
1 About Streaming for Australia

1. This submission is made on behalf of Streaming for Australia (S4A). Streaming for Australia is a coalition of video subscription services, big and small, who collectively serve millions of Australian viewers, offer more choice than ever before, and support thousands of local jobs. We're committed to investing in local productions and talent, bringing diverse, high-quality stories to Australian and global audiences. Our members are Acorn TV, AMC+, AppleTV+, Disney+, Hayu, HBO Max, HiDive, Netflix, OutTV, Paramount+, Prime Video, and Shudder.
2. For more information please visit <http://streamingforaustralia.com.au>

2 Submission Overview

3. S4A welcomes the opportunity to respond to the Exposure Draft of the Privacy (Children's Online Privacy) Code 2026 (the Code) and the accompanying Draft Explanatory Statement (the Explanatory Statement). This submission draws upon S4A's members' engagement at the Office of the Australian Information Commissioner's (OAIC) Streaming Video On Demand (SVOD) roundtable held on 29 April 2026 and reflects the considered views of S4A's membership on how the Code can most effectively protect children's privacy while remaining workable for streaming services.
4. S4A is concerned that the scope and requirements of the Code, as currently drafted, are not proportionate to the privacy risks posed by SVOD services. SVOD services are characterised by professionally curated content, minimal personal information collection, subscription-based access requiring electronic payment, and the availability of parental controls and age differentiated profiles. The Australian Government has broadly acknowledged that SVOD services present a low risk in the context of the protection of minors. A position that is, for example, reflected in the Online Safety (Designated Internet Services – Class 1A and Class 1B Material) Industry Standard 2024 (OSA DIS Standard), under which SVOD services are classified as Tier 3 (lowest risk)¹.
5. We urge the OAIC to ensure the Code applies a flexible, tiered model that is proportionate to the actual privacy risk a service poses to children, rather than disproportionate, blanket coverage across all services. Low-risk services such as SVODs should face minimal compliance obligations under the Code. Only medium and high- risk services should be subject to the Code's full suite of obligations, and this should be expressly stated in the Code itself for certainty.
6. For SVOD service providers, it is essential that processes and regulations are aligned as much as possible across international jurisdictions, recognising national uniqueness while addressing the concern for children's privacy. S4A's members are global operators that already comply with, for example, the United Kingdom's Age-Appropriate Design Code (UK AADC), or the United States of America's Federal Children's Online Privacy Protection Rule's (COPPA). S4A understands the OAIC's

¹ *Online Safety (Designated Internet Services—Class 1A and Class 1B Material) Industry Standard 2024* (F2024L00710), Federal Register of Legislation, 21 June 2024, administered by the Department of Infrastructure, Transport, Regional Development, Communications, Sport and the Arts.

intention is to develop a Code that is aligned with the UK AADC framework. S4A strongly supports this approach and encourages OAIC to consider the US COPPA framework in its development of the Code.

7. We expand on this in more detail in the main body of the submission below, as well as providing other recommendations critical to improve the drafting of the Code.

3 Adoption of a Risk Based and Proportionate Approach

8. SVOD services are of inherently low risk to the types of privacy harms intended to be addressed under the Code, for the reasons set out below.

SVOD Services Are Inherently Low Risk

9. The overarching concern of S4A is that the Code, as drafted, is not proportionate to the privacy risks posed by SVOD services. SVOD services are characterised by professionally curated content, minimal personal information collection, subscription-based access requiring electronic payment, and the availability of parental controls and age differentiated profiles. While practices differ between service providers, SVOD services generally do not require child users to identify themselves. Instead, it is the adult account holder who sets up the children's profile². The nature of information collected in respect of child users is typically limited to their activity on the SVOD service itself (e.g. viewing history), and this information is typically only used within the SVOD itself. SVOD services generally do not offer targeted advertising on children's profiles; this means that there is no business case to retain data for any other purpose than to improve the service for subscribers.
10. These features place SVOD services at the lower end of the privacy risk spectrum, a position that is reflected in the OSA DIS Standard, under which SVOD services are classified as Tier 3 (lowest risk).³ Under the OSA DIS Standard, SVODs fall under the definition of a "classified DIS", which are designated internet services that have the sole or predominant purpose of providing general entertainment, news or educational content and films, computer games or publications that are or would be classified. Classified DIS that have no or very limited ability to post or share information, these services are deemed to be "pre-assessed classified DIS" and have a Tier 3 risk profile under the Standard (the lowest risk profile). Compliance obligations under the OSA DIS Standard for pre-assessed classified DIS are commensurate to the level of risk they pose.

