AUSTRALIAN RESEARCH COUNCIL
Centre of Excellence for the Digital Child.

31 July 2025

Submission to Office of the Australian Information Commissioner

Children's Online Privacy Code – Issues paper

By the Australian Research Council Centre of Excellence for the Digital Child

With thanks to the Centre members and partners who contributed to this submission, including Associate Professor Anna Bunn (Curtin University), Associate Professor Madeleine Dobson (Curtin University), Dr Maria Clara Riveria (University of Wollongong), Dr Andy Zhao (Deakin University), Dr Lois Peach (University of Wollongong), Dr Katrin Langton (Deakin University), Dr Rebecca Ng (University of Wollongong), Jason Weise (the Smith Family), Professor Tama Leaver (Curtin University).

About the Digital Child

The Australian Research Council Centre of Excellence for the Digital Child ('Digital Child') is charged with leading national and global research, policy and practice to ensure that all Australian children are healthy, educated and connected in a rapidly expanding digital world.

The Digital Child is shaping an environment with children, families, and communities so they can navigate their own digital worlds. We know that children's lived experiences are rapidly changing, and that every childhood is now fundamentally digital. Our mission is to create positive digital childhoods for every child in Australia.

We do this by focusing on:

- Healthy digital lives, understanding how digital technology intersects children's lived experiences and providing guidance to families, educators, and policymakers as they navigate this space.
- Educational empowerment, equipping children with the skills they need to live their best digital lives.
- Safe digital spaces, making online engagement safer while promoting healthy digital relationships.

We are excited to make a submission to the OAIC's Children's Online Privacy Code Issues Paper. Our response to the paper questions as well as some broad comments are below. We would be pleased to provide further information to the OAIC.

Contact information

Dr Tara Roberson
tara.roberson@qut.edu.au
+61 7 3138 8515

Broad comments

The Paper discusses how the Code will ensure privacy protections *for children who engage in a digital world*, and that the Code will *apply to online services likely to be accessed by children*.

This submission asserts that the Code needs to go further, and cover additional services or entities that collect, produce, share or process data about children, even prior to children accessing online services themselves.

From the moment they are born, children are *legal subjects* with the right to have others act in their best interest – including protection from the excessive collection and processing of their personal data. These rights are at adds odds with the current lack of data protection in online spaces. Children from their earliest life-stages are data subjects whose personal information is shared, collected and processed, without the ability to exercise their agency, and consent or object to these practices.

Parents are often relied upon to make decisions that protect their children's data privacy. However, as will be further outlined below, parents are often unable to provide meaningful consent regarding the sharing of their own and their children's personal data.

Therefore, children's rights for data protection must be regulated at a higher instance, and the Children's Code provides a unique opportunity to specifically identify and regulate data protection for children, from their earliest life stages.

Agency of children

In the stipulation for the purpose of the Children's Online Privacy Code, it is important that OAIC acknowledges in the Code that children at all ages have agency in their participation and in making decisions related to their interactions with digital technologies and in everyday living activities that generate data and a digital footprint. As such, it is expected that the Code stipulates ways for children to inform the Code not only at its initiation but in regular intervals moving forward.

The Children's Online Privacy Code proposes good reasons for the protection of children, the call for transparency in relation to targeted advertising, and in recognising that children do not have the opportunity to give meaningful consent or control over representations derived from data collected from children's participation related to digital technologies.

Children's privacy – systemic issues

We support the work of the Alannah & Madeline Foundation, which expresses the need for addressing not only visible harms like cyberbully and online grooming but also deeper systemic issues—such as data profiling, algorithmic manipulation, and the monetisation of personal information. At the core of these risks is the vast collection and exploitation of children's data, often without their knowledge or consent. This problem is exacerbated by the massive indiscriminate data collection involved in the creation of Large Language

Models that are driving the current generative AI tools, which including children's data without consent or notice.

Taking a digital inclusion perspective

Our partners at the Smith Family have heard from parents and students that there is a spectrum of digital skills and understanding about safety online, including privacy and data. In recent consultations with families and students, they raised the importance of staying safe online and wanting further information about how to do this. Respondents suggested that resources be provided in a variety of formats and in a way that was easy to access.

