

5 June 2026

Office of the Australian Information Commissioner
GPO Box 5288
Sydney NSW 2001

Email: copc@oaic.gov.au

Privacy (Children's Online Privacy) Code 2026

Thank you for the opportunity to provide feedback the Exposure Draft *Privacy (Children's Online Privacy) Code 2026* (the Code).

The Shopping Centre Council of Australia (SCCA) engaged in the *Review of the Privacy Act 1988* in 2020 (including the original Issues Paper issued in October 2020), 2023 and in the development of the *Privacy and Other Legislation Amendment Act 2024*, which respectively recommended and enabled the introduction of the Code.

Our industry takes privacy issues incredibly seriously and has a standing item on privacy issues at our Board meetings. We closely monitor privacy and children's safety developments across jurisdictions to ensure that they are fit-for-purpose, and our members are able to meet any obligations. We note, for example, the recent introduction of Child Safe Standards in Queensland.

As public and 'crowded places', shopping centres and other retail settings are places that children attend both accompanied and unaccompanied by parents or carers, including as retail staff (noting retail is the largest employer of people aged under 18 in Australia) and customers.

Children and their parents are incredibly important visitors to shopping centres and we take their safety and security seriously.

Our industry actively attracts and runs activities such as 'parents with pram' car parking, children's playgrounds, children's rides, cater for children through retail tenants (e.g. toy shops), along with children's activities (e.g. occasional performances) and annual Santa photos.

Many of our members also have public transport stations located on their shopping centre sites, which generate large volumes of children entering and congregating within the shopping centre. There is generally a large concentration of children within shopping centres after school hours and on weekends. Further, our members' car parks are often used by youths driving P-plate vehicles.

For awareness, our industry also experiences unfortunate incidents with youth crime, including incidents where children are arrested by Police.

Our submission focuses on the applicability and impact of the Code to shopping centre operations that may interact with privacy requirements and range from the provision of free Wi-Fi services within shopping centres and the implications arising from the Code for e-commerce platforms and the purchase and activation of gift cards, to the use of Closed-Circuit Television Cameras (CCTV) for community safety and security purposes.

We have noted the issues relating to Wi-Fi and CCTV in our previous submissions, including noting that CCTV is an important aspect of our safety and security arrangements, including (when needed) to locate reported missing children.

This included, at the time, challenges relating to the need for explicit consent and a person's right to erasure, in relation to CCTV.

CCTV supports shopping centres to deliver on their responsibilities as designated crowded places under *Australia's Strategy for Protecting Crowded Places from Terrorism and Disrupting Hostile Reconnaissance Guidelines*.

We understand that shopping centre Wi-Fi services that are accessible to all visitors, including children, fall within the definition of a 'designated internet service' in the *Online Safety Act 2021*. However, further guidance is required as to whether CCTV and other operations classify as 'designated internet services' for the purpose of the Code, particularly where they are facilitated by internet connectivity and cloud storage services.

In particular, we are concerned about how the requirements to ascertain the age of child, collect, use or disclose personal information about a child consistent with their best interests, obtain consent for the use or disclosure of personal information, and deal with requests to destroy personal information are intended apply in the context of shopping centre operations and existing Australian Privacy Principles and permitted general situations under the *Privacy Act 1988*. We discuss these issues in further detail below.

Ultimately, we submit that the provision of free Wi-Fi services, other retail services such as the purchase and activation of gift cards and the use of e-commerce platforms, should be excluded from requirements of the Code, while clear exemptions should also apply when personal information is collected for the purpose of preventing and detecting retail crime.

Free Wi-Fi Services

As noted above, the requirements of the Code would appear to apply to free Wi-Fi services that are often provided in shopping centres for the use of customers. The requirements of the Code, particularly the general requirements detailed in pt 3, div 1 of the Code are problematic in terms of how they can be complied with by a provider of a free Wi-Fi service.

The ability of a free Wi-Fi service provided by a shopping centre to ascertain with any certainty the age of an end-user is limited, given the simple login process that exists for access to the service. Further, the implementation of an age assurance tool, as referred to in the *Draft Explanatory Statement*, as part of any registration process would create a financial and administrative burden that far outweighs the benefit of verifying the age of a person connecting to a public Wi-Fi service.

While we fully support the intention to protect the privacy and safety of children in online settings, we respectfully submit that a public Wi-Fi service merely facilitates online access, and that age assurance and other requirements would be more effectively placed on the online services that can be accessed through designated internet services.

Placing age assurance requirements on the online services that children may access through internet connectivity would create a closer connection between the requirement and the service that may seek personal information from children.

Shopping centres attract tens of thousands of visitors each day, many of whom access free Wi-Fi services out of convenience. Requiring each user to enter sufficient details to ascertain their age and then verify that information would simply undermine the convenient nature of the service, for no identifiable privacy benefit.