Need for a Risk Tiering Mechanism

11. The draft Code risks an overly broad application of child privacy protection to adult directed platforms that allow child access with adult involvement. The "one-size-fits-all" approach fails to account for material differences across organisations, including the nature, volume and sensitivity of the personal information they handle, the purposes of its use, and the actual risk of privacy harm.
12. S4A recommends the following measures to make the Code substantially more workable:

² We are aware that one S4A member asks the adult account holder to provide a DOB when setting up a child profile, but that they do not use targeted advertising on the child profile.

³ Under the OSA DIS Standard, SVODs fall under the definition of a "classified DIS", which are designated internet services that have the sole or predominant purpose of providing general entertainment, news or educational content and films, computer games or publications that are or would be classified. Classified DIS that have no or very limited ability to post or share information, these services are deemed to be "pre-assessed classified DIS", and have a Tier 3 risk profile under the Standard (the lowest risk profile). Compliance obligations under the Standard for pre-assessed classified DIS are commensurate to the level of risk they pose.

- a) A clear distinction, aligned with the UK AADC, between data practices of easily accessible services and those of subscription-based services characterised by editorial oversight, professional content ratings, and payment barriers;⁴
 - b) Recognition of data processing required for internal operations, aligned with the US COPPA "support for the internal operations" exception,⁵ and core services, aligned with the UK AADC;⁶
 - c) Differentiation between data processing for behavioural advertising and processing limited to the delivery, measurement, and frequency capping of contextual advertisements (adverts that are based on the content viewed by a profile which normally uses a pseudonymous ID);
 - d) Consideration of privacy harms in the context of risk tiering of different categories of service, for example, services that offer public or semi-public profiles; the ability to see a child's online status; personal data that is shared publicly by default; chat functionality or ability to upload user generated content. This should be non-prescriptive but will assist services to identify their risk category.
13. S4A understands the OAIC's position is that not all Code obligations will apply to all services, and that those with a data-minimal approach should have fewer obligations to comply with. S4A strongly supports this position and submits that it should be clearly reflected in the Code itself, not merely in guidance.
14. S4A also notes the Department of Infrastructure, Transport, Regional Development, communications, Sport and the Arts (the Department) has recently released an issues paper regarding proposed draft legislation to implement a Digital Duty of Care in Australia under the *Online Safety Act 2021* (Cth). The duty is intended to be risk-based and proportionate, with the issues paper specifically stating that "[t]he obligations of the duty will be proportionate to a service's risk profile and their opportunity to address risks in the chain of service provision to users. Each service would be required to assess their risks and determine what preventative responses, systems and processes they can and ought to develop and implement to meet the Duty."⁷ S4A encourages OAIC to adopt a similar approach to regulating children's privacy, rather than the blanket approach that is currently being proposed.

4 Scope: The Definition of "Likely to Be Accessed by Children"

15. S4A acknowledges that the thresholds of "likely to be accessed by children" and "primarily concerned with the activities of children" are intended to limit the Code's scope.⁸ Designated Internet Services (DIS), Social Media Services (SMS) and Relevant Electronic Services (RES) that meet the "likely accessed by children" threshold will need to take reasonable steps to ascertain the age of an end-user before collecting their personal information. The Code relies on the broad definition of DIS from the *Online Safety Act 2021* (Cth).⁹ The DIS category under the Online Safety Act is extremely wide-ranging and includes websites and apps (including SVODs). As currently drafted, a vast number of DIS services could meet the "likely accessed by children" threshold and would have to take reasonable steps to ascertain age before collecting personal information, without regard to actual child privacy risks. A substantial number of these services arguably should not be subject to the Code.

