CHILD SAFETY

NQF Online Safety Guide

Table of contents

Contents

About this guide 5

Acknowledgement of Country 6

Using the NQF Online Safety Guide 7

Content warning 9

Chapter 1: Building a Child Safe Culture in the digital environment 11

Introduction 11

Resources 13

Digital technology and children 15

Chapter 2: Using digital technologies safely 15

Collecting, storing and sharing personal information 18

Consent 21

Case Study - Children bringing their devices to outside school hours care 25

Questions to guide reflection on practice 26

Resources 27

Chapter 3: Safe online practices within education and care services 34

Safe online practices 34

Professional development for educators 36

Online supervision 38

Myths about online child abuse 40

Responding to disclosures of online child abuse 42

Reporting online child abuse 44

Case study - Teaching children to be safe online 45

Resources 46

Chapter 4: Embedding online safety 50
Online safety practices 50
How to implement online safety 51
Aboriginal and Torres Strait Islander cultural safety online 53
Preventing online safety risks 54
Unwanted or unsafe contact 55
Case Study - Discussing online friends with children 57
Self-generated sexual content or personal image sharing 58
Image-based abuse and sexual extortion 60
Online grooming 61
Case Study - Discussing online games with children and listening to children's voices 63
Questions to guide reflection on practice 64
Resources 65
Chapter 5: Using electronic devices safely 70
Using electronic devices safely 70
Smart toys 72
Child-friendly search engines and apps 73
Practical ways to make devices safer 74
Optical surveillance devices 75
Keeping personal data safe 77
Case study - Collaborating to create service device rules 79
Questions to guide reflection on practice 80
Resources 81
Chapter 6: Artificial Intelligence (AI) and online safety 86
Use of AI 86

Using AI tools and AI-enabled toys with children 88
Case study - Purchasing a new smart toy 89
The use of AI tools as part of children's learning 90
The use of AI tools by educators to create the curriculum 91
What information can be used by AI tools 94
Educating children about AI and online safety 95
Case study - Using AI to reduce paperwork 96
Questions to guide reflection on practice 97
Resources 98
Glossary 102

About this guide

This Guide has been prepared using resources developed by governments and peak organisations across Australia, namely:

- Australian Human Rights Commission
- Commission for Children and Young People, Victoria
- Department of Education and Training, Victoria
- National Office for Child Safety
- NSW Office of the Children's Guardian
- NSW Department of Education
- The eSafety Commissioner
- ThinkUKnow
- Western Australia Commissioner for Children and Young People

We thank these organisations for their permission to include their information in this publication.

The Australian Children's Education and Care Quality Authority (ACECQA) acknowledges the input of SNAICC, the National Voice for Aboriginal and Torres Strait Islander Children in the preparation of this Guide. In particular, ACECQA acknowledges that this Guide includes information that originally appeared in the SNAICC resource Keeping Our Kids Safe: Cultural Safety and the National Principles for Child Safe Organisations.

Copyright

Acknowledgement of Country

Artist: Chad Briggs
Area: Brisbane
Title of painting: *Lifelines and Bloodlines*

Lifelines and Bloodlines is an original artwork by Aboriginal and Torres Strait Islander artist, Chad Briggs. To learn more about Chad's background and work please visit his website or watch his YouTube video.

The Australian Children's Education and Care Quality Authority (ACECQA) acknowledges all Traditional Owners and Custodians across Australia.

And the Country, Lands, waterways, skies, and seas to which they are connected.

We recognise the contributions, histories, cultures, knowledges, perspectives of education and care of children with Aboriginal and Torres Strait Islander people. We pay our respects to Elders, past and present, and extend that respect to all Aboriginal and Torres Strait Islander people.

Using the NQF Online Safety Guide

This Guide assists approved providers and their staff in collaborating to establish, uphold, and enhance a child-safe culture while reflecting on their roles and responsibilities in this process.

This guide helps approved providers and their staff to:

- work together to create, maintain and improve a child safe culture in online environments
- reflect on their roles and responsibilities in taking these actions.

This guide helps all staff understand and use digital technologies safely with children. It includes:

- approved providers
- nominated supervisors
- service leaders including family day care (FDC) coordinators
- early childhood teachers and educators including FDC educators (collectively referred to as educators)
- support staff including FDC educator assistants
- volunteers
- students on practicum placements
- persons with management or control.

This guide explains how the laws and frameworks listed below work together to create a safe online environment for children:

- Education and Care Services National Law (National Law)
- Education and Care Services National Regulations (National Regulations), including the National Quality Standard
- Approved Learning Frameworks, including Early Years Learning Framework V2.0 (EYLF), My Time Our Place V2.0 (MTOP) and Victorian Early Years Learning and Development Framework (VEYLDF).
- National Principles for Child Safe Organisations (National Principles)
- State or Territory Child Safe Standards.

For example, when teaching children how to use digital technology safely, it's important to follow the approved learning frameworks. These frameworks guide educators in creating a child safe culture, including online safety, and align with the National Principles. Educators should discuss and model the proper use of digital technologies to keep children safe online.

This Guide also helps approved providers and their staff to understand their ethical and legal responsibilities to implement the 10 National Principles and the Child Safe Standards, where applicable, in different states and territories.

Like the National Principles, jurisdictions' mandatory Child Safe Standards provide a framework for making organisations safer for children.

State and Territory Child Safe Standards				
Australian Capital Territory	New South Wales	Queensland	Tasmania	Victoria
	If an organisation is complying with the National Principles, they are deemed to be complying with the NSW Child Safe Standards	Due to come into effect from 1 October 2025 and mandatory from 1 April 2026		11 Child Safe Standards that are legislated for early childhood education and care (ECEC) services

Services must refer to the relevant legislated Child Safe Standards in your jurisdiction and any associated guidance provided by your state or territory, to ensure compliance.

More information about building a child safe culture is available in the NQF Child Safe Culture Guide.

Content warning

Information included in the attached guide contains content about child maltreatment, abuse and harm, including child sexual abuse, and may cause distress for some people.

Some of the content of this guide may be difficult for people with lived experience of child maltreatment, abuse, neglect, racism or who have experienced barriers to expressing their human rights or exclusion from an organisation due to their cultural identity.

If you have concerns about the safety of a child or young person and wish to make a report, details are available on how to report in your state or territory. More information on making a report is also contained in this guide.

If a child is in immediate danger or risk of harm call the police on Triple Zero (000).

If you or someone you know needs support, help is available:

- For support, contact 13YARN on 13 92 76 (at any time, 24/7) or go to 13yarn.org.au.
- Visit Strong Brother Strong Sister at sbssfoundation.org for information and support and mentoring programs for Aboriginal and Torres Strait Islander young people
- For domestic, family, and sexual violence counselling and support, contact
- 1800RESPECT - Phone: 1800 737 732
- For short-term support if you are feeling overwhelmed or having difficulty coping or staying safe, contact Lifeline - Phone: 13 11 14
- For free professional phone and online counselling for anyone affected by suicide living in Australia, contact Suicide Call Back Service - Phone: 1300 659 467
- Sexual Abuse and Redress Support Service - Phone: 1800 211 028
- Bravehearts (support for child sexual abuse survivors) – Phone: 1800 272 831
- For free 24/7, confidential and private counselling service specifically for children and young people aged 5 to 25 years, contact Kids Helpline - Phone: 1800 55 1800
- For information and support for anxiety, depression and suicide prevention for everyone in Australia, contact Beyond Blue - Phone: 1300 224 636
- For information and support for anyone who is affected by complex trauma, contact
- Blue Knot Foundation - Phone: 1300 657 380
- For LGBTIQA+ support and referrals- QLife - Support and Referrals - Phone: 1800 184 527
- For counselling and support for Australian men, contact MensLine Australia - Phone: 1300 789 978
- For advice for men about family violence, contact Men's Referral Service - Phone: 1300 766 491
- Your organisation may also have access to an employee assistance program (EAP) – ask your employer for details.

Chapter 1: Building a Child Safe Culture in the digital environment

Chapter 1: Building a Child Safe Culture in the digital environment

Play

Scan QR code to watch the video or use this link

Introduction

Approved providers and their staff need to know how to create and maintain a child safe culture when using digital technologies. This involves everyone being clear about their roles and responsibilities.

A child safe culture is fostered when everyone is actively involved in creating, maintaining and improving a child safe environment.

It's crucial to keep children safe when they use digital technologies so they can access online learning opportunities safely. Children have the right to quality education and care in a safe environment. Providers and staff should protect, empower and educate children to be safe from online child maltreatment and abuse.

Children's rights

Children are safer when providers and services see them as active citizens. It's important to acknowledge their rights and teach them that they have the right to:

- contribute
- be heard
- be listened to
- be taken seriously in matters related to their online safety.

The United Nations Conventions of the Rights of the Child was originally created in the same year as the internet, so was not able to consider children's access to, or interactions with, the online environment.

However, in 2021, additional information was adopted which sets out children's rights in the digital world. Young people aged 11-17 have written a version for young people to understand, called In Our Own Words.

New technologies

With the constant and emerging development of digital technologies, supporting educators and children to understand the benefits, identify the risks, and take action to address them, is key to keeping children safe online.

While digital technologies offer enormous benefits and potential, children also face a range of risks, including safety, privacy and security risks in using a range of devices, apps, games, and platforms. Exposure to harmful content, cyberbullying and new and emerging risks, including those which may be created or amplified through the use of Artificial Intelligence (AI) tools and technologies, needs careful consideration.

Approved providers and their staff should stay updated on new technologies and manage associated risks. For example, digital toys controlled by apps on other devices such as phones or tablets. Gaps in cybersecurity protection may allow hackers to access wi-fi connections to identify the device location, with the potential to access audio and video functions, which can pose a safety risk to children.

Continuous improvement in online safety practices is essential.

Resources

It is important for online safety practices to be kept up to date and align with the National Quality Framework (NQF), including the National Quality Standard (NQS), the Education and Care Services National Law (National Law), the Education and Care Services National Regulations (National Regulations), and the Approved Learning Frameworks.*

Approved providers and their staff need to know how to create and maintain a child safe culture when using digital technologies and this approach should also reflect the National Principles for Child Safe Organisations and Child Safe Standards, where they exist in your state or territory.

