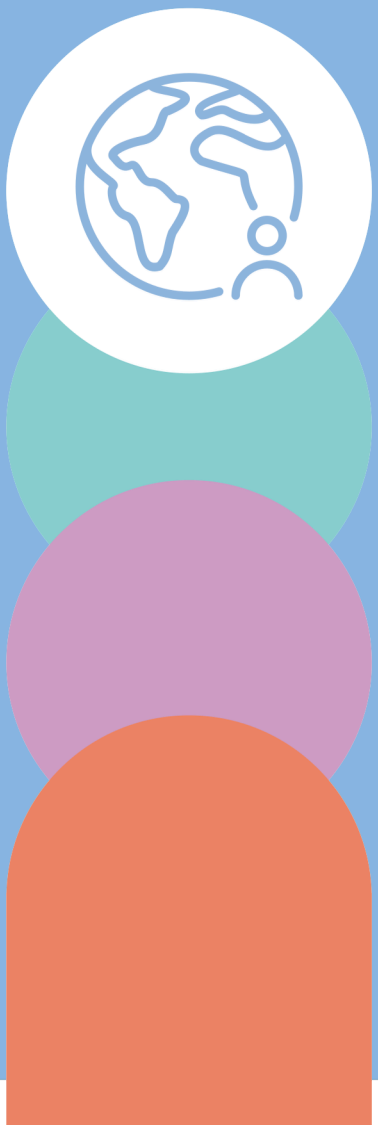
PART 3

Citizenship

Young children are active citizens in the digital contexts in which they play, learn, live and grow. Citizenship invites children to respect their own rights and those of others, relate to their communities and to appreciate the diverse backgrounds and experiences of people. Children's digital rights, privacy and online-safety education provide a foundation for safe, fair and equitable participation in digital contexts.

The guiding principle for Citizenship is: Young children's citizenship is upheld and fostered in digital contexts.



3.1 Children's digital rights: use, access and participation

Across the world, many people use the internet as a primary means of participating in society. People use the internet to access and engage in education, employment, health, entertainment and political activities. Access to the internet is therefore recognised as an important human right that facilitates the social and economic participation of people in society (Reglitz, 2023). The United Nations (2021) *General Comment No. 25 on Children's Rights in Relation to the Digital Environment* advocates for 'meaningful' technological access, including internet access, that 'can support children to realise the full range of their civil, political, cultural, economic and social rights' (p. 1).

However, fair and equitable use and access to the internet is not available to all children. Socioeconomic status, geographical location, cultural background and gender influence internet use and access by children and families in ways that either support or reduce their capacity to participate in society (Department of Infrastructure, Transport, Regional Development, Communications, Sport and the Arts, 2024; Lythreatis et al., 2022). For many children, their early childhood education and care setting may provide their primary opportunity to access and use the internet. This could be because they do not have any internet-enabled devices at home, internet access is not affordable, or they are geographically distant from stable internet provision. Meanwhile, technological innovations such as biometrics, Internet of Things, webcams, extended realities, AI and automated systems are part of the digital contexts children and their families may be part of, even when their own internet use and access is limited. For example, closed circuit television recording their activities in public spaces, automation used in social security decision-making, or early childhood education and care services using digital documentation to record personal information about children. Given the diverse experiences children and families have with the internet and digital technologies, the concept of children's digital rights in early childhood education and care settings is becoming more accepted (AGDE, 2022). Educators can support children's agency and voice in safely using and accessing the internet and digital technologies (Danby et al., 2025).

3.2 Digital privacy

Digital privacy considers how people and their data are represented, stored and re-used on the internet—with and without personal permission. Digital privacy is a serious issue for young children who may be vulnerable to how their digital data is created and managed by adults. For example, a young child might view a digital photograph of themselves on screen as a source of immediate pleasure and delight. However, young children are not always aware of how images or videos of them are used by well-meaning adults, or how AI can also be used to manipulate or fabricate images. The *National Model Code* (ACECQA, 2024) confirms that early childhood education and care services should have strict controls in place to safely store and use images and video recordings of children, and that only service-owned devices can be used to take images and video of children. Adults can model digital consent with children by asking permission to take their photograph and only posting pictures and videos of them on secure digital documentation platforms. Services should have family consent for any images and videos taken of young children and used in digital documentation platforms.

'The concept of children's digital rights in early childhood education and care settings is becoming more accepted.'

Even in situations where controls and child and family consent are in place, digital documentation can be inadvertently shared by educators or families, and children may appear in posts or data-sharing among adults they do not know. Children's right to privacy and informed consent around the use of their data may also be impacted by educators and services using AI applications for programming and planning, especially when observations or images of children are uploaded to AI to generate suggested learning experiences (Berson et al., 2025). Other issues can arise when services do not confirm with families or children how their digital data will be stored, for how long, and how it will be destroyed once children leave the service. This can include personal and sensitive information such as their name, address, age, social security details, health information, immunisation status, their family's employment details, and the number of adults and/or other children living in the child's home. More than one set of collected personal data can compromise children's and families' online identity through data triangulation. It is essential for services to have comprehensive policies in place regarding the management, use and retention of children's and families' personal data, images and videos.