⁴ ICO, *Age appropriate design: a code of practice for online services* at p.45-46, 88-89.

⁵ *Children's Online Privacy Protection Rule*, 16 CFR Part 312.

⁶ ICO, *Age appropriate design: a code of practice for online services*, Standard 12: Profiling.

⁷ <https://www.infrastructure.gov.au/sites/default/files/documents/digital-duty-of-care-for-australia-developing-duty-of-care-framework-for-online-services-used-by-australians-may2026.pdf>

⁸ *Privacy (Children's Online Privacy) Code 2026* (Exposure Draft), s 7.

⁹ *Online Safety Act 2021* (Cth), s 14.

16. The OAIC has indicated that it is working closely with the United Kingdom Information Commissioner's Office (UK ICO) guidelines, and that it is considering factors such as whether a service is attractive to children, targeted at children, or used by a significant number of children. S4A submits that the OAIC must publish this guidance before finalising the Code. Without clear guidance on when a service is in scope, no implementation planning can proceed with regulatory certainty.
17. S4A recommends either:
 - (a) A clear standard of "directed to children" (aligned with COPPA), rather than "likely to be accessed";¹⁰ or
 - (b) A list of criteria to assess the "likely to be accessed" standard, aligned with the UK ICO's AADC, considering:
 - i. the nature and content of the service and whether that has particular appeal for children;
 - ii. the way in which the service is accessed;
 - iii. terms or conditions that indicate an intention for the service or part of a service to be accessed by children;
 - iv. existing evidence that there are significant numbers of children on the service; and
 - v. any measures put in place to prevent children gaining access.¹¹
18. The UK AADC recognises that whether a service is "likely to be accessed by children" depends on "whether the content and design of your service is likely to appeal to children, and any measures you may have in place to restrict or discourage their access to your service".¹² The Code should explicitly recognise SVOD service characteristics (e.g. having parental controls, requiring a method of payment) as factors that reduce the likelihood of children accessing a service without adult involvement. Further, as the OAIC will be aware, in Australia SVOD content is governed by the National Classification Scheme (the Scheme), including classification markings, consumer advice, and age-appropriateness. The Scheme already provides clear, enforceable rules for content safety, including protections for children. To prevent overlapping / conflicting requirements which will be administratively burdensome to comply with, children's content safety protections for SVOD services under the Code should be aligned with existing requirements under the Scheme.

5 Scope: service likely to be accessed by children

19. Section 7 of the Exposure Draft states that the Code only applies to the provision of a SMS, a RES or a DIS that is likely to be accessed by children, or primarily concerned with the activities of children.¹³ The Explanatory Statement gives the example of a bank that offers a pocket money app for children, as well as a business banking and home loan app for adults.
20. OAIC should provide clarity on where different parts of a service are targeted and likely to be used by different age groups. In the context of SVODs, the Code should only apply to child profiles on SVOD services, child-directed areas and where the SVOD service has actual knowledge that a child user is

¹⁰ Children's Online Privacy Protection Rule, 16 CFR Part 312.

¹¹ ICO, *Age appropriate design: a code of practice for online services*, Services covered by this code.

¹² ICO, *Age appropriate design: a code of practice for online services*, Annex A.

¹³ *Privacy (Children's Online Privacy) Code 2026* (Exposure Draft), s 7.

accessing content on the SVOD platform. In practice, SVOD services are adult directed, meaning, children can use certain elements of the service but they do so under parental supervision.

21. In the SVOD context, the same app or website may be accessed in order to watch children's content (for example, on a tab or separate page marked as child or family content) as well as other content. Additionally, where a child profile is being used, the content displayed on the app or website will be tailored for that child user. For SVODs, the example given in the Explanatory Statement is not well suited: there is not a separate child-only app or website that is distinct from the general-audience app or website.