Continuous improvement in online safety practices alongside education and training is essential to ensure all staff and children can engage with digital technologies in safe and meaningful ways, while minimising the opportunities for children and young people to be exposed to harm online.

Approved providers and services should consider the connections between the online safety practices used at the service and these frameworks, to enhance the safety and quality of the online environment for children.

Whilst these are the key principles that mention online safety, it is also important to consider children's digital rights and safety across the spectrum of National Principles. For example, child safety and wellbeing is embedded in organisational leadership, governance and culture - this cannot be achieved without effective safeguarding from online harms.

* Including Early Years Learning Framework V2.0 (EYLF), My Time Our Place V2.0 (MTOP) and Victorian Early Years Learning and Development Framework (VEYLDF).

To access resources related to this chapter, please scan the QR code or click this link.

Scan the QR code to access all the resources from this chapter

Chapter 2: Using digital technologies safely

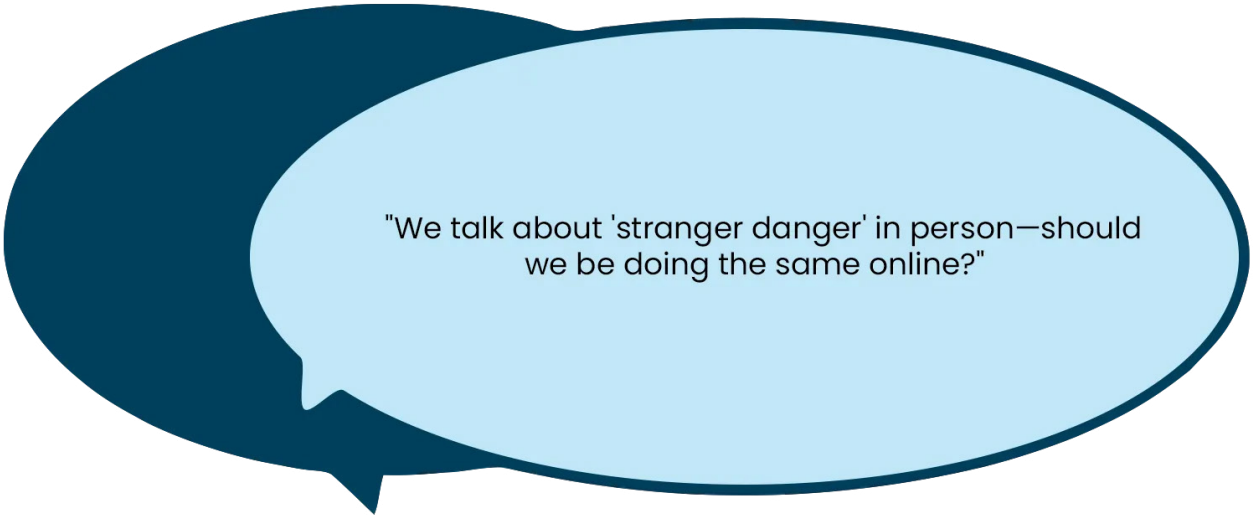
Chapter 2: Using digital technologies safely

Scan QR code to watch the video or use this link

Digital technology and children

Digital technologies offer many benefits to children but also bring safety challenges. For example, people can use online environments to manipulate or isolate a child without oversight from a trusted adult if adequate supervision is not in place.

Children are increasing their use of technology to communicate and maintain social connections, learn and relax, but are still developing their knowledge and understanding about risks in online environments and what to do if they feel unsafe. They may not see differences between online and physical environments, for example, they may see online friends as trustworthy, even when they've never met them in person.



Technology makes it easier for perpetrators of child maltreatment and abuse to reach children, for example by manipulating an image of themselves to seem safe, so it's hard for children to know what's real and what's unsafe.

Safe online practices for educators and children

Setting safe online practices for educators and children helps minimise child maltreatment and abuse. Everyone should be:

- informed about how to stay safe online
- protected from cyber security threats, through the appropriate use of password protections, software and hardware security measures
- ready to act if risks arise
- supported to prevent and respond to online safety incidents.

For support in promoting online safety, services may wish to use trusted eSafety providers, such as those endorsed by the eSafety Commissioner.

What does this look like in practice?

For approved providers and service leaders

- In addition to the NQF Child Safe Culture Guide Policies Checklist, the service's policies and procedures should include the following points about children's safety, online:
  - describe online safety expectations for educators, children and families, including, but not limited to:
    - age and developmentally appropriate use of technology
    - professional use of service-issued devices and online environments by all staff, through the Code of Conduct
  - the safe use of digital technologies, including but not limited to devices (including wearable devices), networks, platforms, apps, and networked toys
  - how staff collect, store, secure, use, disclose and destroy children's personal information, including:
    - the capture, use, storage and disposal of images, videos and voices of children
    - the use of surveillance and monitoring devices
    - images and videos taken of children, including managing the risks of sharing images such as a *geotag inadvertently revealing a child's location

*Geotag - a piece of electronic data that shows where someone or something is and can, for example, be attached to a photograph or comment on social media.

    - obtaining parental or guardian authorisation for the handling of personal information, including taking and retaining images and videos of children
  - undertaking a risk assessment and identify if children's personal devices (including wearable devices) can be used at the service and in what circumstances.
- Help staff identify and reduce online risks, while respecting children's privacy.
- Stay updated on online safety and share information and provide training to educators.

For educators

- Actively supervise and monitor what children do on devices.
- Inform children and their families, in culturally appropriate ways, about how the service uses technology and resources to teach children about online safety.
- Teach children basic digital safety messages in age and developmentally appropriate ways.
- Avoid personal accounts or devices for work-related communication or documentation.
- Be alert to potential signs of exposure to inappropriate material or online harm (e.g. changes in behaviour, secrecy).
- Model respectful and safe online behaviour, including not oversharing, and asking before taking photos.
- Talk with families about how online safety is promoted at the service and how they can support it at home.
- Encourage children to talk to a trusted adult if they see or experience something online that makes them feel uncomfortable.

For everyone

- Regularly check online risks and update safety plans, including when any issues or concerns are identified.
- Undertake regular training on online safety.

Collecting, storing and sharing personal information

Collecting, storing, and sharing children's personal information responsibly is vital for online safety, as it protects their wellbeing and ensures sensitive data is secure from misuse.

A child's personal information includes things like their full name, date of birth, address, contact details, health information, assessments or evaluations and identifying images (including geotagged images that may reveal the child's location).

Sensitive information is personal information that includes information or an opinion about an individual's:

- racial or ethnic origin
- political opinions or associations
- religious or philosophical beliefs
- trade union membership or associations
- sexual orientation or practices
- criminal record
- health or genetic information
- some aspects of biometric information.

Privacy Act

Generally, sensitive information has a higher level of privacy protection than other personal information.

Most NQF providers must comply with the Privacy Act 1988 (Cth) (Privacy Act), in relation to a child's personal information where they:

- have an annual turnover of more than $3 million
- are connected to a larger organisation with an annual turnover of $3 million
- supply a health service and hold health information, which includes in its definition an education and care service, even if this is not the NQF service's primary activity
- are a state or territory agency which is an incorporated company, society or association.

The Privacy Act contains 13 Australian Privacy Principles which govern standards, rights and obligations regarding the collection, management, use, disclosure, security and destruction of personal information.

Protecting children's personal information

It's important to know when children's personal information might be disclosed, and to get permission from their parents or guardians first. For example, before:

- sharing personal information with a third-party service provider, like a social media app or online service to share learning with families
- sharing personal information with inclusion support workers
- displaying a child's medical plan where any visitor to the service can see it.

Children's personal information that may be online can be misused when:

- people try to contact children inappropriately
- photos of children are shared more widely than intended
- photos are taken from social media and websites and used inappropriately or illegally
- parents or family members seek information about a child as part of a domestic dispute.

Following a review of the Privacy Act, a law passed in 2024 requires the Information Commissioner to create a Children's Online Privacy Code within two years. This code will help protect children from online dangers and will apply to online services that children are likely to use.

Approved providers and their services are encouraged to use the National Model Code for Taking Images or Videos of Children while Providing Early Childhood Education and Care (National Model Code). While this code focuses on centre-based services for children under 5, any service can use the National Model Code and Guidelines and apply them to their service context.

What does this look like in practice?

For approved providers

- Require signed parent/guardian consent to collect and share personal information, including images and videos, of their children. Explain how this consent can be withdrawn when circumstances change.
- Tell parents/guardians how and where their child's personal information will be used and stored
- Identify who can gather and access children's personal information, like photos and videos.
- Control how children's personal information is being shared online or through apps.
- Specify how devices can be used for taking and sharing photos and videos of children.
- Follow the National Model Code and Guidelines for Taking Photos or Videos of Children while Providing Early Childhood Education and Care.


Outside School Hours Care and Family Day Care guidance

- If considering allowing school age children to use their own personal device whilst at the service, undertake a risk assessment to assess the risks, including how to manage them taking or not taking images of other children at the service.

For educators

- Always ask children for permission before taking their photo or video and explain how it will be used. Don't force a child to be in a photo if they don't want to.
- Be aware of and implement the intent of parent/guardian's consent around collection and sharing of their child's personal information.
- Teach children to ask for permission before taking a peer's photo or video and explain how it will be used.