The Smith Family reports that 30% of the students they support live in families where they do not have access to laptop that is connected to the internet. This digital exclusion leads to a lack of opportunity to build foundational digital literacy skills. When children and young people are not regularly accessing digital platforms, they are less likely to understand how to opt out, restrict access or delete data. Those who are more digitally excluded will be more vulnerable to exploitation of their privacy data being utilised online.

For families from low-income backgrounds there is a greater reliance on free apps or services and so it is critical that these services also display clear and simple information for children and young people about what data is being collected and how it might be used.

For families with limited digital access, parents may also lack the confidence, knowledge and ability to understand the harms related to collecting data online from children. Any education around the privacy codes should not only be directed at children and young people but also in upskilling parents/carers who also may not have this knowledge or understanding.

From The Smith Family's perspective, a link needs to be made with the lack of access that some children and young people have to digital resources and how that will also impact on their understanding about data sharing online.

Specific interventions

Best interests test in development of services and collection, use and disclosure of information

The Issues Paper makes clear that: 'The Code may also include additional requirements if they are not contrary or inconsistent with the APPs.' The following comments therefore seek to suggest additional requirements that could be included in the Code and responds to the invitation in the Issues Paper to comment on issue more broadly.

As a minimum, the Australian Code should consider standards that mirror those in the UK's Age-Appropriate Design Code. The comments below suggest areas in which those standards can be expanded upon, for inclusion in the Australian code.

Best interest test

The UK's Age-Appropriate Design Code includes a best interests test that applies to the development of online services likely to be accessed by children. A similar test should be included in this code. The Privacy Act Review Report 2022 did suggest 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' (Proposal 16.5).

However, it is suggested that the test should extend beyond the design and development of services and include a provision that those entities bound by the Code should ensure that the collection, use and disclosure of children's personal information is fair and reasonable in the circumstances. This was proposed in the Privacy Act Review Report 2022 (Proposal 12.1). That Report also set out a range of legislated matters that could be considered in determining whether a collection, use or disclosure is fair and reasonable (Proposal 12.2). Where personal information relates to a child, the list of matters included a requirement to consider whether the collection, use or disclosure is in the best interests of the child.

Although the Australian government accepted both proposals in principle, they were not introduced into the *Privacy and Other Legislation Amendment Act 2024*. It is possible they may be introduced as part of tranche two of the Privacy Act reforms. This requirement, and the requirement to consider best interests in determining what is fair and reasonable, could be included in the Code, if they are not contrary to or inconsistent with the APPs. These requirements (it is suggested) are not contrary to or inconsistent with the APPs *except* in so far as the application of the fair and reasonable test might prevent direct marketing that would otherwise be permitted under APPs 7.2 and 7.3.

This could be dealt with, however, in the code by making it clear that the 'reasonable expectation' criteria (one of the criteria that must be met if direct marketing is to be permitted) is unlikely to be met if the use of the personal information for direct marketing is not in the child's best interest (noting that guidance from the OAIC on these APPs makes clear that the reasonable expectation test is an objective one, having regard to 'what a reasonable person, who is properly informed, would expect in the circumstances.')

Detrimental use of information

The UK Age-Appropriate Design code prohibits the use of children's personal data in 'ways that have been shown to be detrimental to their wellbeing, or that go against industry codes of practice, other regulatory provisions, or Government advice.' The Australian code should make it explicit that the use or disclosure of data in ways shown to be detrimental is not permitted and will automatically mean that the use will be considered *not* fair and reasonable.

This is not contrary to or inconsistent with the APPs except potentially insofar as the APPs permit direct marketing where the criteria set out in APP7.2 or 7.3 are met. In the same way as described above, this could be resolved through the Code (by stipulating that where the use is detrimental – and thus not fair and reasonable – the objective test as to reasonable expectations is unlikely to be met).

Alignment with the Privacy Act Review Report

The Privacy Act Review Report proposed a prohibition on direct marketing to a child 'unless the personal information used for direct marketing was collected directly from the child and the direct marketing is in the child's best interests' (Proposal 20.5); a prohibition on targeting to a child, with the exception that it is in the child's best interests (Proposal 20.6); and a prohibition on trading in the personal information of children (Proposal 20.7). These proposals were accepted in principle but have not come through in the first tranche of reforms. They may come through in the second tranche. Regardless, consideration should be given to introducing these prohibitions through the Children's Code.