Without exclusions, the significant resources required to implement an age assurance tool for a free service provided for the convenience of customers are likely too great to justify continuance of free Wi-Fi services. This would be a poor public policy outcome given the negligible privacy benefit of the Code applying to Wi-Fi services.

Further, even if verification were not required, the veracity of the age information relies on the truthful input of information by the user.

As a flow-on consequence of the difficulties in ascertaining the age of the end-user, the requirements in the remainder of the Code, particularly the consent requirements in pt 3, div 2, are inherently difficult to comply with.

Accordingly, we recommend that public Wi-Fi services be excluded from the Code, particularly as these services are already required to comply with the Australian Privacy Principles.

Recommendation 1 Free Wi-Fi services that may be accessed by children should be excluded from the Code, in recognition of the existing privacy obligations they must comply with and the difficulty in ascertaining the age of the end-user.

Safety and security technology

Shopping centres deploy a range of safety and security mechanisms, including CCTV and body worn cameras on security guards, the footage from which may be uploaded to cloud storage services. Each of these mechanisms may be facilitated through designated internet services. We submit, however, that clarity is required as to whether the use of cloud-based CCTV that may capture and store footage of a youth offender is intended to be considered an activity or service that is “primarily concerned with the activities of children”.

The use of CCTV in retail settings is primarily to deter and detect antisocial and criminal incidents. When an incident occurs, the CCTV is intended to capture footage of the incident regardless of the age or identify of those involved in the incident.

Further, there are a range of different resourcing models across shopping centres for the monitoring of CCTV. For example, some large centres have control rooms that have staff monitoring CCTV 24/7, some that have staff only during core trading hours, and some that have different levels of staffing during peak trading times. Some shopping centres don’t have control room. The different levels of staffing make it impossible for consistent compliance with monitoring footage that features children.

This is distinct to other services that are specifically intended to capture footage of children. For example, the services referred to in s 5 of the *Draft Explanatory Statement*, such as early childhood development applications, family photo sharing applications, online school management systems and internet-connected baby monitors, are all specifically intended to capture and store information about children. In contrast, cloud-based CCTV may capture many more incidents involving adults than and cannot be said to be specifically intended to monitor children.

Recommendation 2 Clarity should be provided to confirm that services that incidentally capture footage or information about children are not “primarily concerned with the activities of children”.

While we recommend above that the intention should not be for services that may incidentally capture information about children to be within the scope of the Code, there are significant issues with the requirements of the Code should our recommendation not be followed.

For example, footage of an incident may indicate that a child is present, it is unlikely that the exact age of the child could be ascertained except with the assistance of law enforcement.

Further, requirements in the Code restrict or conflict with how any personal information in incident footage may be used, particularly in terms of providing incident footage as evidence to law enforcement. CCTV footage is an important component of the criminal justice process, and is used as part of the police investigation stage and right through to being tendered as evidence in criminal trials and Coronial Inquests.

For example, while s 10(6) provides an exception of the applicability of s 10 of the Code in circumstances where a permitted general situation (as per s 16A of the *Privacy Act 1988*) exists, and indirectly applies to s 11 regarding the use or disclosure of personal information about a child by virtue of the reference in s 11(2) to Australian Privacy Principle 6.2(c). WE also note the exception is also included in s 32 in respect of requests to destroy personal information about children. The SCCA supports these exceptions.

However, it not clear that any permitted general situation exception applies to pt 3, div 2 of the Code in relation to consent, or to pt 3, div 4 in relation to access to and correction of personal information about children, and the destruction of personal information about children.

The lack of exceptions in these provisions may result in a perverse outcome in which personal information obtained through CCTV footage and stored on a cloud-based service may be shared with law enforcement, but the consent of the child or their guardian was required for the footage.

To address this inconsistency, we propose that an exception from all requirements of pt 3 of the Code be introduced when a permitted general situation under s 16A of the *Privacy Act 1988* exists.

Recommendation 3 The requirements of pt 3 of the Code should not be applicable when a permitted general situation under s 16A of the *Privacy Act 1988* exists.

Other services

Gift Cards

We also seek clarity about the applicability of the Code on the purchase and activation of shopping centre gift cards, where those activities require online registration.

The SCCA is very alert to the regulatory framework for managing the risk associated with gift cards. We have recently worked closely with AUSTRAC and other industry partners to design an implementable and risk-based anti-money laundering and counter-terrorism financing framework that mitigates the risks that AUSTRAC is concerned about, while recognising the practical difficulties that gift card operators and retailers would face in checking and verifying the identification of all customers purchasing and redeeming gift cards.

There are no age-limitations on the purchase and use of gift cards, provided the products being purchased are not age-limited. As such, children may purchase and redeem gift cards. Where a gift card is purchased online, or requires digital activation, there may be circumstances in which personal information is required to be provided via online services.