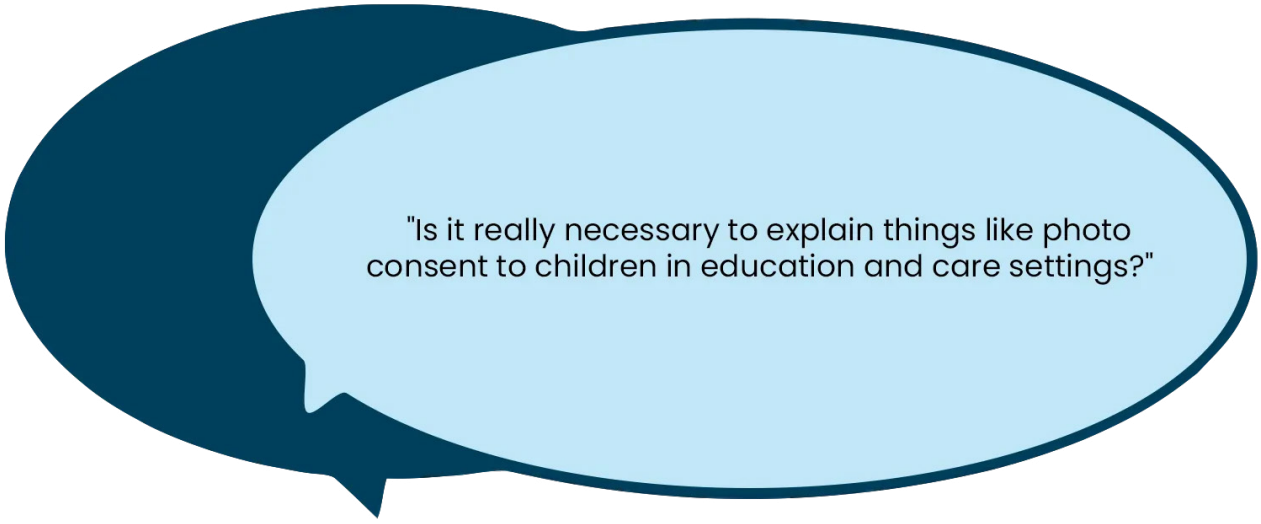
For everyone

- When sharing children's personal information with families, include steps to keep them safe, including:
  - make sure online platforms are password protected and use multifactor authentication
  - understand where and how information is stored and the terms and conditions of the online platforms being used
  - immediately remove access to any online platforms when a child is no longer enrolled.
- Think about whether it's safe to share information with families via social media.
- Don't take photos or videos of children in inappropriate situations, for example, when they are upset, during nappy changes, or in the bathroom.
- Don't put photos or videos online of children who:
  - are/have been subject to child protection, family court or criminal proceeding, or other legal matters where their identity must be protected (following legal instructions).
  - are experiencing family violence and need to stay anonymous
  - have parents who are concerned about their child's digital footprint and request limited or no online photos.
- Talk to children and families about how their personal information is used, including who can access it (including any photos children take of their peers).

Consent

Consent is the informed and freely given agreement to engage in an activity. It involves one person seeking permission from the other before engaging in an activity and the other person 'affirming' or giving their permission for that to happen. Consent must be informed, voluntary, current and specific.

In some situations, the Privacy Act requires organisations to get consent to collect, use, or share personal information. For children and young people, legally, this consent is given by their parents or legal guardians. In addition, it is important to involve children in decisions about their images and provide information about consent in ways they understand as this helps teach online safety practices, builds their independence, and respects their rights. Helping children and families understand that consent can also be withdrawn at any stage is also important.



Useful Tool available

You can access the ***Consent and children's rights*** in the Tools section at the end of this chapter or use this link if you are using the web version of this PDF.

What does this look like in practice?

For approved providers

- Make sure policies respect children's privacy and support their independence.
- Get written consent from families for taking or recording images of their child.
- Explain to families how children's images will be used, accessed, stored and destroyed.
- Explain to families how they can change or revoke this consent.
- When needed, get consent from families for other professionals (like NDIS support workers, inclusion support professionals, students on practicum placements and their supervisors) to take images or videos.
- Explain to families how they can change or revoke this consent.

For service leaders

- Help educators to listen to children's opinions and how to action them.
- Help educators understand why children's participation in decisions about their images is important.

For educators

- Embed a culture of gaining consent from children around taking and sharing their photos and images and provide information about consent in ways they understand.
- If a child's family has given consent:
  - regularly ask the child if they would like their image or video taken
  - explain to a child why their image or video is being taken
  - tell the child who may see their images and videos
  - give the child time to decide whether or not to have their image or video taken.
  - support the child to be able to withdraw their consent at any time.

Consent for children under 5

Useful Tool available

You can access the ***Empowering children under 5 by asking them to give consent for photos or videos*** in the Tools section at the end of this chapter or use this link if you are using the web version of this PDF.

Empowering children under 5 by asking them to give consent for photos or videos	
Concept	**What does this look like in practice**
Give children information and time to decide.	After asking a question, be comfortable with silence whilst the child thinks. Don't try to fill the silence by making a decision for the child or moving on to another learning experience.
Support children to make decisions or change their mind.	Offer children choices, e.g. "Would you like your photo taken to show to Mummy, or would you like to show her how you climb when she picks you up?"
Consider children's views and take children's responses seriously.	Acknowledge children's responses. Repeat back to children what you have heard or seen from their non-verbal cues. Action a child's request. Don't continue trying to convince the child to let you take their photo.
Provide visual cues for non-verbal children, so they can make a choice.	Hold up the camera or tablet for the child to give a non-verbal response. Model options for both a 'yes' and a 'no' non-verbal responses, e.g. shaking head side to side (no) and up and down (yes), making a happy or sad face, using sign language, or using visual picture cards.

Empowering children under 5 by asking them to give consent for photos or videos	
Concept	**What does this look like in practice**
Look for non-verbal cues that the child is agreeing or not agreeing to have their image or video taken.	**Agreeing** Child is looking at camera, making happy sounds and smiles. Child displays a facial expression that is confident and engaged. Child is nodding their head up and down. **Not agreeing** Child is crying or looks upset. Child continues to play and doesn't look up or move if the photo is of a small group of children and the child would need to move to be captured within the image. Child turns their head away or pushes the tablet/camera away. Child avoids eye contact with the educator or moves away. Child is shaking their head side to side.
Provide information to children on the proposed cycle of their image or video taken.	Engage children in ongoing learning experiences to help them understand how, where and why their image or video will be used by the recipient. i.e. using a device (phone, camera or tablet), viewing a photograph digitally or printed, displaying the photo and how the photo is then used by the recipient, i.e. in a journal or a website. Consider the intentional use of words and terms associated with consent and image or video use, i.e. posting images, or public audience, to familiarise children with the proposed use of their image or video.

Case Study - Children bringing their devices to outside school hours care

Children bringing their devices to outside school hours care

An after school care service operates on a school site. Many children walk to school and need their phones for safe travel. They hand in their phones before the school day starts and pick them up before going to after school care.

The service knows that children use digital tools to express themselves and connect with others and so has undertaken a risk assessment to understand how to maintain children's safety.

Limited knowledge of the apps available on each device and how to supervise their use. The service has identified these risks:

Devices may not have proper security settings.

Children may access and share inappropriate content or receive unwanted contact.

Children may take photos of other children without permission.

Inequity in learning and leisure/relaxation opportunities for children who do not have their own devices.

After undertaking the risk assessment and consulting with the school about its policies on the use of phones on school premises outside of school hours, the service decides to allow children to use their own devices, but only in the following circumstances:

- Families must fill out a form (which is regularly updated to keep up to date with evolving technologies) agreeing that the device meets the service's minimum-security requirements and only contains the service's 'allowed' apps.
- Children must hold a completed Be Secure Online certificate from the eSafety Commissioner.
- Children can only use devices in a designated area.
- Children 9 years and older can use their own devices. Children 8 years and younger can only use the service's devices to engage with digital technology.
- Children must not let other children use their device.

The service also has these staff procedures:

- Regularly checking the environment to ensure safe device use and adjust positioning as needed.
- Looking for areas where children might use devices outside of the designated area.
- Communicating with children about what they are using their devices for, their favourite apps and why they enjoy playing with them.
- Communicating with children about how to use their devices safely and what security settings are enabled.

Questions to guide reflection on practice

These questions help you think about what you're doing well and what you can improve.

Safe online practices within education and care services:

- How does the service identify, assess and manage risks online?
- How do educators ask children about their views on online safety in a developmentally appropriate way?
- How do service leaders teach staff and families about online safety?
- How do educators help children learn to stay safe online?
- How do educators teach children about consent and ask them about whether to have their image taken or recorded?
- How does the service talk to families about when and how their child's images and videos will be taken, accessed, stored, used and destroyed?
- How does the service gain permission from families to take and share images and videos for specific purposes?
- How does the service support a child who may need to use personal devices, for example for a medical reason or, for a non-verbal child, as a communication tool within the service?

Outside School Hours Care and Family Day Care guidance

- How does the service manage personal devices that school-age children may have access to, if it allows personal devices in its policy and procedures?

Useful Tool available

You can access the ***Questions to guide reflection on practice*** in the Tools section at the end of this chapter or use this link if you are using the web version of this PDF.

Resources

To access resources related to this chapter, please scan the QR code or click this link.

There are several tools available for this chapter. You can access these in the Tools section on the next page or select each link below if you are using the web version of this PDF.

Questions to guide reflection on practice

Empowering children under 5 by asking them to give consent for photos or videos

Consent and children's rights

NQF Online Safety Guide self and risk assessment tool

Scan the QR code to access all the resources from this chapter

Chapter 2: Resource tools

To access tools related to this chapter, please scan the QR code or click this link.

Scan QR code to access Chapter 2 tools

Questions to guide reflection on practice

Australian Children's Education & Care Quality Authority

Using digital technologies safely

These questions help you think about what you're doing well and what you can improve.

- How does the service identify, assess and manage risks online?
- How do educators ask children about their views on online safety in a developmentally appropriate way?
- How do service leaders teach staff and families about online safety?
- How do educators help children learn to stay safe online?
- How do educators teach children about consent and ask them about whether to have their image taken or recorded?
- How does the service talk to families about when and how their child's images and videos will be taken, accessed, stored, used and destroyed?
- How does the service gain permission from families to take and share images and videos for specific purposes?
- How does the service support a child who may need to use personal devices, for example for a medical reason or, for a non-verbal child, as a communication tool within the service?
- How does the service manage personal devices that school age children may have access to, if it allows personal devices in its policy and procedures?