3.3 Online safety

In previous generations, online safety was mostly considered necessary for older primary and secondary school–age children. However, many young children now regularly access the internet using touchscreen technologies, internet-connected devices such as watches or voice assistants, and by playing with internet-connected toys and robots (Kidron & Rudkin, 2023). Using touchscreen technologies, children watch online content, interact with apps or go directly online for gaming experiences. When playing with internet-connected devices and toys, children often enjoy integrating popular-culture characters from digital media and games into their play. Internet devices and toys can record children's voices and actions. AI embedded in internet devices and toys can create responses to children's play that generates curated user data and promotes continued interactions with children. In addition, biometrics can capture young children's faces, eyes or fingerprints and be used to authenticate their access to the internet. The many interactions young children have with the internet mean early childhood educators must consider how to promote online safety for young children.

> There are four main areas of online safety for educators to consider. These are **content**, **conduct**, **contract** and **contact** (Livingstone & Stoilova, 2021).

Content refers to the material children access and view online. Young children can be exposed to inappropriate content via the internet, such as violent, illegal or sexualised materials; advertising and games that promote gambling; and advertising for unhealthy food products (Stoilova et al., 2021). Research shows that high levels of product advertising via digital media increases young children's requests for unhealthy food and drink (Barker et al., 2022). Consumption of these products is associated with higher levels of overweight and obesity in early childhood. Online material accessed by young children can also reinforce gender, religious or cultural biases that do not help children become respectful participants in their communities.

Educators can reduce content risks by pre-viewing content they intend to use with children, using filters and setting restrictions on devices and networks used in early childhood settings. Educators should always co-view content with children. Educators can also seek guidance about appropriate digital content for young children from trusted providers or developers of digital games, apps and online content. Appropriate online content for young children fosters citizenship values of respect, tolerance and inclusion, promotes pro-social behaviours and provides opportunities for learning. Trusted providers and developers of appropriate and safe online material for young children include recognised government agencies and not-for-profit groups focused on the best interests of children.
Conduct is about how children interact, engage and behave with other people and digital activities online. Young children have slightly different conduct risks online to older children. Older children may be more likely to experience social exclusion, cyberbullying, image-based abuse, sexual extortion,

exposure to child sexual abuse material and other illegal and restricted content due to being online with more independence than young children (eSafety Commissioner, 2025). For young children, conduct risks can occur when they are using digital technologies that appear suitable for their age group, but are based on manipulative design features. Manipulative design features benefit the designer and not the child. They can include pop-ups, time pressures to complete in-game activities, character inducements to stay connected, and prizes for continued activity (Radesky et al., 2022). Manipulative design can also involve children in infinite scrolling, exposure to algorithms and recommender systems, and intermittent reward schedules that keep them using technologies. Pop-ups are another important conduct risk for young children because they tend to click on them thinking this will close the pop-up and enable them to continue with their activity. Young children also click on pop-ups when they are not yet able to read the text and can inadvertently select options that open the pop-up when trying to make it disappear. These clicking actions engage the pop-up so that children may accidently download viruses to the device, proceed to make digital in-game purchases without adult approval, or are re-directed to another online site where they may be exposed to inappropriate content.

Internet-connected toys and household objects used by children can retain their online connection even when children are not playing with them and continue to record data, such as conversations, without children's knowledge. Some apps used by children and educators in early childhood settings—even those that appear to operate offline—record large amounts of data about children without user knowledge. Data about the amount of time children spend using an app and their engagement levels can be recorded and sent over the internet to the app developer to inform future iterations of the app, or to directly target children for continued play, advertising or promotional materials. Wearable technology such as wristband activity and location trackers can also record data about young children's activities and whereabouts. AI chatbots embedded in children's toys may also pose conduct risks for children by generating, recording and reusing data about their language patterns, developmental progress and play preferences. Data recorded via internet-connected toys, household objects, AI, apps and wearables is called data harvesting and may be used by product companies to initiate further contact with children to promote additional purchase of products.

Not all digital technologies, apps, toys, AI and digital platforms developed for use with, by and for young children have been designed with in-built conduct safety protections. Often online safety concerns associated with these products are not identified until after market release. Being aware of conduct risks in terms of accidental downloads, in-app purchasing, site re-direction and data harvesting can help educators take a proactive approach to young children's online safety. For example, if using activity trackers with children to promote learning about health and wellbeing, educators should first check permission options for data harvesting and ensure these are turned off. Educators can also teach young children to respond to unwanted pop-ups by clicking the corner 'x' to close, or to seek adult help if they encounter pop-ups. During online game or app play, educators can engage young children in conversations about respectful interactions with people, such as avoiding name-calling and teasing, and turn-taking among peers. Educators should engage in active supervision of children when using AI-enabled products in early learning settings.

'Educators should engage in active supervision of children when using AI-enabled products in early learning settings.'