6 Purpose of age assurance

22. Section 8 of the Exposure Draft requires entities to take reasonable steps to ascertain the age of the end-user before collecting their personal information.¹⁴ This obligation applies to all end users. Further, we note that the purpose of age verification is not to determine whether the user is under or over 18 years of age, but rather to ascertain the user's actual age - a more substantial measure than what is required under the *Online Safety Amendment (Social Media Minimum Age) Act 2024* (SMMA), where in-scope services must take reasonable steps to prevent users who are under 16 from having accounts on their service.
23. We note that the UK AADC acknowledges that a service provider may be able to rely upon confirmation of a user's age from an existing account holder who the service provider knows to be an adult. Given the nature of SVOD services, and their use of personal information, we submit that such an approach is appropriate under the Code, and should be expressly recognised in the Code.
24. S4A further submits that compulsory upfront age assurance fundamentally contradicts the Code's data minimisation principles. Current age estimation technologies remain largely unproven at scale and introduce significant security risks. They rely on biometric or identity data that, if compromised, could produce the type of harm the Code is designed to prevent. The Code's separate age thresholds amplify these difficulties. SVOD providers must classify users across multiple age bands simultaneously, creating ongoing operational uncertainty while the underlying technology continues to mature.

7 Content Personalisation

Personalisation of SVOD services

25. Section 9 of the Exposure Draft requires entities to "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".¹⁵ The Explanatory Statement uses the example of a child signing up for an online messaging service. It provides that "the collection or use of the child's personal information to provide personalised recommendations, targeted advertising or make service improvements would not generally be strictly necessary to deliver the core messaging service".¹⁶

¹⁴ *Privacy (Children's Online Privacy) Code 2026* (Exposure Draft), s 8.

¹⁵ *Privacy (Children's Online Privacy) Code 2026* (Exposure Draft), s 9(1).

¹⁶ *Privacy (Children's Online Privacy) Code 2026* (Explanatory Statement), 8.

26. S4A submits that while this interpretation is appropriate for messaging services, its potential application to SVOD services raises significant concerns. Curated recommendations and content preferences based on viewing history are a functional core of an SVOD service and are not an optional add-on. A streaming service that cannot recommend content based on viewing history is fundamentally diminished. By way of example, it is reasonable to expect that a child who watches Bluey or the Wiggles on a SVOD service would be presented with the same or similar content. This content will have also been subject to rating and classification, additionally reducing risk relative to user generated content platforms. In this context, personalisation of content increases the likelihood that a child viewer will be presented with content that their parent or guardian is comfortable with. Turning off personalisation will degrade the user experience and require greater supervision by parents and guardians when their child is using a SVOD service.
27. S4A further submits that the “strictly necessary” threshold may prevent SVOD providers from adopting beneficial data uses that genuinely serve children’s interests, including safety and content moderation features, fraud prevention mechanisms, service integrity measures as well as general improvements to service quality over time. The limitations proposed by the “strictly necessary” test could have implications that impact other Australian regulatory frameworks and is therefore unnecessary and disproportionate.
28. The UKAADC stipulates that settings must be “high privacy” by default unless the service can “demonstrate a compelling reason for a different default setting, taking account of the best interests of the child”¹⁷. S4A maintains that content personalisation on SVOD platforms meets this threshold. The benefit of assisting children to discover age-appropriate, professionally-rated content consistent with their viewing history advances the best interests of the child.
29. The UK AADC expressly acknowledges that “taking account of the best interests of the child does not mean that you cannot pursue your own commercial or other interests”, provided that the best interests of the child is accounted for as a primary consideration where a conflict arises.¹⁸ Equivalent language should be incorporated into the Code to provide commercial clarity and certainty. S4A would also appreciate clarity from OIAC on how a best interests of the child threshold would be applied to low risk services such as SVOD’s. S4A members interests align with parents and the Australian Government. We want informed consumers and to hand choice and control measures to parents who can control what their children watch.

Recommended Approach

30. S4A recommends:
 - (a) Replace “strictly necessary” with “necessary”, which is supplemented by non-exhaustive OAIC guidance to determine necessity;
 - (b) Section 9 in the Code be aligned with the UK AADC, which recognises that a different default setting is permitted where consistent with the best interests of the child;
 - (c) The OAIC should also have regard to data minimisation post collection as part of a risk-based approach. The use of pseudonymous data, for example, is important for many low-risk data processing such as content recommendations;

¹⁷ ICO, *Age appropriate design: a code of practice for online services*, Standard 1: Best interests of the child.