Empowering children under 5 by asking them to give consent for photos or videos

Australian Children's Education & Care Quality Authority

Using digital technologies safely

Concept	What does this look like in practice
Give children information and time to decide	After asking a question, be comfortable with silence whilst the child thinks. Don't try to fill the silence by making a decision for the child or moving on to another learning experience.
Support children to make decisions or change their mind	Offer children choices, such as "Would you like your photo taken to show to Mummy, or would you like to show her how you climb when she picks you up?"
Consider children's views and take children's responses seriously	Acknowledge children's responses. Repeat back to children what you heard or saw from their non-verbal cues. Action a child's request. Don't continue trying to convince the child to let you take their photo.
Provide visual cues for non-verbal children, so they can make a choice	Hold up the camera or tablet for the child to give a non-verbal response. Model options for both a 'yes' and a 'no' non-verbal responses, e.g. shaking head side to side (no) and up and down (yes), making a happy or sad face, using sign language, or using visual picture cards.

Empowering children under 5 by asking them to give consent for photos or videos

Look for non-verbal cues that the child is agreeing or not agreeing to have their image or video taken	**Agreeing** Child is looking at camera, making happy sounds and smiles. Child displays a facial expression that is confident and engaged. Child is nodding their head up and down. **Not agreeing** Child is crying or looks upset. Child continues to play and doesn't look up or move if the photo is of a small group of children and the child would need to move to be captured within the image. Child turns their head away or pushes the tablet/ camera away. Child avoids eye contact with the educator or moves away. Child is shaking their head side to side.
Provide information to children on the proposed cycle of their image or video taken	Engage children in ongoing learning experiences to help them understand how, where and why their image or video will be used by the recipient, that is using a device (phone, camera or tablet), viewing a photograph digitally or printed, displaying the photo and how the photo is then used by the recipient, that is in a journal or a website. Consider the intentional use of words and terms associated with consent and image or video use, that is posting images, or public audience, to familiarise children with the proposed use of their image or video.

Using digital technologies safely

> *"From birth to teenage years, children have had numerous photos taken of them and shared, often without their knowledge, let alone consent. It is no wonder they arrive in the teen years with little understanding of their rights and responsibilities. As early childhood educators you can be powerful agents of change in incorporating consent for image taking and sharing into your daily practice and laying the foundations for children's future respectful social media use."*
>
> **Deanne Carson, Body Safety Australia**

Educators should always get families' consent to take and share images or videos of their child online. It is also important to help families understand how the service supports children's right to privacy online. Educators should also be aware of any families who do not wish to have their children's images taken, and have measures in place to make sure their images are not taken.

Some families may want many updates, but it's important to respect the child's rights and involve them in decisions about taking and sharing images and provide information about consent in ways they understand. For example, don't force a child to be in a photo if they don't want to. This teaches good practices and respectful behaviour.

Modelling consent and respectful data sharing practices from an early age are the first steps in supporting children to be empowered and confident when making their own choices to share their images or videos online. For example, the Young Children in Digital Society's article Developing a culture of consent talks about ways to gain consent with 3 to 5 year olds.

Teach children to ask for permission from their peers before taking photos or videos of them. The Royal Commission into Institutional Responses to Child Sexual Abuse highlighted the importance of teaching children to say 'no' to unwanted photos or videos. Ignoring a child's 'no' can make them feel powerless and more vulnerable to abuse. As noted in Principle 2 of the National Principles, children should be informed about their rights, participate in decisions affecting them and be taken seriously.

Educators should teach children from a young age that they have ownership and autonomy over their own bodies and can decide if they want their image or video taken. This helps them have a say in what happens to their body. An educator responding to a child may be the first adult to truly listen to the child, which shows them that their voice is very important.

Chapter 3: Safe online practices within education and care services

Chapter 3: Safe online practices within education and care services

Scan QR code to watch the video or use this link

Safe online practices

Approved providers, service leaders and educators should know how to keep children safe online. They should help children learn to be safe online too. This means actively supervising children when they use devices.

Everyone needs to know how to identify, report, and respond to incidents or allegations of online child maltreatment and abuse. They should also know how to guide children's behaviour appropriately and maintain their dignity and rights.

There are both NQF and state/territory specific requirements for reporting harm to a child, including online harm, which must be followed. Knowing the appropriate reporting and referral pathways is critical. Incidents involving children who are exhibiting concerning and/or harmful sexualised behaviours are potential indicators that they have been exposed to inappropriate content online, or they are being subjected to manipulative behaviours.

Besides mandatory reporting to authorities, online child sexual exploitation, like grooming (being subjected to manipulative behaviours) and extortion, can be reported to the Australian Centre to Counter Child Exploitation (ACCCE). The ACCCE, led by the Australian Federal Police, works with various agencies to prevent online child exploitation.

Child sexual exploitation and abuse material online should also be reported to the eSafety Commissioner. The Commissioner can take action to remove this content and other forms of harmful content.

Services should keep improving their online safety practices, stay updated on new technology and its risks, and provide training to help educators keep children safe.

Managing screen time

Sedentary screen time during early childhood may have long-term impacts on a child's development. It's important to review current guidance and speak to families about the amount and nature of screen time their children have at home and at the service.

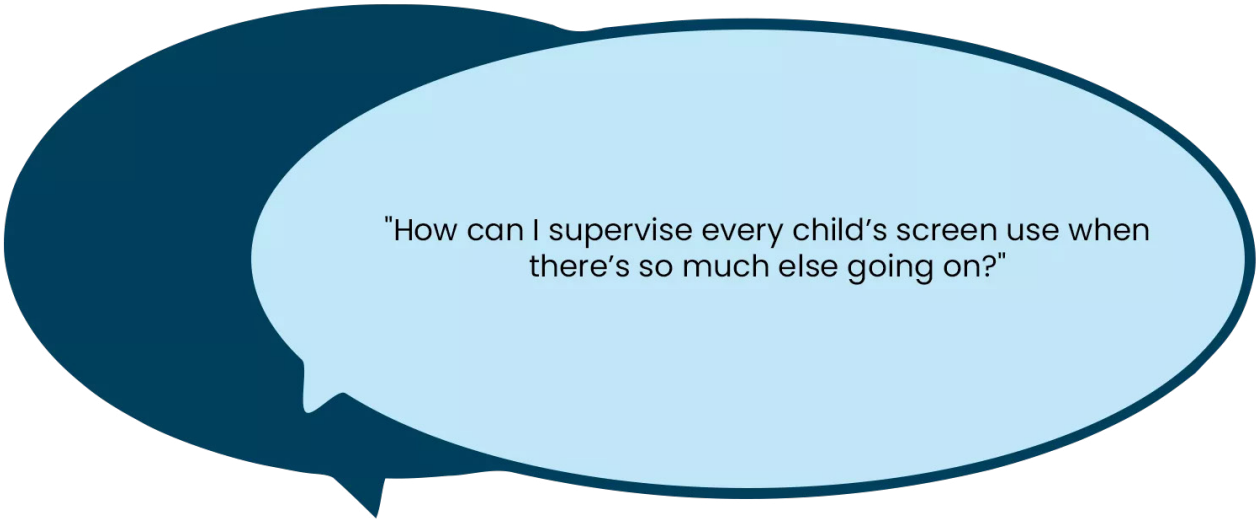
The Australian Government has published physical activity guidelines by age which set out recommendations for the maximum amount of screen time children in different age groups should have per day.

The eSafety Commissioner and Digital Child have also published useful screen time advice.

Professional development for educators

Ongoing training helps educators keep up to date with risks and ways to keep children safe, online.

When staff are well-informed, trained, and supported, they are much better placed to implement the service's child safe values. Approved providers and service leaders should invest in building staff skills and confidence to create a child safe culture.



Training should be designed to meet the needs of different staff and services. It should also be strengths-based and trauma-informed, meaning it takes into account the emotional impact of the training content. Child safety training can be confronting and can trigger emotions. It's important to have support systems in place, like employee assistance programs, to help staff cope with these feelings.

What does this look like in practice?

For approved providers and service leaders

- Keep up with the latest online child safety information and share it with educators.
- Use the NQF Child Safe Culture Guide and NQF Online Safety Guides, including questions to guide reflection on practice to inform training and discussions with staff.
- Undertake research on the content of apps, platforms, websites and games proposed to be used or currently being used by children and educators at the service, on service-issued devices.
- Know what safety issues to look out for to support educators to safely use devices within their educational program with children. Provide time for educators to undertake this research, if it is part of their role.

For educators

- Take an interest in what children usually do online, including which apps, websites and games they use.
- Help children use the internet safely at the service, and teach them how to stay safe online.
- Teach children about how to use apps, websites and games safely.
- When researching new apps, games, platforms or websites, know what safety issues to look out for and ask for permission from service leaders before downloading anything onto service-issued devices.

For everyone

- Learn to identify and respond to online safety risks, like grooming (being subjected to manipulative behaviours), cyberbullying, excessive use of devices and screen time, and inappropriate images.

Online supervision

Supervising children when they use electronic devices is very important to keep them safe from unwanted contact and online grooming, including being subjected to manipulative behaviours online. Even if an adult is in the same room, they need to actively supervise the child's online activities.

Higher-risk behaviours for children online can include:

- uploading private information or images
- engaging with inappropriate content (both inadvertently and purposefully)
- making in-app purchases
- interacting with unsafe individuals.

Supervision helps prevent incidents and enables educators to step in if something goes wrong. It also creates a supportive environment where children feel comfortable asking for help without fear of punishment.

Additional supervision considerations may exist in OSHC and FDC environments where:

- school aged children may be more likely to bring their own device to the service, with agreement between services and families
- it may be more difficult to define an appropriate space for children to use a device to ensure adequate supervision.

What does this look like in practice?

For service leaders

- Make sure the service's supervision plan includes the online environment.
- Monitor the use of service devices by educators to ensure they are used appropriately.
- Support educators to report when other staff use devices inappropriately.