It is suggested that these prohibitions are not contrary to or inconsistent with the APPs, with the possible exception of a prohibition on direct marketing. Again, that could be largely overcome in the same way as discussed above.

Nudge techniques

The UK Age-Appropriate Design Code includes a standard on nudge techniques and provides that services should 'not use nudge techniques to lead or encourage children to provide unnecessary personal data or weaken or turn off privacy protections.' The Australian code should include a similar standard, as this is not inconsistent with the APPs.

The requirement in the Australian code should go further and stipulate that entities should not use such techniques to encourage children to avoid engaging with privacy policies (such as, for example, where a box stating 'I have read, understood and agree to the privacy policy' is pre-ticked).

A right to deletion

The issues paper at the start discusses some input around the need for children and young people being able to have their data deleted.

The right for children to have many forms of online data be deleted at a certain age – probably the age of legal adulthood – is desirable, and encourages young people to experiment and fashion their identities and reputation online without being framed by that early play forever (Mayer-Schonberger, 2013). The right to deletion, though, should be

a right children choose to enact, not necessarily something that's automatic. While it is understandable and desirable in many contexts, especially on social media platforms and for-profit purposes, etc - it would be problematic if a universal right of deletion was mandated across all actors. For example, in the NFP space where services are delivered online to children. Certain data needs to be kept for appropriate provision of those services, additionally appropriate record keeping was one of these areas surfaced in the Royal Commission into Institutional Responses to Child Sexual Abuse. Having a general right to deletion but allowing specific services to articulate a clear rationale for keeping certain types of data, largely where that data is for the greater good of children overall now or into the future, should be possible.

Bad actors and good actors

On page 9, the Code stipulates the need to protect children from "bad actors such as hackers and scam actors". A dichotomous label will need to address such labelling and offer examples of what "good actors" might be. Considering that the mining of children's data can be misused not only by hackers and scam actors, but the use of such labelling may also be deceiving.

Location of data

Australia could take a similar stance that all data remains within Australia geographically and within the remit the Australian legal system as similarly stipulated in the European Union's General Data Protection Regulation (GDPR). Children should know where data is stored geographically and its trajectory from the APP entity to another institution or organisation, if relevant.

Response to Issues Paper questions

1. Scope of services covered by the Code

1.1 Are there additional APP entities, or a class of entities, that should be covered by the Code

Digital platforms for learning and entertainment purposes, including 'edtech' platforms, and parenting platforms should be specifically included on the APP entities list. We assert that the Code should cover any mobile application which collects data about a (developing) child/ren.

Data surveillance of children begins before they are born, and mobile applications aimed at parents (to be) play a key role in these processes. In the contemporary media environment, children's data is collected from their earliest life-stages and "even before birth", as asserted by Australian Children's Commissioner Anne Hollonds (2021) – echoing arguments made by many high-profile academics researching children and technology (Barassi, 2020; Holloway, 2019; Mascheroni & Siibak, 2021) and by children's rights advocates (Children's Commissioner, 2018; Cannataci, 2021). Practices such as the sharing of ultrasound images (Leaver, 2015), or the use of pregnancy-tracking apps and other *baby apps* are specific examples brought forward in this context (Hollonds, 2021; Langton, 2024a, Leaver, 2015). These digital practices contribute significantly to the vast amount of data being routinely collected about children, adding up to around "72 million data points before a child reaches the age of 13" (Holloway, 2019).

The prevalent use of *baby apps* – including fertility-, pregnancy-, and baby-tracking applications, results in the collection of a wide range of personal data about children. These apps are designed to support parents throughout the transition to parenthood – from family planning over pregnancy to early parenthood – and while many of these apps are 'free' to download and use, users commonly 'pay' for the use of these apps with their personal data. This personal data frequently encompasses not only the data of the apps' primary users – commonly parents, or parents-to-be – but also their children. App entities share this data with third-parties for monetisation, including consumer profiling (Hamper, 2024; Kemp, 2023). Because this data is not deemed 'health' data, and it is not explicitly recognised as data about children, no special protections apply. The indiscriminate handling of children's data in these contexts increases privacy risks for children, both through data-sharing with third-parties, as well as through unnecessarily long data storage periods – increasing the risk of children's data being shared with bad actors in data breaches.