¹⁸ ICO, *Age appropriate design: a code of practice for online services*, Standard 1: Best interests of the child.

- (d) Personalisation and recommendations based on viewing history (excluding behavioural advertising) should be expressly recognised as part of the core service for SVOD platforms, meaning this processing should not be disabled by default; and
- (e) Similar to the approach taken by the UK AADC, the Code expressly recognises that commercial interests are not always inherently incompatible with the best interests of the child. That said, the best interests of the child should be accounted for by the commercial entity as a primary consideration where a conflict arises.

8 Multiuser and Multi Device challenges

Unique Nature of Streaming Consumption

- 31. Streaming services are consumed by multiple users at the same time on the same device, such as the living room television or shared tablet. This is different from many other services, which operate on a single user / single account / single device model, such as social media and gaming. We encourage the Code to account for this reality.
- 32. Age assurance and verification are particularly difficult on a service intended for multiple users. The Code does not adequately address the question of whose age must be verified, whether it is the primary account holder, each individual who accesses the service, or each user for whom a profile has been established on the SVOD platform.

How Consent Flows in a Multiuser Experience

- 33. The Code should clarify how consent operates in a multi-user environment. It must address whether the primary account holder's consent extends to all users of the SVOD platform, or whether consent is managed on a profile-by-profile basis. The Code should also explain whether non-primary account holders who access the platform may withdraw consent or provide their own independent consent.
- 34. In an SVOD context, it will typically be the case that the service provider will not have the contact information of any user, other than the primary account holder. It would be incongruous if the Code were to require this kind of information to be collected in order that SVOD providers are able to comply with the Code.
- 35. S4A submits that it should be sufficient to assume that the primary account holder is the holder of parental responsibility if they set up children's profiles and exercise parental controls. The collection of payment details by an account holder, who then makes decisions about children's profiles and consents through that mechanism, should be expressly recognised in the Code or guidance as a sufficient basis for establishing parental responsibility.

9 Voluntary consent and bundling, informed and current consent

- 36. The bundled consent prohibition in Section 14(3)(b) of the Exposure Draft should be anchored to purpose, not to individual processing activities.¹⁹ A consent request that relates to a single identified purpose should not be treated as "bundled" merely because it encompasses multiple processing steps

¹⁹ Privacy (Children's Online Privacy) Code 2026 (Exposure Draft), s 14(3)(b).

in pursuit of that purpose. Requiring separate consent for each discrete activity within a coherent operation creates consent fatigue and undermines the quality of the consent process itself.

37. In the SVOD context, delivering a personalised viewing experience may involve collecting viewing history, analysing preferences and generating recommendations. Mandating individual consent for each step is operationally unworkable and does not meaningfully strengthen privacy protection for children.
38. Sections 15 and 16 of the Exposure Draft of the Code establish that consent to collection, use or disclosure of personal information about a child must be informed and current and sets out proposed requirements to achieve this. The practical effect of these proposed requirements, are an annual re-consent that must be facilitated by a service provider and navigated by account holders. S4A urges the OAIC to replace the 12-month mandatory re-consent requirement with a 'reminder'. Reminders would enable children and parents to review privacy settings and to uphold the principles of transparency and remaining informed. A 12 month re-consent requirement creates greater pressure on complex services, and can contribute to consent fatigue. S4A notes that, the UK AADC, for example, is not as prescriptive on informed consent requirements compared to what OAIC proposes in the Code, and in particular, does not generally require periodic renewal of parental consent on the basis of time elapsed. It is important that regulatory requirements around consent are streamlined, to encourage fewer, clearer, more meaningful consent interactions and avoid consumers becoming subject to constant consent layering.