Outside School Hours Care and Family Day Care guidance

- If considering allowing children to use their own personal device whilst at the service, undertake a risk assessment to assess the risks, including how to manage which games, websites, app and platforms they may access and gaining written confirmation from families that they are age appropriate, safe and have parent controls activated.

For educators

- Be in the same play space and actively supervise children using devices.
- Communicate regularly with children about what they enjoy doing online and how to stay safe online.
- Use speakers for online games or limit communication to text-based chat to monitor conversations.
- Check the games and sites children use, ensure age restrictions are active, and prevent children from uploading images.

For everyone

Block, report and remove users from online platforms to prevent inappropriate contact with children. See the eSafety Commissioner's information on how to stay safe online for more information.

Myths about online child abuse

Online perpetrators often use myths about child maltreatment and abuse to engage in illegal activities with children. Abusers may use these myths to hide their actions or threaten children to keep the abuse secret.

Approved providers and service leaders can help all educators, staff and volunteers in the service understand the difference between facts and myths about child sexual abuse through discussions and training. This helps keep children safe.

Common myths about online child sexual abuse

These myths have been sourced from ThinkUKnow and are not true.

- Online child sex offenders are always older males.
- Online child sex offenders are always 'online strangers'.
- High school aged children are more at risk of online child sexual exploitation.
- Only females are at risk of online child sexual exploitation.
- Online child sexual exploitation doesn't happen in Australia.
- Parental controls and privacy settings are enough to keep children and young people safe online.
- Children's games (on gaming consoles or apps) are always safer.
- Children and young people in smaller or more remote towns are safer from online child sex offenders.
- Online grooming is a long process so there would be time for educators or families to notice the signs.

Common facts about online child sexual abuse

These facts have been sourced from ThinkUKnow and can be shared with educators and volunteers to dispel any misconceptions.

- Online child sex offenders can be any age, gender and from any background.
- Online child sex offenders can be known to the victim. It's sometimes assumed that children are targeted by 'online strangers'. This isn't always the case.
- Anyone under the age of 18 can be a victim of online child sexual exploitation.
- Australian law enforcement continues to disrupt online child sex offender networks in Australia.
- Multiple strategies are recommended for online child safety.
- Any site, game, app or platform with an internet connection can be used by online child sex offenders.
- Online child sexual exploitation is a borderless crime.
- It can take only minutes for online child sex offenders to gain trust and form 'friendships' with potential victims.

For further information about myths and facts about child sexual abuse in the NQF Child Safe Culture Guide.

Responding to disclosures of online child abuse

All staff need to create an environment where children feel safe and supported to talk about online maltreatment and abuse.

Children see the internet and social media as a big part of their lives, but they might not see online risks the same way adults do. They might not know what to do if they feel unsafe or are being targeted. It's important for children to know they can talk to a trusted educator about things that happen online, or if they have questions, no matter what happened.

Educators should be open and non-judgmental if a child asks for help. A negative reaction might stop a child from seeking help in the future.

What does this look like in practice?

For everyone

- Listen and respond to all safety concerns without using leading questions.
- Undertake all reporting requirements necessary in your state/territory.
- Tailor responses to the child's needs and circumstances.
- Identify local support agencies for help that is age and developmentally appropriate for children and families.
- Listen without judging and give full attention to create a safe space for the child to share.
- Reassure the child that you believe them and praise their bravery for speaking up.

- Ask the child what they need to feel safe.
- Explain the next steps and let them know you might need to share some information to keep them safe, but you'll keep the rest private.
- Remain calm and manage any personal emotions that arise, such as shock or anger.
- Write down what the child told you soon after the conversation. Make sure all adult witnesses also write down details.
- Only ask for more details if the child wants to share more. If they give enough information, don't keep asking questions.
- Sensitively interrupt the child if they begin to disclose in front of other children and move the conversation to a safe and private space.
- Seek support and debrief after the incident has been managed, for your own wellbeing.
- Collect as much evidence as possible, like screenshots and usernames, and be aware of record-keeping rules under the NQF and child protection legislation. Do not take screenshots or photos of illegal and restricted content.

Reporting online child abuse

Approved providers and all staff should know their reporting obligations, including those to regulatory authorities, child protection agencies, and reportable conduct schemes.

Besides mandatory reporting to authorities, online child sexual exploitation, like online grooming and extortion, can be reported to the Australian Centre to Counter Child Exploitation (ACCCE). The ACCCE, led by the Australian Federal Police, works with various agencies to prevent online child exploitation.

Child sexual abuse material online should also be reported to the eSafety Commissioner. The Commissioner can take action to remove the content and other forms of harmful content.

However, don't save or share nude or sexual images or videos of anyone under 18 or any other illegal or restricted content. See the eSafety How to collect evidence page for more information.

Case study - Teaching children to be safe online

Teaching children to be safe online

Elsa is a room leader at a long day care service. She knows a lot about online safety and helped create the service's safety practices. To keep improving, she looks for new information and checks the eSafety Commissioner's Early Years program for educators.

She finds areas to improve, especially in using play to teach children about digital safety. She visits the PlayingITSafe website and reviews play-based activities to get ideas to teach children safe online habits.

As many children talk about making video calls with their family, Elsa asks educators to try the "Who can help?" activity. This activity helps children decide who they should talk to and who they shouldn't, teaching them to identify trusted adults both offline and online.

Educators report that the activity helped children understand the difference between "faces they know," "faces they don't know," and "faces they can trust," and that they should only communicate with trusted adults online.

Questions to guide reflection on practice

These questions help you think about what you're doing well and what you can improve.

- How do services identify, assess and manage online risks?
- How do all staff know who is responsible for setting up devices and maintaining their safety and how to get help?
- How are new apps and games checked for age and developmentally appropriate content before they are used?
- How do educators check with families about parental controls and age restrictions if children's personal devices are used at the service?
- How are all staff made aware of the additional steps to report online child maltreatment and abuse to the eSafety Commissioner and the Australian Centre to Counter Child Exploitation, and who to ask for help?
- Are staff likely to believe, listen to and/or take action to help children (including babies) who have experienced online harm?
- What training do educators undertake and do they feel confident in responding to a child's online safety concerns?
- How are short-term staff, volunteers, and students inducted in online safety at the service?

Useful Tool available

You can access the ***Questions to guide reflection on practice*** in the Tools section at the end of this chapter or use this link if you are using the web version of this PDF.

Resources

To access resources related to this chapter, please scan the QR code or click this link.

There are several tools available for this chapter. You can access these in the Tools section on the next page or select each link below if you are using the web version of this PDF.

Questions to guide reflection on practice

Scan the QR code to access all the resources from this chapter

Chapter 3: Resource tools

To access tools related to this chapter, please scan the QR code or click this link.

Scan QR code to access Chapter 3 tools

Questions to guide reflection on practice

Australian Children's Education & Care Quality Authority

Safe online practices within education and care services

These questions help you think about what you're doing well and what you can improve.

- How do services identify, assess and manage online risks?
- How do all staff know who is responsible for setting up devices and maintaining their safety and how to get help?
- How are new apps and games checked for age-appropriate content before they are used?
- How do educators check with families about parental controls and age restrictions if children's personal devices are used at the service?
- How are all staff made aware of the additional steps to report online child maltreatment and abuse to the eSafety Commissioner and the Australian Centre to Counter Child Exploitation, and who to ask for help?
- Are staff likely to believe, listen to and/or take action to help children (including babies) who have experienced online harm?
- What training do educators undertake and do they feel confident in responding to a child's online safety concerns?
- How are short-term staff, volunteers, and students inducted in online safety at the service?

Chapter 4: Embedding online safety

Chapter 4: Embedding online safety

Scan QR code to watch the video or use this link

Online safety practices

Creating a safe environment for children includes identifying opportunities and risks within the service's online environments and using key practices to support them. Teaching children to be safe online is an important part of this.

References to digital technology have been strengthened in the updated national approved learning frameworks, but to support each child's learning, educators need to use these technologies safely. Digital devices can also help non-verbal children and those whose first language isn't English, supporting their rights and inclusion in the service's program.

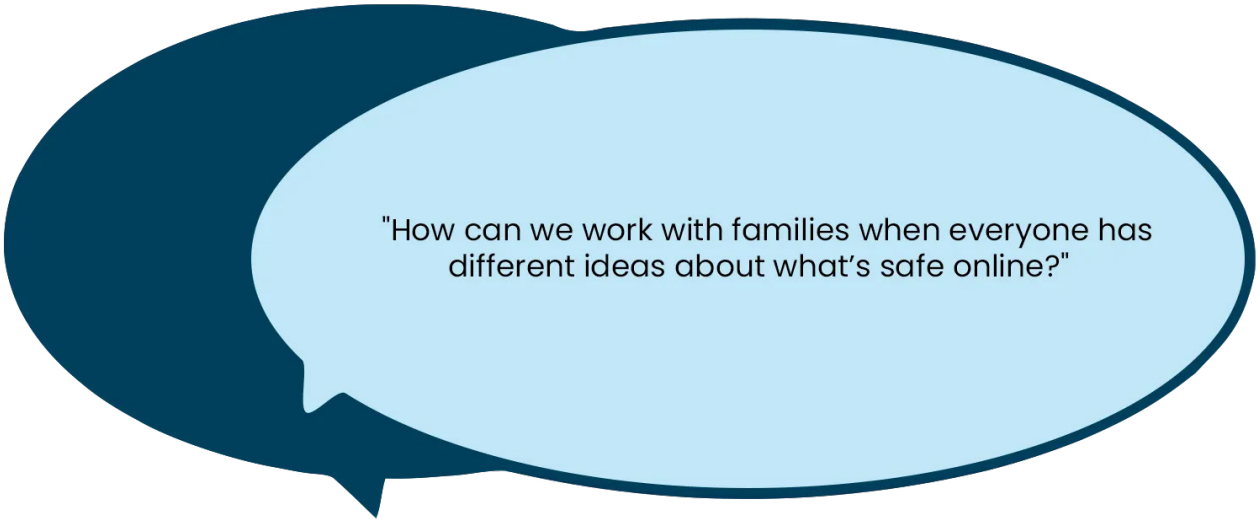
Early Childhood Australia's Statement on young children and digital technologies is a useful resource with research, guiding principles, and practical advice for educators on using digital technologies. The resource looks at four known areas of importance in early childhood education:

1. Relationships
2. Health and wellbeing
3. Citizenship
4. Play and pedagogy.

How to implement online safety

Approved providers and their staff should work with families to build a shared understanding of safe online environments for children.