The responsibility for the management of children's data collected in these apps must be regulated by a higher instance. Baby app users/parents feel that informed, meaningful consent for the sharing of their own and their children's personal data during baby app use is not possible, and there is increasing resignation and acceptance of pervasive data-sharing. Research into users' attitudes towards the datafication of parenthood through baby apps, confirms that the monetization of personal data through baby apps is becoming increasingly normalized and accepted (Hamper, 2024). This normalization is promoted by a sense of widely reported digital resignation (Draper &

Turow, 2019) – when users resign themselves to give up their personal data in exchange for access to a digital service.

Online sources of parenting support – including mobile applications – play a crucial role in the lives of Australian parents, who are often physically separated from sources of familial or professional parenting support (Cann et al., 2021; Langton, 2024b). The increased vulnerability that parents experience during the transition to parenthood and in early parenting (Virani et al., 2019; Langton, 2024a, 2024b), means that parental support needs frequently conflict with their children's right to privacy – complicating parental decision-making regarding the sharing of personal data required to access parenting support through baby apps.

The privacy policies of baby apps are often excessively long, vague, and contradictory (Kemp, 2023) – negating users' ability to opt-out of data-sharing or provide meaningful 'informed consent' (Okoyomon et al., 2019). These factors result in a sense of powerlessness, supporting the perception that "for many [parents] today, it has become impossible to escape this process of datafication, or to protect the privacy of their children" (Barassi, 2020, p. 34).

Emerging findings from "Tracking the Trackers", a study of children's first personal data

Research Fellows Katrin Langton from Deakin University and Rebecca Ng from the University of Wollongong, recently conducted analysis of app code for 38 popular baby apps, including 11 fertility-trackers, 16 pregnancy-trackers, and 11 baby-tracking apps. Additionally, the privacy policies of three highly popular apps were reviewed.

The aim of the study was to explore the infrastructural data-sharing capabilities of baby apps, and how these correlate with how the collection and sharing of users'/children's data are presented in baby apps' privacy policies.

They have so far found:

1. Ambiguity in baby app's privacy policies may change the ways users and policymakers think about children's data, downplaying the sensitivity of the data collected, and allowing its embedding into a wide range of data-processing practices, including machine-learning
2. Permissions for data access unnecessarily increase over time, and data from apps by the same developer is increasingly consolidated
3. Baby-tracking applications now commonly integrate AI-capabilities into their functionalities. Considering the rapid rise of AI and the increasing integration of AI 'solutions' and predictions into everyday decision-making, it is crucial to consider who is served through access to vast amounts of data on children's bodies and family routines.

These practices may breach children's rights to non-discrimination in ways that are difficult to anticipate and cannot be undone.

At a minimum, data entered into baby apps identifies to advertisers/commercial actors that a child exists, but often these apps promote the recording of children's personal information - including gender, age, (estimated) date of birth, location, behavioural and health information. This data can easily be shared and aggregated well beyond the contexts in which it was originally provided (Kemp, 2023). Once baby app users' and their children's data traces are passed on to third parties, the data is outside of the parents'/app user's control, and cannot be retrieved, viewed, corrected or deleted.

This data-sharing may have serious and permanent implications for children, if data is consolidated into online profiles, constructing a consumer identity and influencing children's self-understanding and online participation well before they ever generate digital traces themselves. It may also have serious implications regarding identity theft and fraud. The United Kingdom's financial institution Barclays has estimated that data from "sharenting" practices – including any information shared about children's names, birthdates and home address, and other family details deduced data traces that are collated over time, will account for two-thirds of identity fraud facing young people (Children's Commissioner, 2018). These data traces can include ultrasound images, or personal data collected and stored through baby apps. Data analysis for online profiling and prediction of young people's behaviours, routines and abilities, based on their available data traces, is also likely to become more prevalent, through increasing integration of AI technologies and sophisticated machine-learning.

