PART 3: CITIZENSHIP

Citizenship in digital contexts recognises that young children are active participants in their communities now and into the future. As citizens, young children respect their own rights and those of other people, and develop an appreciation for cultural, racial, gender and religious diversity. Digital rights, digital privacy, online safety and cyber-safety education provide a foundation for early citizenship in digital contexts.

3.1 Children's rights to digital access

The increased use of networked digital technologies by people from around the world underpins the notion of digital rights. Across the globe, people now use the internet as a primary method of communication, and to share, store, retrieve and collect digital information or 'data'. It is used daily for activities associated with education, employment, health, entertainment and political participation. In the digital age, the internet is recognised as an important form of social infrastructure that enables people to participate in their communities (Livingstone & Third, 2017). For this reason, it is increasingly considered that all people should have the right to access digital technologies and the internet. In 2016, the United Nations Human Rights Council passed a non-binding resolution recommending that countries should not block citizen access to the internet (United Nations Human Rights Council, 2016).

It is estimated that one in three people who access the internet worldwide are under 18 years of age (Livingstone, Carr & Byrne, 2016). Research suggests that children also consider digital access a basic human right (Livingstone et al., 2016). Technological innovations such as voice recognition, Internet of Toys, Internet of Things, virtual reality and artificial intelligence are increasingly shaping the digital context in which children participate. As such, while the concept of digital rights in early childhood education and care settings is new, it is likely to grow in importance.

Yet digital access is not fairly and equally available to all children. Issues of finance, geographical location, cultural background and gender (Warschauer & Matuchniak, 2010) influence digital access by children and their families in ways that promote and/or reduce social participation. For many children, early childhood education and care settings may provide their primary point of access to digital technologies and the internet. For this reason, young children's digital rights regarding technology use, internet access, and learning how to participate in digital contexts safely and productively will become increasingly important areas of professional learning and practice for the sector over time.

3.2 Digital privacy

In addition to recommending citizen access to the internet, the United Nations Human Rights Council (2016) also promoted the human right to privacy online. Digital privacy considers how people and their information are represented and stored on the internet—with and without personal permission. Digital privacy is a serious issue for young children who often do not have explicit knowledge or control over 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 educators and family members. Many adults do not routinely ask young children for permission to take their photograph, or to post pictures and videos of them on social media sites and/or digital documentation platforms.

Even in situations where parental consent is required for images of children to be used in early childhood education and care services, social media and 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. Other issues can arise when services do not confirm with families or children about how long their digital data will be held 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, employment details of kinship members, parents and/or caregivers, and the number of adults and/or other children living in the child's home. By attending to these issues, early childhood education and care services can provide some of the first models of appropriately enacted digital privacy that children and families experience as they enter the education system.

3.3 Online safety

In previous generations, managing online safety was generally only considered necessary for older primary and secondary school age children. However, current research shows that many young children now regularly access the internet via touchscreen technologies and the Internet of Toys (Holloway & Green, 2016). Touchscreen technologies enable children to watch online content, use internet-connected apps or go directly online for gaming experiences. Using the Internet of Toys, children can integrate internet-connected, popular-culture figurines, dolls and/or soft toys into digital media, digital games, and/or have the toys record their voices and actions in ways that generate an internet-based response from the toy. The increasing level of interaction that young children have with the internet means early childhood educators must consider how to promote online safety for young children.

There are three main areas of online safety for educators to consider: content, conduct and contact (Livingstone & Haddon, 2009).

Content refers to the material children access and view online. Young children can be exposed to inappropriate content via the internet, such as violent and/or sexualised materials, advertising and games that promote gambling, and promotions for unhealthy food products (Warburton & Highfield, 2017). Research shows that high levels of product advertising via digital media increases young children's requests for unhealthy food and drink (Cairns, Angus & Hastings, 2009; Livingstone, 2006; McGinnis, 2006). 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 and/or cultural biases in ways that are unhelpful for building children's capacity to participate in and contribute to their communities.

Educators can reduce content risks by using filters and setting restrictions on devices and networks used in early childhood education and care settings. Educators can use these practices as examples to help families learn how to promote and provide safe online experiences for children at home. Educators can also seek guidance about appropriate digital content for young children from trusted providers and/or promoters of digital games, apps and online content. Appropriate online content for young children fosters citizenship values of respect, tolerance and avoidance of discrimination, promotes pro-social behaviours and provides opportunities for learning. Trusted providers and promoters of appropriate and safe online material for young children may 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 bullying, sexting or social exclusion online due to using social media (Office of the eSafety Commissioner, 2018b; Office of the eSafety Commissioner [Australia], Netsafe [New Zealand] and UK Safer Internet Centre with the University of Plymouth [UK], 2017). For young children, conduct risks can occur if they accidently access or download copyrighted or illegal material. Also, when using Internet of Toys, touchscreen devices and/or apps on mobile devices, young children experience conduct risks by accepting pop-ups (Kervin, 2017). This occurs when children click on pop-ups thinking it will close and enable them to continue with their activity, or when they are not yet able to read pop-up text and so select an option that makes the pop-up disappear. These clicking actions typically engage the pop-up so that children

inadvertently download viruses to the device they are using, proceed to make digital in-game purchases without adult approval, and/or are re-directed to another online site where they may be exposed to inappropriate content.