It is important to help children to understand how to use technology and the internet safely. Ongoing professional development around these topics is important to keep children safe because technology changes quickly.



What does this look like in practice?

For approved providers and service leaders

- Discuss what makes children feel safe, especially those who are experiencing vulnerability or disadvantage.
- Help children identify trusted adults they can ask for help if they feel worried, confused, or unsafe online or before doing anything new on a device.
- Ask children what they have learned on their device or platform and why they enjoy using it.
- Use the eSafety Commissioner's play-based resources based on the Mighty Heroes bush characters (animations and activities) to explore digital concepts like protecting personal information, respectful relationships and being a good digital citizen.
- Discuss online behaviour, respectful relationships, and consent with children in ways that are graduated and age and developmentally appropriate in recognition of the evolving capacity of the child.

- Communicate with children and families about online risks (in an age and developmentally appropriate way), using conversation starters from the eSafety Commissioner: Talking about child sexual abuse online with 0- to 12-year-olds. Inform families about how the service communicates with children about these issues, ahead of time, to build a shared understanding of child safety.
- Create child-friendly guides or agreements for acceptable use of service-issued devices, for example the eSafety online safety agreement or PlayingITSafe Pre-school technology agreement.

Aboriginal and Torres Strait Islander cultural safety online

Understanding, respecting and including Aboriginal and Torres Strait Islander cultural perspectives is crucial for creating a culturally safe environment, both in person and online.

eSafety Commissioner research has identified that Aboriginal and Torres Strait Islander children are almost three times more likely than the national average to have had offensive things said to them because of their race, ethnicity, gender, nationality, sexual orientation, religion, age or disability whilst online. Negative online experiences like this can have deep impacts on children's mental health and reduced engagement with learning.

Parents and caregivers of Aboriginal and Torres Strait Islander children are more likely than parents and caregivers of Australian children overall to be aware of their child's experiences of online hate and exposure to potentially harmful content online material, instruct their child on ways to use the internet safely, regularly monitor their child's online activities and use parental control tools such as blocking software.

What does this look like in practice?

For approved providers and service leaders

- Consult with families, Aboriginal and Torres Strait Islander Elders and staff, and local community knowledge holders about culturally appropriate content and priorities for children's online learning.
- Include photos and information about Aboriginal and Torres Strait Islander community events and local Aboriginal and Torres Strait Islander artworks in the service's online environments.
- Include an Acknowledgement of Country and Aboriginal and Torres Strait Islander flags on the service's website.
- Use culturally appropriate content warnings, such as a warning that there may be images, voices and names of deceased people on the service's website.

For educators

- Incorporate Aboriginal and Tores Straight Islander cultural perspectives and foster a strong sense of identity and belonging within children's online and digital learning experiences.
- Implement the principles and practices of the approved learning frameworks to embed culturally safe environments, respect for diversity, and inclusive practices for children's online learning.

For everyone

- Use culturally safe online games, apps, songs, music, and videos that include Aboriginal and Torres Strait Islander perspectives for all children.
- Engage Aboriginal and Torres Strait Islander families to understand their concerns or ideas about digital media use.
- Make sure Aboriginal and Torres Strait Islander children and families feel safe and heard, respect their cultures and identities, and actively involve them in developing and maintaining a safe online environment.

Preventing online safety risks

All online environments can pose a risk to children if not monitored and managed appropriately. It's important for educators and staff to be aware of these risks and how to reduce them. Managing these risks can help prevent child maltreatment, abuse and harm.

Responsible use of digital platforms

While websites, platforms, apps, and games can be misused, they also offer many positives like growing knowledge, fostering creativity, promoting problem-solving, enabling socialisation, and providing relaxation or entertainment.

Supporting children in safe online navigation

When educators work with children to develop their skills to navigate these issues safely, children can benefit from the positive aspects of being online.

Unwanted or unsafe contact

Unsafe contact is when someone who connects with a person online wants to harm them. Unwanted contact is any type of online communication that makes a person feel uncomfortable, unsafe or harassed.

Online hate

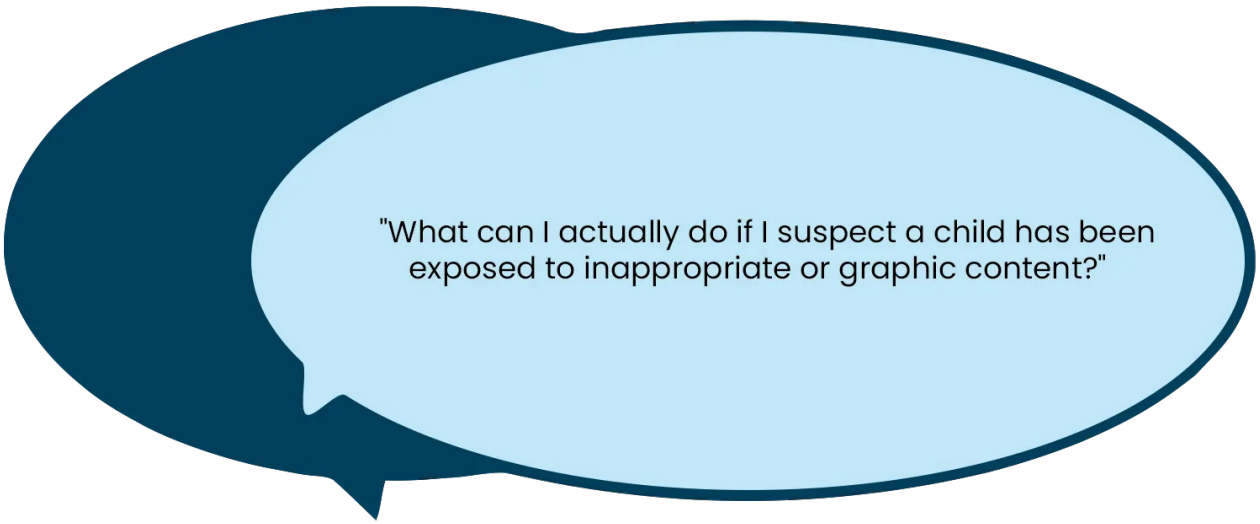
Online hate is hateful posts about a person or group based on their race, religion, ethnicity, sexual orientation, disability or gender.

Research from the eSafety Commissioner has identified that children and young people from certain groups, such as Aboriginal and Torres Strait Islander children and young people, LGBTIQA+ young people, and children and young people with disability, are more at risk of negative online experiences such as online hate.

Hateful comments about a cultural or religious group are unfortunately very common for children and young people to see online. In some cases, this may include radical/extremist content.

Inappropriate content

Inappropriate content may be an image, video or written words that can be upsetting, disturbing or offensive. It may include sexually explicit material, false or misleading information, violence extremism or terrorism, hateful or offensive material.



Encounters with online pornography are common, whether it is intentionally sought out or not. For children and young people, accidentally encountering pornographic material can be confusing, distressing and, at worst, harmful. In addition, exposure to graphic, violent or misleading messages about sexual practices and gender stereotypes can lead to children developing misconceptions and damaging ideas about sex and intimate relationships.

What does this look like in practice?

For approved providers and service leaders

- Ensure that all children and families, including Aboriginal and Torres Strait Islander children and families, children with additional needs, LGBTIQA+ children, and children from diverse backgrounds know their cultures and identities are respected.
- Ensure that any apps, online games, smart toys and technology toys used at the service are appropriate/designed for the children's developmental stage and age group.

For educators

- Teach children they have the right to feel safe and say 'no' to anything that makes them feel unsure, uncomfortable, or unsafe.
- Encourage children to think about the consequences of their actions online, including the harms of cyberbullying and sharing inappropriate images, for example by following the Be an eSafe kid framework.
- Teach children to consider others' feelings when sharing content, even if it's meant as a joke.

- Support children to report online cyberbullying to the platform and the eSafety Commissioner.
- Supervise children while they're on a connected device and use technology settings and parental controls to manage what children can access on service-issued devices.
- Have age and developmentally appropriate conversations with children around harmful or illegal content, including sexual content, so children know to seek help if needed. Inform families about how the service communicates with children about these issues, ahead of time, to build a shared understanding of child safety.
- Communicate with children about why they might share content and if they really know who they are talking to online.
- Explain that not everyone online is who they say they are and that children should not give out personal information such as their name, birthdate, school and address, online or that of others.

Case Study - Discussing online friends with children

Discussing online friends with children

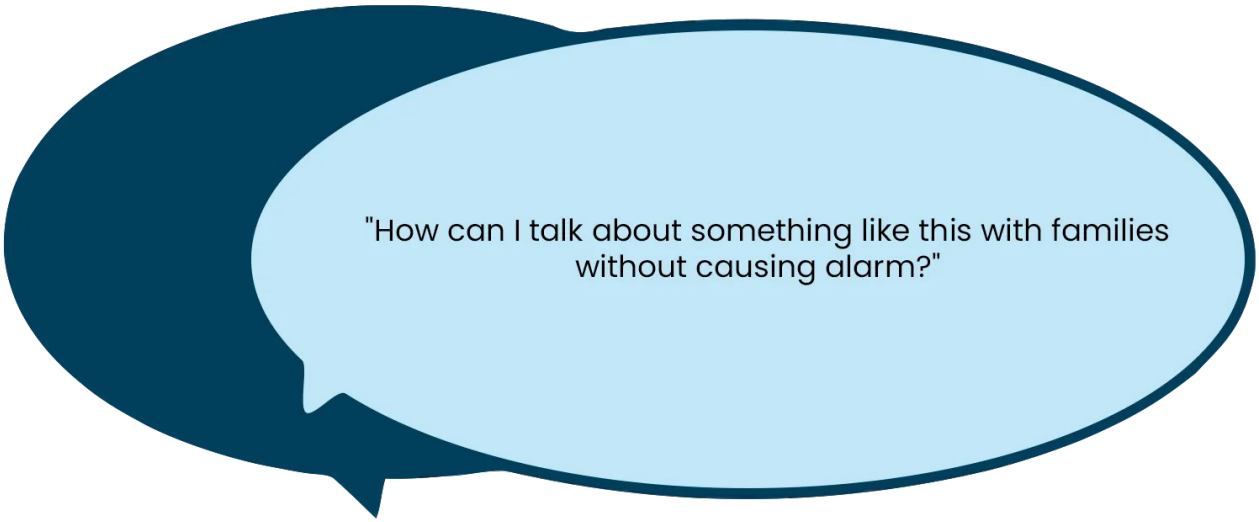
Kiran, an educator at OSHC, talks to some of the older children about two of the apps they use. He tries to teach them not to accept friend requests from unknown people, but they don't understand why it's a problem. Kiran discusses this with Sylvia, the service coordinator.