10 Parental verification

39. The verification methods suggested in the Explanatory Statement, including video conferencing, government digital identity and bank-provided tokens, do not scale to the volume at which SVOD platforms operate.²⁰ These approaches create unnecessary barriers for parents and do not account for the wide range of family circumstances and levels of digital access across Australia. For SVOD services, where the primary account holder has already been verified as an adult through payment information, requiring further parental verification is duplicative.
40. S4A submits that the Code recognise practical, scalable verification methods, including account-holder confirmation as a legitimate means of establishing parental responsibility.

11 Register of Privacy Impact Statements

41. The requirement to publish a register of privacy impact assessments (**PIAs**) departs from international best practice and risks exposing commercially sensitive information. The UK AADC requires entities to maintain PIAs internally and provide them to the regulator upon request but does not mandate public disclosure.²¹
42. The benefit to the public of disclosing the existence of commercially sensitive risk assessments is unclear, particularly where the register adds no privacy protection for children beyond what would be achieved through a model where PIAs are maintained internally and provided to the regulator upon

²⁰ *Privacy (Children's Online Privacy) Code 2026* (Explanatory Statement), 12.

²¹ ICO, *Age appropriate design: a code of practice for online services*, Governance and Accountability

request. A public register imposes costs and confidentiality risks on entities without a corresponding benefit.

43. The OAIC's argument that the private sector should publish PIAs because government agencies already do so is flawed. Government agencies publish PIAs as part of broader public accountability obligations and compliance frameworks that do not apply to private entities. Extending a public sector transparency measure to them requires its own justification, not merely an argument by analogy. In any event, we note that *the Privacy Act 1998* (Cth) provides that only Commonwealth agencies are legally required to provide PIAs in Australia²². Respectfully, it would be a regulatory overreach for the OAIC to include this as a requirement on private companies under the Code, when this is not provided for in the underlying legislation.
44. S4A thus recommends that any mandatory requirement for SVOD's to prepare PIA's should be removed from the Code. Rather, the Code should expressly state that PIAs should be conducted and maintained internally on a voluntary basis, and made available to the OAIC on a best efforts basis upon request, without a mandatory public register. This approach is also aligned with the UK AADC.

12 Transitioning Users from Childhood to Adulthood

45. The Code should address how services can best serve a user who is transitioning from childhood to adulthood, and how to graduate them to the adult experience. Key questions that the Code does not adequately address include:
 - a. what kinds of notices are required;
 - b. what kinds of data can be preserved once the transition is made; and
 - c. whether opt in affirmative consent is required to turn off all safeguards, or whether safeguards can be turned off by default since the scope of the Code no longer applies.
46. The UK AADC categorises children aged 16 to 17 as "approaching adulthood" and recommends that services both "provide full information in a format suitable for this age group" and "allow them to choose between written and video/audio options".²³ The Code should provide clear guidance on graduated protections and the process for transitioning users to adult settings.

13 Notification of Children When Parental Consent Is Provided

47. Section 13(3) of the Exposure Draft requires an entity to provide an age-appropriate notice to a child when a person with parental responsibility provides consent.²⁴
48. We urge that the Code clarifies how this requirement is intended to operate in shared household and shared device environments common to streaming services, where accounts, profiles and devices are often used by multiple family members. It may not be possible to reliably identify the individual child user or provide child specific notifications at the point consent is given. On that basis we suggest that such a notification should not be required where these circumstances apply.

²² *Privacy Act* (Cth), s 33D.

²³ ICO, *Age appropriate design: a code of practice for online services*, Standard 4: Transparency.

²⁴ *Privacy (Children's Online Privacy) Code 2026* (Exposure Draft), s 13(3).

14 Alignment with International Frameworks

49. For SVOD service providers, it is essential that processes and regulations are aligned as much as possible across international jurisdictions, recognising national uniqueness while addressing the concern for children's privacy and safety. S4A's members are global operators that already comply with the UK AADC and the US COPPA. S4A understands the OAIC's intention is to develop a Code that is aligned with the UK AADC framework. S4A strongly supports this approach and urges OAIC to also consider the US COPPA framework as it develops the Code.
50. However, if the Code were to deviate significantly from this international alignment by, for example, diverging substantially from the UK AADC, S4A's members may be required to implement Australia-specific design changes, which would be burdensome and unnecessary where the UK AADC's privacy-protective framework is already well established and operating effectively in a comparable jurisdiction.