Children's data privacy must be future-proofed, against the negative implications that may result from the AI-driven processing of their personal data Aside from explicitly identifying, personal information, many of the data traces produced during baby app use pertain to everyday family routines and are seemingly mundane. Yet, as long as there are enough of them, algorithmic analysis and specifically AI capabilities are employed to produce commercial value through predictions and evaluations of this data. These assessments are often highly simplified and reductive, despite narratives of 'data-driven insights' that lean into long-standing power dynamics associated with scientific authority (Moretti & Maturo, 2018) and data as trustworthy (Beer, 2019). The kind of 'transparency' assumed to be provided in privacy policies, does not provide sufficient basis for meaningful consent (Ananny & Crawford, 2018; Okoyomon et al., 2019) – making the use of children's data in the training of AI tools and other automated systems even more concerning.

Including baby apps' data and commercial entities in the entities regulated through the children's code would not only significantly contribute to future-proofing children's data privacy, but also the data privacy of all users of baby apps, including the bodies of (pregnant) women, who are particularly vulnerable and disproportionately datafied (Cahn & Manis, 2022; Kemp, 2023).

The entities who stand to gain commercially from the sharing of users' and children's personal data, need to take responsibility for users' and children's data privacy. Children's rights as *legal subjects*, must outweigh their commercial value as *data subjects*.

Example: There is 'offline' precedence for instances of excessive and problematic data-sharing, including the in-person collection of mothers' and newborns personal information through commercial actors.

One example is the maternal 'goody bag' provider Bounty, which shared personal information about new mothers and their babies, which they directly collected from new parents at the hospital bed while distributing 'baby essentials' such as nappies and samples of creams etc., to then share this data with third parties for advertising and marketing purposes (Murgia, 2019). Data collection from baby apps is not dissimilar, in how they collect data directly from new parents who are experiencing increased vulnerability and reliance on support that makes opting out of these services difficult, only to share this information for commercial gain.

Recommendations for risk mitigation

- App providers need to ensure any subsequent data processing does not interfere with children's right to privacy as children's best interest must outweigh the business interests of the commercial entities behind baby apps (United Nations, 2021, para. 68-69).
- App providers must take responsibility for the way that children's data may be processed by third-parties, particularly if it may be passed on to further data-processors and data-brokers, including marketing and advertising networks (United Nations, para. 40 & 42).
- Fines or other remedies for misuses of children's personal data need to apply, to encourage compliance

Summary of issues related to parenting apps

- User data from baby apps frequently encompasses children's data
- Users cannot meaningfully consent to the collection of this data on their children's behalf, since purposes of data collection and future uses of data cannot be accurately detailed and anticipated by app entities or app users, leaving children's data unprotected
- Data is often retained for unnecessarily long periods (Kemp, 2023, p. 26), exposing users and their children to risk of potential data breaches
- Data can be shared with third parties, including data-brokers who may circulate this data well beyond the contexts in which it was provided, and for which users provided their consent
- Data may be combined with other data traces, which could enable data-brokers to identify children specifically and accumulate data profiles about them, that can shape children's online experiences (access to information, media content, opportunities for online participation), their self-understanding and identities
- These issues are especially concerning in the age of AI

1.3 Is there criteria that should be used to determine whether a particular APP entity, or class of entities, is appropriately included or excluded from the scope of the Code?

Any entity that collects, shares, or processes children's data (meaning data *by* as well as *about* children), needs to be included. Children's data is frequently used as a stand-in for children themselves, and emerges well before children ever actively engage in the digital world, through the data traces shared and collected *about* them. If the aim of the code is about protecting not only flesh-and-blood children, but also their digital data and identities that may precede their own digital engagements while significantly increasing the risks of harm to children from data privacy infringements, it needs to specifically define *what* (and *when*) data being generated during online engagements, is children's data.

If it is not possible to specifically say whether an entity does collect data about children, but children's data *may be* collected during app use, all data produced in the context of app use should be considered sensitive, or a kind of 'family data', to which additional protections should apply (e.g. shorter retention periods, strict limitations on data-sharing and processing).