At other times, Internet of Toys used by children may 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 education and care settings—even those that appear to operate offline—can record large amounts of data about children without user knowledge. Digital 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 and/or advertising and promotional materials. Microchips embedded in children's clothing, and wearable technology such as wristband activity trackers, can also record data about young children's activities and location. Data recording via Internet of Toys, apps and wearables is called data harvesting, and may be used to initiate further contact with children to promote additional purchase of products.

Not all digital technologies, apps, toys and digital platforms developed for use with, by and for young children have been designed with in-built conduct safety protections, and online safety concerns associated with these products may not be 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 can first check permission options for data harvesting and ensure these are turned off. Educators can also help young children learn how 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 other people, such as avoiding name-calling and teasing, and/or promoting turn-taking among peers.

Contact involves children engaging with people online. Children may have contact with known people online, such as friends, family or kinship members through video conferencing, digital documentation platforms or social media. But they may also have contact with people unknown to them, for example when playing in online virtual worlds or participating in multi-player, internet-based games. Children may reveal personal information such as their name, age and address to people they meet online, or they may be exposed by others to inappropriate material or interactions.

Proactive adult supervision of young children's online activities is important (Buckleitner, 2008). Supervision may vary according to the online environment children are using. For example, watching educator-selected content on an approved government or not-for-profit streaming app may not carry the same contact risk for children as engaging in a networked gaming platform. Educators can also help children learn that not everyone they encounter when using internet-enabled devices is someone they know. Early childhood educators are already well-versed in teaching young children the importance of talking with trusted adults, and can build on this skill to help young children learn that not everyone they will engage with while using the internet is a trusted adult. It is important that adults remain open to hearing from children about their online experiences (both positive and negative) so that children learn from a young age that adults can support them in their engagement with other people online.

3.4 Cyber-safety education

Children can learn how to participate safely and productively in digital contexts through cyber-safety education (Office of the eSafety Commissioner, 2018a). International research shows that children worldwide are accessing the internet more and more often (Livingstone, Mascheroni & Staksrud, 2017), which has led to national and international recommendations that cyber-safety education begin with young children before they start school (Children's Commissioner for England, 2017; Joint Select Committee on Cyber-Safety, 2011). Cyber-safety education in the year before school can support the capacity of young children to share information in safe online environments

as per the 'Digital Technologies Process and Production Skills' Learning Area for Foundation through to Year 2 of the Australian Curriculum.

There are many examples of well-designed, cyber-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 to understand the internet as a network of technologies, these approaches focus on teaching children how to engage in safe behaviours online.

However, cyber-safety education for young children provided in the years prior to school cannot simply be adapted from programs developed for older children, because young children do not understand digital technologies and the internet in the same way as older children and adults (Ey & Cupit, 2011; Yan, 2005). Young children identify the internet as the device they are using, or as the social practices they observe people engaging in online. For example, children describe the internet as being 'in my iPad', or suggest the internet is for 'doing emails' and 'playing games' (Edwards et al., 2016). These descriptions provide an important insight into what young children understand about the internet.

For younger children, education needs to start by building early thinking about the networked nature of digital technologies. Because children learn best through play and social interactions, educators can design play activities that help build young children's understanding of how digital technologies are interconnected, or networked. For example, children could send 'emails' as messages in an envelope attached to a series of pretend computers or touchscreens that have been 'networked' with each other in the home-corner using string. This can help children visualise how digital networks are created and used to 'send' emails as a way of sharing information.

Using the internet with young children in early childhood education and care settings also creates real-life learning opportunities for cyber-safety education. Educators can explain how information is created and shared by people on the network. Educators and children can consider the quality of the content and information they access on the internet and the extent to which it meets their purposes.

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

Practice advice:

1. Participate in professional learning opportunities to build educator 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.
2. Seek permission from children and families to use digital documentation, including photographs of children via social media and/or other digital documentation platforms.
3. Develop policies and guidelines about the collection, use, retention and deletion of digital data held about young children and families.
4. Ensure proactive adult supervision of young children's online activities, including the use of filters and restrictions on devices and networks in the early childhood education and care setting.
5. Maintain conversations with young children about their online experiences, both positive and negative, to ensure they are supported by adults in their online engagements.
6. Help children develop an understanding of the internet as a network that people use to generate, store, retrieve and share information.
7. Model internet use with children for learning purposes and provide opportunities for assessing the quality and relevance of information.
8. Direct families towards government and/or not-for-profit organisations for advice on the selection of digital media, content, apps and games that are appropriate for use by young children.