Sylvia explains that telling children not to talk to people online won't work because they see "online friends" as real friends. Children and young people may not see online friends as unsafe people, especially if they've been groomed through being subjected to manipulative behaviours online. It's important for children to know that not everyone online is who they say they are. There's a difference between people they know in real life and those they've only met online. Proving someone's identity online can be hard because they might only share what they want others to know.

Kiran uses this information to change his approach. He learns more about the two apps the children use, to discuss online friends more specifically. He encourages the children to think carefully before accepting new friend requests and to consider if they really know who they're talking to online.

Self-generated sexual content or personal image sharing

Self-generated sexual content includes photos or videos of a sexual nature taken by a person of themselves. This can be called personal image sharing, sexting, sending a selfie, or sending a pic. If the person in the image is under 18, it is considered child sexual exploitation or abuse material, which is illegal to produce, store or share.



There are many reasons why children or young people might send these images, like exploring their feelings, feeling good about themselves, thinking everyone is doing it, or peer pressure. Sometimes, they might take these images without knowing it's risky or inappropriate. In more serious cases, they might be forced to take these images by someone they trust or know. The eSafety Commissioner has written a resource to help discuss child sexual abuse online with 0-to-12 year olds.

Recently, more children aged 8-12 have been tricked into taking inappropriate pictures of their younger siblings and sharing them online. This often happens as a dare or at the request of an online "friend."

What does this look like in practice?

For educators and service leaders

- Teach children to always ask a trusted adult before talking to someone new online or adding a new friend.
- Encourage children to check with a trusted adult if someone they don't know contacts them or asks them to do something online. This helps involve adults in the conversation.
- Share safety messages with children and families, including being careful about who children talk to online or add on social networks.
- Explain that once children send an image or video, it can be hard to know who else might see it or where it could end up.
- Teach young children what personal information is and why they should be very careful about sharing this information online. This helps them understand the importance of keeping intimate images private.
- Encourage children to identify and question suspicious online interactions.
- Teach children why it's important to set all accounts to private, not share passwords or usernames, and how to block and report people online.
- Encourage children to tell educators and their families which apps, games, and websites they use or want to use.

For Outside School Hours Care and Family Day Care

- Teach children about the risks of sending self-generated sexual content and what to do if pressured to do so, like saying no, changing the subject, expressing discomfort, and telling a trusted adult.

- Understand that schools and families may have different approaches, so it's important to work with them to ensure children hear consistent messages.

Image-based abuse and sexual extortion

Image-based abuse happens when intimate, nude, or sexual images (including images of children) are shared without permission, or someone threatens to share them. This includes photos or videos created or altered using AI technology, such as generative AI tools.

Sexual extortion, or 'sextortion', is a serious form of image-based abuse. Where this involves a child, it can involve online blackmail, where a perpetrator coerces, manipulates, or grooms a child or young person into generating intimate images or videos and then threatens to reveal these if the child or young person does not give in to their demands.

In these cases, perpetrators can first be nice and charming, but then become manipulative and cruel, and make a child or young person feel there is no way out of the situation, including using blackmailing and threatening to share explicit content online.

In exchange for not sharing the content, perpetrators often ask for more explicit photos, videos, or money. Fear and manipulation can make victims feel like there's no way out. Children and young people might feel they've done something wrong, and fear being punished by families or law enforcement if their involvement is discovered.

What does this look like in practice?

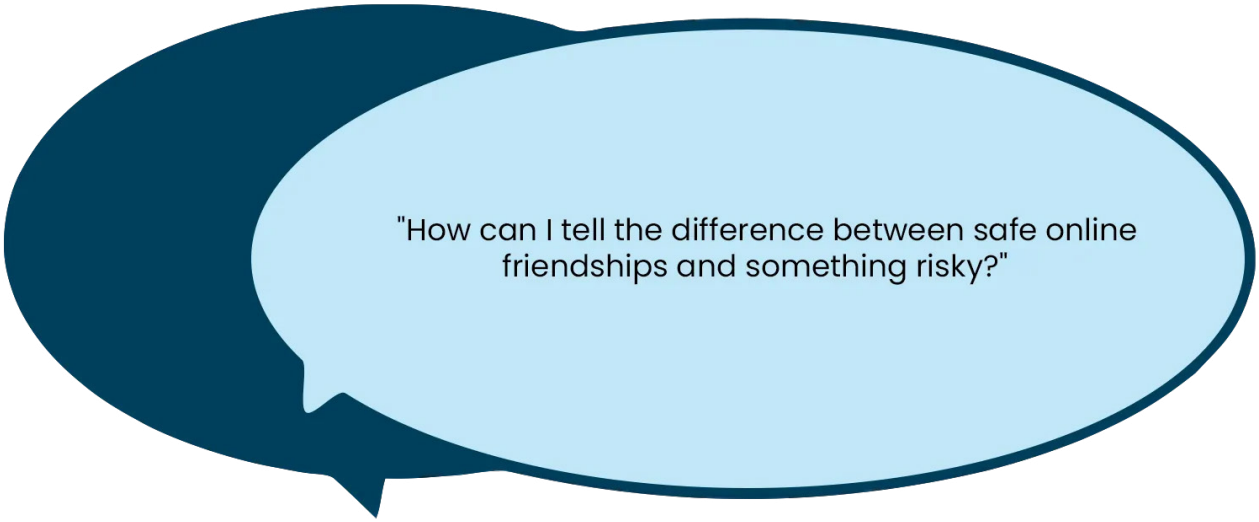
For educators

- Teach children about the importance of strong privacy settings and not accepting unknown friend or follower requests.
- Always ask children if they want their photo or video taken or shared.
- Teach children from a young age that not everyone online is who they say they are.
- Teach children that if they receive a sexual image, they should tell a trusted adult, delete it and not share or save it.
- Make sure children only use apps and games that are age and developmentally appropriate.

Online grooming

The National Office for Child Safety defines grooming as intentional behaviours that manipulate and control a child, as well as their family, kin and carers, other support networks, or organisations in order to perpetrate child sexual abuse.

Grooming, through manipulative behaviours, is when an adult prepares a child for sexual abuse. Perpetrators may sexually abuse children by using manipulative behaviours or strategies as part of a process commonly involving prosocial behaviours violating personal boundaries, to obtain sexual contact with children in the periods prior to, during and following sexual contact. Grooming can happen in person or online. It is a sexual offence and must be reported.



Online grooming is when someone makes contact with a child online to facilitate child sexual abuse. Police investigate suspected online grooming if a report of unwanted or inappropriate contact has been made.

Perpetrators use manipulative behaviours and often pretend to be another child and direct the child to chat on platforms with image-sharing capabilities to get sexual photos or videos, or to arrange meetings. Online grooming can be a step before asking to meet in person.

What does this look like in practice?

For educators

- Have open and honest discussions with families and children about technology, how to use online environments, the risks involved, and how to learn about them.
- Be aware of the common behaviours to look out for with online grooming.
- Know how to prevent grooming.
- Know how to report online child maltreatment and abuse to the eSafety Commissioner and federal police, including grooming.

For more information see Grooming behaviours used for obtaining sexual contact in the NQF Child Safe Culture Guide.

Additional reporting for online maltreatment and abuse

Besides mandatory reporting to authorities, online child sexual exploitation, like grooming and extortion, can be reported to the Australian Centre to Counter Child Exploitation (ACCCE). The ACCCE, led by the Australian Federal Police, works with various agencies to prevent online child exploitation.

Child sexual abuse material online should also be reported to the eSafety Commissioner. The Commissioner can take action to remove the content and other forms of harmful content.

However, don't save or share nude or sexual images or videos of anyone under 18 or any other illegal or restricted content. See the eSafety Commissioner's How to collect evidence page for more information.

Useful Tool available

You can access the ***Embedding online safety and common behaviour to look out for with online grooming*** in the Tools section at the end of this chapter or use this link if you are using the web version of this PDF.

Case Study - Discussing online games with children and listening to children's voices

Discussing online games with children and listening to children's voices

At OSHC, Jacob's educator, Tegan, asks him about his weekend. Jacob mentions playing Fortnite but is hesitant to share more, fearing judgment for playing a violent game. Tegan listens without judging and asks why Jacob likes Fortnite. This is the first time an adult has shown interest in something Jacob is passionate about.

Over the next few weeks, Tegan talks to Jacob about online safety without criticising his enjoyment of Fortnite. Jacob feels comfortable sharing that he meets new people online who ask personal questions about his school and family. Tegan explains the importance of recognising suspicious behaviour, such as being asked personal questions or being invited to chat on another app.

Since Jacob's online interactions happened at home, there's no need to notify the NQF Regulatory Authority. However, Tegan realises it may still need to be reported under her state's child protection legislation. She makes notes of her conversations with Jacob and reports this to her service leadership team. She checks online for advice and informs Jacob's father about the situation, providing a link to the ThinkUKnow Fact sheet on Online gaming safety fact sheet.