2. When and how the code should apply to APP entities

2.1 What threshold should determine when a service is considered 'likely to be accessed by children'?

Guidance from the UK Information Commissioner on the UK Age-Appropriate Design Code provides that a service is likely to be accessed by children if it is either (a) intended for children; or (b) not intended for children but likely to be accessed by a significant number of children. The ICO also explains that a service is likely to be accessed by a significant number of children if 'under 18s form a material group of people that use that service'. In determining what constitutes a 'significant number' (or material group), the ICO suggests that this requires an assessment of the number of users; the number of child users as a proportion of total users; and an assessment of the data processing risks posed to children.

It is also made clear by the ICO that:

> '"Significant" in this context does not mean that a large number of children must be using the service or that children form a substantial proportion of your users. It means that there are more than a de minimis or insignificant number of children using the service.'

In terms of the Australian code, it is suggested that the threshold should be comparable in that children are considered likely to access a service if is intended for them and/or if there is more than a de minimis or insignificant number of children using it. However, consideration should be given to using a descriptor other than 'significant': perhaps 'not insignificant' or, simply, 'material'. The following could be considered:

A service is likely to be accessed by children if it is:

(a) Intended for children; or

(b) Accessed or likely to be accessed by a material number of children.

In this context, materiality is to be determined by reference to the seriousness and extent of the information privacy risks; the total number of users; and the proportion of child users to adult users.

In the context of the UK, there was a deliberate decision not to set any particular number of child users, for reasons specified by the ICO. That should also be the case in terms of the Australian code. It could also be worth clarifying that a site is accessed by children where there is evidence that children are interacting with it/using it, even if access into the site has been gained because of the assistance of an adult.

As with the Age-Appropriate Design Code, several factors should be considered in determining whether a service is likely to be accessed by children. A non-exhaustive list should be provided in guidance.

Age gating and other controls may support APP compliance with the code but raise issues regarding inclusivity and discrimination and may not account for the context of use, e.g., children's co-use or parental access. Digital literacies and privacy education may be adopted as an alternative or additional mechanism to sustainably support privacy outcomes.

3. Age range-specific guidance

3.1 Would age-based guidance be appropriate and assist APP entities in tailoring protections and interfaces appropriately and effectively?

Responsive age-based guidance stands to make a helpful contribution in terms of meeting children's needs across different ages and considerations. It is heartening to see that the guidance will be contextual in terms of aligning to not only the age of young children, but their identities and needs. This reflects a supportive and rights-based approach which best serves children and young people as a diverse community.

3.2 In terms of providing guidance for the processing of children's personal information by APP entities covered by the Code, how appropriate do you consider the above age ranges would be?

The proposed age ranges should recognise a wholistic view of children as age brackets do not necessarily indicate a level of maturity and development of critical thinking. The management of children's digital participation is dependent on the social supports available to the child and each child's critical understanding of local and global issues.

Additionally, "0-5: pre-literate and early literacy" can be better classified for the following reasons:

- The use of "birth to 5" instead of "0-5" is in accordance with early childhood education terminologies.

- "Prior to school" or "early childhood" may better capture this period of a child's life. "Pre-literate" is not acceptable as a classification as all children develop literacy skills through their interactions with others from the moment they are born. Changing the classification label recognises that all children have a range of literacy experiences by the time they begin primary schooling.

4. APP 1 – Open and transparent management of personal information

4.1 What communication methods should APP entities use to ensure privacy policies are meaningfully understood by children of different ages, abilities and backgrounds?

In the same way that children and young people are diverse, so are their communication needs, styles, and preferences. Communication methods should be varied, adaptive, and creative to ensure that key messages are amplified, accessible, and best positioned to be understood and embraced by children and young people. This is also helpful in terms of supporting parents and other caring adults (such as teachers) to engage in dialogue with children and young people about these important matters. Methods might include: static multimodal information and live online and in-person discussions for children to share their experiences and understandings of the collection of their data and their understandings of online privacy.

When engaging in responsive and adaptive communication with children and caring adults, there are several guides and resources which can assist with ensuring that messaging is accessible (e.g. responsive to children's ages, stages, and abilities; using accessible and flexible language) and that multiple modes of communication are considered (e.g. using visual formats, considering creative ways to make messaging 'child friendly'). Potentially abstract concepts such as privacy and consent should be explained in developmentally appropriate and supported ways. Communicating with children should be flexible to children's needs according to the situation or context and may include adapted and accessible language, storytelling, real-world scenarios or analogies, or play-based approaches.

