code.**
17. **Consent should not be required for use or disclosure of non-sensitive personal information, including for secondary purposes.**

3.6 Direct marketing

The Code introduces the following additional restrictions on direct marketing to children:[47]

- Organisations may only use or disclose personal information about a child for the purpose of direct marketing if:
    - APP 7.2 applies (that is, the personal information was collected directly from the individual and the individual would reasonably expect the personal information to be used for the purpose of direct marketing);
    - consent is obtained; and
    - the use or disclosure of the information is consistent with the best interests of the child. (Part 3 Division 1, section 11(3))

  Note 1 to section 11(3) makes clear that APP 7.3 does not apply, or in other words, entities may not use or disclose personal information about a child for direct marketing where that information was collected from a third party or where the use would not be reasonably expected by the child.

- In complying with APP 7.2(c), an entity must provide a clear, simply and easily accessible means by which a child may request not to receive direct marketing communications (Part 3 Division 2, section 29)
- That assent of a child under 15 must be obtained to use or disclose personal information about the child for the purpose of direct marketing (Part 3 Division 2, section 20)
- In complying with APP 7, an organisation may only use or disclose sensitive information about a child for the purpose of direct marketing if
    - the entity has explicit consent,
    - the information was collected directly from the child or the person with parental responsibility;
    - the organisation provides a clear, simply and easy to use means for the child to request not to receive direct marketing communications (opt-out) and

[47] legislation.gov.au/Details/C2016C00614

- the use or disclosure is consistent with the best interests of the child. (Part 3 Division 1, section 11(4))

In other words, for both sensitive and non-sensitive information, the following requirements apply:

- Direct marketing is only permitted with consent (and assent for children under 15)
- Use/disclosure of PI for direct marketing be in the child's best interests
- The information must have been collected directly from the child
- The child must reasonably expect the marketing use
- There must be a simple opt-out mechanism.

ADMA's key concerns in relation to the consent/assent requirements and 'best interests of the child' requirements are outlined in sections 3.3 and 3.5 above. We also note the following additional concerns specific to the direct marketing provision:

- **Consent** – the direct marketing provisions introduce consent requirements for uses and disclosures of *non-sensitive* personal information as well as sensitive categories, as well assent requirements for under 15s. ADMA is concerned that this will lead to consent being unmanageable for children, parents and entities, and may discourage direct marketing which is in the best interests of children (for example, health and wellbeing initiatives, age-appropriate learning content or online safety messages). Requiring consent for routine data-collection shifts responsibility for privacy to young people and will teach children to click-through without regard to the implications of what they are agreeing to. In our view, an overarching 'best interests of the child' requirement, together with existing data minimisation requirements under the APPs, more effectively minimises privacy harms for children.
- **Best interests** – as outlined in section 3.3 above, 'consistent with the best interests of the child' principle should operate as an overarching design principle so that entities can make determinations holistically based on context, and appropriately balance privacy, safety and other rights of the child (see section 3.3 above). There may be a range of interests to balance in an assessment of consistency with the best interests of the child, including access to information and services, digital inclusion, transparency of privacy practices and minimisation of unnecessary data collection, and agency, for example.

In addition, ADMA is also seeks clarification that 'direct marketing' continues to mean the use or disclosure of personal information to communicate directly with an individual to promote goods or services, consistent with the OAIC's guidance to date, as well as the Privacy Act Review Report 2022.[48] Targeted advertising enables entities to both serve appropriate content as well as exclude inappropriate content for reasons including age, safety and relevance. For these reasons, it would not be helpful or consistent with the Government's public policy objectives to require consent for delivering targeted online experiences, and targeting may be used by entities to facilitate experiences which are consistent with 'the best interests of the child'. These communications should remain outside of the scope of the direct marketing provisions. [49]

Recommendation:

18. 'Direct marketing' should continue to be defined as the use or disclosure of personal information to communicate directly with an individual to promote goods

[48] https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/organisations/direct-marketing; Privacy Act Review Report 2022, see 20.3, 196.

[49] https://www.oaic.gov.au/privacy/australian-privacy-principles/australian-privacy-principles-guidelines/chapter-7-app-7-direct-marketing

or services. Consistent with the approach taken in the Privacy Law Review Report 2022, it should not capture targeted advertising more broadly.

3.7 Destruction

Part 3 Division 5 provides that a child, or a parent if the child is under 15 years, may request an entity to destroy specified information and if the child or parent so requests, the entity must destroy that information.

ADMA does not support this provision and recommends that it be removed. APP 11 already requires entities *to take reasonable steps* to destroy or de-identify personal information once it is no longer needed for a permitted purpose. The existing requirements to destroy or de-identify information are rigorous and their precise application to a particular scenario depends on the circumstances, as set out in OAIC guidance on APP 11.[50] We are concerned that the Code leaves no room for assessment of the circumstances of the entity, the nature of the personal information or whether destruction is feasible.

Mandatory destruction requirements will not always be technically feasible in practice (see Section 2.5), particularly in relation to complex distributed systems, backups, logs, or downstream systems. In some circumstances, retaining certain information may support important safety, security, and integrity functions, including the provision of age-appropriate experiences and the exclusion of harmful or inappropriate content. These scenarios are recognised by the requirement to 'take reasonable steps' and the OAIC's guidance on APP 11.2.

Similar concerns were raised by stakeholders during the Privacy Act Review process in response to the proposal to change the standard to a requirement to take '*all* reasonable steps' to destroy or de-identify personal information. That proposal was not ultimately recommended. The Report instead recommended that the OAIC Guidelines in relation to APP 11.2 should be enhanced to provide detailed guidance that more clearly articulates what reasonable steps may be undertaken to destroy or de-identify personal information.[51] ADMA supports this recommendation. We remain of the view that some flexibility is required to deal with circumstances where destruction would be technically impossible, unreasonable or not appropriate in the circumstances.

Recommendation:

19. **The requirement that personal information must be destroyed on request should be removed from the Code.**

[50] https://www.oaic.gov.au/privacy/australian-privacy-principles/australian-privacy-principles-guidelines/chapter-11-app-11-security-of-personal-information; For example see para 11.30.

[51] Privacy Act Review Report 2022, Recommendation 21.5.