15 Direct Marketing in Shared-Household Environments

51. Section 11(3) of the Exposure Draft restricts the use or disclosure of a child's personal information for direct marketing purposes.²⁵ S4A submits that the Code should clarify that household-level marketing communications addressed to the adult primary account holder (for example, watchlist reminders, new-season notifications, and recommendations of forthcoming content) are not within the scope of this restriction, even where a child profile exists on the account. Without that clarification, SVOD providers face material uncertainty about ordinary subscriber communications that are not directed to or about any identified child user.

16 Transparency obligations and Child-Friendly Privacy Policies

52. The OAIC should simplify the compliance pathway under Section 23 of the Exposure Draft of the Code.²⁶ A privacy policy or communication should be taken to be age appropriate if it is written for a person aged 15 or over and includes a clear direction for users under 18 to consult a parent or guardian about any privacy matters. This approach allows most services to maintain a single, high-quality privacy policy. It avoids the need to develop parallel versions for multiple age groups, a process that is resource-intensive and offers limited benefit to children's understanding of their privacy rights given SVOD platforms are primarily directed at adults.
53. Section 28 of the Exposure Draft of the Code, which creates a right to request information about data handling, should be removed.²⁷ The enhanced transparency obligations under Division 3 of the Exposure Draft, together with the existing access regime under Australian Privacy Principle 12,²⁸ already provide children and their parents meaningful insight into how personal information is collected, used, and disclosed. A separate right to request this information duplicates existing protections and adds procedural complexity without additional benefit.

²⁵ *Privacy (Children's Online Privacy) Code 2026* (Exposure Draft), s 11(3).

²⁶ *Privacy (Children's Online Privacy) Code 2026* (Exposure Draft), s 23.

²⁷ *Privacy (Children's Online Privacy) Code 2026* (Exposure Draft), s 19.

²⁸ *Privacy Act 1988* (Cth) sch 1, Australian Privacy Principle 12.

17 Child assent for users under 15 years

54. The dual assent-plus-consent requirement for children under 15 in Section 20 of the Exposure Draft of the Code is largely duplicative.²⁹ The best interests' obligations and parental consent requirements in the Code already protect children effectively. Adding a separate child assent step before parental consent can be sought creates unnecessary friction, particularly in shared-household SVOD environments where the account holder has already set up child profiles and enabled parental controls.
55. The OAIC should reconsider whether the assent requirement is proportionate, especially for low-risk services where the added procedural burden is unlikely to improve privacy outcomes meaningfully.

18 Data deletion

56. Section 32 of the Exposure Draft requires entities to destroy personal information about a child upon request.³⁰ The de-identification of personal information should be recognised as an acceptable alternative to destruction. Where personal information can be effectively de-identified such that it is no longer reasonably identifiable, the privacy risk to the child is eliminated while allowing the SVOD service provider to retain data for legitimate purposes such as service improvement and aggregate analytics.
57. The right to destruction should also be subject to exceptions consistent with those recommended by the Attorney-General's Department in the Privacy Act Review Report, including where complying with the request is technically impossible or would impose an unreasonable burden on the entity.³¹

19 Implementation Timeline

58. Sufficient time should be provided to allow for the Code to be implemented.
59. The S4A recommends a minimum transition period of two years for the Code to come into effect, since many of these obligations will require significant design changes and substantial efforts to classify content in the catalogue and then apply proper metadata to impose the relevant restrictions. We submit that SVOD service providers require time to explain to end users how and why their services will change due to the Code's implementation.

²⁹ *Privacy (Children's Online Privacy) Code 2026* (Exposure Draft), s 20.

³⁰ *Privacy (Children's Online Privacy) Code 2026* (Exposure Draft), s 32.

³¹ Attorney-General's Department, *Privacy Act Review Report* (Report, February 2023) 182.

20 Conclusion

60. Thank you for the opportunity to provide this submission. Please do not hesitate to contact me if S4A can provide any further information, details or examples or otherwise assist with this review process.

Paul Muller

Convenor, Streaming for Australia