Contact involves children engaging with people online. Children may contact people they know online, such as friends, family or kinship members using video-chat, messaging, digital documentation platforms or social media. But children may also encounter people they do not know, for example when playing in virtual worlds or multi-player, internet-based games. AI can be used by people children do not know to analyse their in-game activity and identify them as targets for grooming. AI can also be used by people unknown to children to interact with them about their interests, creating false identities and relationships as a means of exploitation. Children may reveal personal information such as their name, age and address to people or AI they encounter online whose intent is to trick or manipulate them. Children can also be exposed by people or AI to inappropriate content or conversations online.

Early childhood educators are committed to teaching young children about trusted adults in their lives and the importance of asking trusted adults for help. Educators can extend this teaching so that young children understand a trusted adult can help them use the internet safely. It is important that adults remain open to hearing from children about their online experiences so that children learn from a young age that adults can help them.

Active adult supervision of young children online is critical (Pons-Salvador et al., 2022). Active supervision involves applying filters and controls to devices and networks, checking privacy and location settings, being physically present with children when using the internet, and having discussions with children about their internet use.

Contract risks occur when young children are exposed to terms and conditions that they may inadvertently accept. This is most likely to happen when children are using online games or apps. Some terms and conditions children accept might agree to the collection and on-selling of their personal data. Children might also make in-app purchases, buy game tokens or sign up for long-term use of a game or app.

Adults can minimise contract risks by ensuring payment options are turned off devices and that in-app purchases are disabled on games that children use. Active adult supervision of young children online provides appropriate opportunities for modelling privacy and data protection with children against contract risks, such as selecting 'required only' user permissions on websites and apps, using passwords and ensuring two-factor authentication.

3.4 Online-safety education

Children can learn how to participate safely and productively in digital contexts through online-safety education (Ladd & Traver, 2023). Research shows that children are accessing the internet more often than in the past (Konca, 2022). The increase in young children's internet use has led to the inclusion of online-safety education in the EYLF V2.0 (AGDE, 2022) and international recommendations for online-safety education in early childhood education and care (e.g. United Kingdom Council for Internet Safety, 2019). Online-safety education in the early years can support children to explore how people safely use technologies as per the Australian Curriculum (ACARA, n.d.).

There are many examples of well-designed online-safety education resources for primary and secondary school–age children, for example www.thinkuknow.org.au, www.esafety.gov.au and www.esmart.org.au. Because older children are more likely than younger children to understand the internet as a network of technologies, these approaches focus on teaching children how to engage in safe behaviours online and where to find trusted help and support.
Online-safety education for young children cannot simply be adapted from programs developed for older children, because young children do not understand the internet in the same way as older children and adults (Danovitch, 2019). Young children identify the internet as the device they are using, or as the social practices they observe people engaging in online. For example, preschool-aged children describe the internet as being 'in my iPad', or as being available for 'doing emails' and 'playing games' (Edwards et al., 2018).

For younger children, online-safety education can begin with early understandings about digital technologies as networked. Because children learn through play and social interactions, educators can design play experiences that help young children understand that digital technologies are connected. For example, educators can create internet play walls with images of devices connected by strings that children can use to send messages and share emoticons. Pretend internet play can also be supported by connecting non-working devices in office or home play stations with string. Pretend play with phones or devices made from cardboard or wood facilitates opportunities for children and educators to discuss how data is shared via wireless networks. Research suggests that opportunities for play-based learning about the internet facilitates children's online-safety education, such as ensuring that children seek adult support when using the internet, or that children always co-view digital content with a trusted adult (Edwards et al., 2025).

Using the internet with young children in early childhood education and care settings also creates real-life online-safety learning opportunities. For example, educators can model using passwords and two-factor authentication, avoiding pop-ups and not being distracted by suggested content. Educators and children can also participate in shared discussions about the quality of content and information they access on the internet and the extent to which it meets their purposes.

Citizenship

Principle: Young children's citizenship is upheld and fostered in digital contexts

Practice advice:

01 Participate in professional learning opportunities to build understanding about young children's digital rights and how these relate to young children's socioeconomic, geographic, gender and culturally based experiences in digital contexts.

02 Commit to working ethically with children and families when using digital documentation and AI, including obtaining consent to use images and video of children via digital documentation platforms and educational AI applications.

03 Develop policies and guidelines about the collection, use, retention and deletion of digital data held about young children and communicate these to families.

04 Ensure active adult supervision of young children's online activities, including the use of filters and restrictions on devices and networks, checking privacy and location settings, and always co-use devices with children in the education setting.

05 Facilitate and maintain conversations with young children about their online experiences, both positive and negative, to ensure they are supported by trusted adults in their online engagements.

06 Help children develop an understanding of the internet as a network that people and AI use to generate, store, retrieve and share information.

07 Model internet use with children for learning purposes and provide opportunities for assessing the quality and relevance of information generated by people and AI.

08 Direct families towards government and trusted not-for-profit organisations for advice on selecting digital media, content, apps, games and AI that are appropriate for use by young children.