Additional clarity would be appreciated as to the applicability of the Code on services such as gift cards that children may access and the provision of any personal information is incidental to the service being offered.

In the case of gift cards, the practical difficulties in implementing age assurance processes have been acknowledged by regulators such as AUSTRAC. Accordingly, the Code should not apply to the designated internet services that facilitate the registration or activation of gift card products.

Recommendation 4 The Code should not apply to specific services where other regulators have acknowledged that implementing age assurance processes are not feasible, particularly gift cards.

E-commerce Platforms

We also note the potential implications for e-commerce platforms that sell children's products.

Noting the purpose of the Code is to protect the privacy of children, there can be no benefit in requiring adults purchasing products for children to have to participate in age assurance processes.

While they may well be purchasing products that are "primarily concerned with the activities of children", in most cases any exchange of information does not require details about a child to be included as part of the transaction. We also note below in recommendation 6 the need for further clarity to be provided as to the point at which a service is "primarily concerned with the activities of children".

In addition, and similar to the gift cards issue discussed above, children may also access e-commerce platforms to purchase products. These services are transactional in nature, and where people under the age of 18 make purchases, are for products that are low-risk from a safety perspective for children given there are no legal age-restrictions on their sale and the information being provided as part of a purchase is subject to strict existing privacy controls.

We recommend that e-commerce platforms that sell children's products or may be accessed by children be excluded from the Code, given the well-established privacy processes and requirements in retail settings, and the impracticalities of implementing age assurance processes for the sale of products that are not age-restricted.

Recommendation 5 E-commerce platforms should be excluded from the Code in recognition of existing privacy controls, the low-risk nature of any personal information provided, and the impracticality of implementing age assurance processes in digital retail settings.

Further Guidance

While the inclusion of "reasonable steps" requirements, particularly in s 8 and s 13 of the Code, are not novel, what constitutes reasonable steps is dependent on the specific context.

Within the breadth of services that may be within the scope of the Code, there may be a range of different steps that are considered reasonable to ascertain the age of an end-user.

For example, a reasonable step for a social media service may be to implement an age assurance tool, given the age verification requirements that are part of the under-16 social media ban. But a reasonable step for another service may require the end-user to self-declare their age with no verification requirement.

We also note that the *Draft Explanatory Statement* states that “what steps are reasonable in the circumstances depend on the risk of harm that may arise from any collection, use or disclosure of the end-user’s personal information.”

Although we welcome the confirmation in the *Draft Explanatory Statement* that the OAIC will maintain guidance on age assurance technologies, broader guidance is required beyond specific age assurance technologies.

As our submission has highlighted, clarity is required for many aspects of the Code. Critically, guidance is necessary to support organisations to understand whether the services they provide are within the scope of the Code, what may constitute “reasonable steps” with reference to the service type, the potential harm that may arise, and the feasibility of implementing certain steps.

We also seek clarity as to the intended scope of a service that is “primarily concerned with the activities of children”. For example, as we’ve discussed in this submission, CCTV is used to obtain footage of any incident, regardless of the age of those involved. However, it is unclear whether footage of individual incidents would be considered in isolation, rather than in the context of all uses of CCTV. We recommend that guidance also include clarity as to the point at which an activity or service is considered to be “primarily concerned with the activities of children”.

- Recommendation 6 Guidance should be published, including with examples, by the OAIC that provides:**
- **Clarity as to the scope of services subject to the Code;**
 - **Whether an activity or service is “primarily concerned with the activities of children”; and**
 - **Context-specific examples of “reasonable steps”.**

Next Steps

We appreciate the opportunity to provide our feedback on the Code.

We note the Code is required to be registered no later than 10 December 2026, but the commencement date is yet to be determined.

As we have highlighted in previous submissions, and this submission, organisations performing services that are subject to the Code will need to procure, establish, and adjust a variety of processes and systems.

Further, where services are contracted to other parties (such as shopping centre Santa photos as we referred to above), contractual arrangements may also need to be updated to reflect any new requirements of the Code.

We would welcome the opportunity to engage further with the OAIC and the Privacy Commissioner ahead of the Code being registered and beyond, particularly in respect of any provisions that may need a delayed commencement as a result of the process and system updates that may be required subject to the final Code.

Shopping centres also procure a variety of services that be subject to the Code. Given the breadth of the services, targeted engagement between the SCCA and the OAIC would also support broader industry engagement with service providers to ensure that they are aware of any new obligations that they may have.

We would also welcome an opportunity to discuss issues as they relate to community safety and security, which we engage on extensively on including directly with law enforcement and other agencies.

Once again, we appreciate the opportunity to inform the development of the Code and look forward to engaging with the OAIC and the Privacy Commissioner further.

Sincerely,



Chief Executive
SCCA