Finally, the policies themselves should be designed with target groups in mind and tested with users in the intended groups. There is literature on child-friendly design and transparency (e.g., Ingride Milkaite and Eva Lievens, Child-Friendly Transparency of Data Processing in the EU: from Legal Requirements to Platform Policies).

4.2 How should APP entities ensure APP1 obligations are met when their services are used by both adults and children, particularly when children are not the intended primary users?

Clear and obvious links to child friendly privacy policies should be provided. Entities should make sure that where users are under 18 and need to agree to a privacy policy before signing up, they are directed both to the full version and the child-friendly version.

APP entities could help ensure obligations are met when children are not the intended audience by considering mechanisms that develop privacy as default. Additionally, simple, child-friendly language and short, accessible information formats may also be

appropriate for adults in contexts where adults are considered the primary users and children may be unintended users).

4.4 What steps should APP entities take to ensure children, and their parents, can easily make privacy-related inquiries or complaints, and how should APP entities respond in a child-appropriate way?

APP entities complaint procedures may respond to children by using age-appropriate, accessible communication, including age-appropriate language and visuals, especially where the entity is likely to used by younger children. APP entities should demonstrate understanding of children's concerns and describe the consequences or potential actions taken in a simple way, avoiding legal or complex terminology.

Links to web-forms or email addresses for the purpose of privacy-related inquiries and complaints should be prominently displayed (eg on a home page) and not buried within terms and conditions or a privacy policy.

6. APP 3 – Collection of solicited information

6.4 Genuine consent How can entities obtain genuine consent from children, or their parents or guardians, for the collection of sensitive information?

APP entities may gain genuine consent from children in circumstances where the nature and intended use of data is explicitly explained to children and where they can reasonably withhold or withdraw consent without consequence (e.g., see previous comment about 'lite' versions of services). Whilst parental or guardian consent is necessary, APP entities should acknowledge the rights and abilities of children to take part in decision-making that concerns them, their data, and their privacy. APP entities could obtain genuine consent in circumstances where children have been able to respond to consent procedures in ways that are meaningful for them, including through processes which acknowledge that children communicate in a variety of ways and account for this by enabling forms of expression that include but are not limited to written language, such as through gesture, symbols, or images.

Ethical practices should be undertaken with a genuine, caring disposition by entities seeking to obtain consent from children and their caring adults, especially where the collection of sensitive information is involved. It is key to note that ethical practices should be apparent throughout the lifecycle of any project, from its inception through recruitment and onward into data collection and analysis (e.g. through engagement with relevant ethical frameworks; also by embracing a strong image of the child as a core part of framing any project which seeks to engage with children). There are ways to ensure that a deep sense of ethical literacy are embraced (e.g. through careful, reflective consideration of children and families), that any recruitment and subsequent data collection is respectful and responsive (e.g. guided by trauma-informed principles and practices), and that wherever possible, children have the opportunity to continuously consider their assent/consent or dissent regarding participation (e.g. in keeping with rights-based approaches to child participation). Methods of communication should be responsive to children's ages, stages, abilities, and needs, and as accessible as possible for

children and families alike. Creative, responsive methods are recommended to ensure that children and families are confident in their awareness of what data collection involves (e.g. using visual formats, considering creative ways to make messaging 'child friendly').

6.5 Do you have any specific views on how APP 3 should be applied, or complied with, in relation to the privacy of children?

APP entities should offer children options for temporary data collection, permanent data collection and for these options to be reviewed regularly.

It should be made explicit that the collection of data from third parties, for purposes of data enrichment, is not permissible (see Kathryn Kemp, 'The Forgotten Privacy Principle').

Where tools make it impossible to disentangle children's data once it has been collected or scraped, such as Large Language Models driving the current generative AI tools, that fact should be made transparent to all users, including children (Leaver & Srdarov, 2025).

8. APP 5 – Notification of the collection of personal information

8.1 Communication about data collection What methods can be employed to ensure children are aware of data collection practices in a manner that can be easily understood by children?

See 6.4