Tegan conducts a session on online safety for all children, using videos to explain the difference between friends met in person and online. She includes culturally relevant eSafety Commissioner First Nations online safety videos for Aboriginal children to ensure they feel safe and connected.

After the session, Tegan talks to a small group of children, including Jacob, about how to handle suspicious accounts or friend requests. They agree that the best action is to tell a trusted adult, who can help collect evidence, report, and block the person. Tegan uses advice from the eSafety Commissioner's Someone is contacting me and I don't want them to resource. Limited knowledge of the apps available on each device and how to supervise their use.

Questions to guide reflection on practice

These questions help you think about what you're doing well and what you can improve.

- How can the service identify and manage any potential risks associated with the use of online devices?
- How do the approved provider and service leaders ensure all educators understand the indicators of grooming, online child abuse and exploitation?
- How do approved providers and service leaders ensure educators engage in professional learning about online safety, enabling them to identify and mitigate the risks?
- How do educators support children to learn about online safety?
- How do educators balance children's privacy with the need to provide a safe online environment for children?
- How do educators provide appropriate supervision when children are using digital technology? What does appropriate supervision of the online environment look like at your service?
- How do educators support families to be aware of online safety risks?

Useful Tool available

You can access the ***Questions to guide reflection on practice*** in the Tools section at the end of this chapter or use this link if you are using the web version of this PDF.

Resources

To access resources related to this chapter, please scan the QR code or click this link.

There are several tools available for this chapter. You can access these in the Tools section on the next page or select each link below if you are using the web version of this PDF.

Questions to guide reflection on practice

Common behaviour to look out for with online grooming

Scan the QR code to access all the resources from this chapter

Chapter 4: Resource tools

To access tools related to this chapter, please scan the QR code or click this link.

Scan QR code to access Chapter 4 tools

Questions to guide reflection on practice

Australian Children's Education & Care Quality Authority

Embedding online safety

These questions help you think about what you're doing well and what you can improve.

- How can the service identify and manage any potential risks associated with the use of online devices?
- How do the approved provider and service leaders ensure all educators understand the indicators of grooming, online child abuse and exploitation?
- How do approved providers and service leaders ensure educators engage in professional learning about online safety, enabling them to identify and mitigate the risks?
- How do educators support children to learn about online safety?
- How do educators balance children's privacy with the need to provide a safe online environment for children?
- How do educators provide appropriate supervision when children are using digital technology? What does appropriate supervision of the online environment look like at your service?
- How do educators support families to be aware of online safety risks?

Common behaviour to look out for with online grooming

Australian Children's Education & Care Quality Authority

Embedding online safety

Common behaviour to look out for with online grooming

Unsolicited friend requests

Some people may send unexpected friend or follower requests using fake identities, hoping children will accept.

Asking personal questions

Some people may ask personal questions about children's age, school, or siblings. They may ask where a child is using their device to find out if a child is alone or unsupervised.

Promising something in exchange for self-generated child abuse material

Some people offer 'likes' or gaming codes in exchange for child exploitation material. They might pretend to be from a company and promise to make the child a model or influencer, asking for photos that are child abuse material.

Fake social media accounts

Some people create fake accounts pretending to be celebrities or influencers to trick children into thinking they are interacting with the real person.

Chapter 5: Using electronic devices safely

Chapter 5: Using electronic devices safely

Scan QR code to watch the video or use this link

Using electronic devices safely

Using electronic devices safely includes choosing the right technology, understanding its risks and benefits, and teaching children how to use technology safely.

Services should think broadly about what technology includes, for example, tablets, computers, smart toys, technology toys, games consoles, baby monitors, security cameras, etc. As technology advances, new risks emerge, so services may wish to seek specialist ICT advice for cybersecurity and to stay up to date with new information. Advice may be sought on areas such as:

- the setup, ongoing monitoring and maintenance of cyber-security protections on all technology used in the service
- keeping up to date with evolving technologies and updates to prevent serious ICT issues regarding child safety, financial losses, cyber security threats, data leaks and privacy breaches

- understanding tracking technologies that websites and apps may use to collect information about users.

Use parental controls on electronic devices

Approved providers and service leaders should set up privacy and safety protections on all service devices. Tools are available to control access to appropriate content based on children's age and development. They can be used to block, filter, monitor, and limit online content on service devices, alongside supervision and other safety strategies. To keep children safe, it is important to limit access to functionalities such as location, camera, photos and videos already stored on the device, and the ability of the device to listen to its surroundings.

Smart toys

Smart toys are very similar to any other smart device in that they can interact with a person using them. Smart toys are connected to the internet, often have a microphone and/or camera, and try to mimic human intelligence. Children can ask them questions, and they respond like a chatbot.

Many smart toys collect data, including video, audio, and location information. This data can be used by a company for unknown purposes or sold to others. Data breaches can happen, where hackers access this data and use it for harmful purposes.

What does this look like in practice

For everyone

When choosing a smart toy:

- think about how much control the child has over the toy
- check if the toy is pre-programmed or can answer open-ended questions
- see if more than one child can collaboratively play with the toy at the same time
- find out what data the toy collects, where and how the data is being stored, used and disclosed, and if you can change the settings or permissions.

Child-friendly search engines and apps

Child-friendly search engines try to block websites and content that aren't safe for children.

Child-friendly search engines

Services can set these search engines as the default on children's browsers, however ads and unsafe content can still appear. This risk can be minimised by effectively supervising children while they use the internet.

Child-friendly apps

The eSafety Commissioner has advice on how to choose good online content for children under 5.

They also give tips on online tools and features, such as checking if an app has features including sharing content, photos and videos, messaging, voice chats and video calls, live streams, games, in-app purchases, location sharing and encryption.

There's an app checklist for parents and the eSafety Guide which services can also use to help decide if an app is safe and suitable for children of different ages.

See the resources page for more information.

Practical ways to make devices safer

The eSafety Commissioner has tips on keeping online environments safe, such as web browsers, gaming consoles, smart TVs, computers, tablets, smartphones, streaming services, and social media. They also have advice for Aboriginal and Torres Strait Islander families and children on how to connect safely, online.

They also have advice on useful review and rating sites to use as a starting point when looking for information about content such as movies, apps, games and websites.

What does this look like in practice?

For approved providers and service leaders

- Regularly check who can access IT systems and devices and remove access for people who leave the service.
- Follow privacy laws when using online tools to share information with families.
- Keep a record of devices, who can access them, and their login details.
- Enable internet browser security and check internet history regularly.
- Check privacy settings and age restrictions regularly.
- Install and update safety and security software, internet filters, and pop-up blockers.
- Update login details and passwords often, especially when staff change.
- Where possible, use individual logins for computers or tablets to track usage.

For everyone

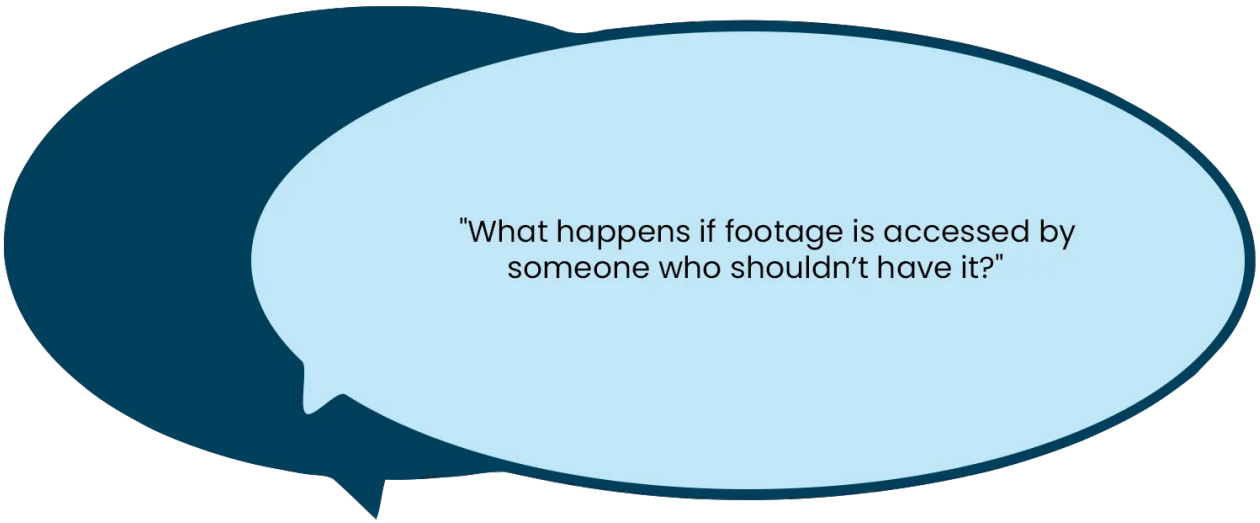
- Check the risks of smart toys and, where possible, disconnect them from the internet to avoid hacking.
- Turn off chat functions on apps and games.
- Choose app settings that turn off location sharing and enable privacy controls.
- Ensure devices are only used in designated areas of the service, where staff can actively monitor children's use.
- Encourage children to ask for help from a trusted educator if they see something they are not sure about or feel unsure, uncomfortable or unsafe, for example, if any pop-ups appear or they notice something unusual occurring.

The eSafety Commissioner has an Online safety for under 5s booklet with practical advice for families. Educators can use the tips to help children and families stay safe online. The booklet and poster are free for Australian education and care services to use.

The PlayingITSafe and eSmart websites have free resources and play-based activities that educators can print and incorporate into learning experiences.

Optical surveillance devices

Optical surveillance devices, such as a security camera, webcam or CCTV, help keep places safe by deterring poor behaviour. Surveillance devices can't stop all bad actions, but they can show what happened if something goes wrong. They can't prevent children from being harmed or replace the need for educators to directly supervise children, like checking if they're sleeping safely.



Services should not rely on or become complacent in assuming that surveillance devices throughout the service will be enough of a deterrent to prevent all staff from undertaking inappropriate behaviour. There should not be surveillance devices in places where people expect privacy, like children's bathrooms. Further information about the use of security cameras has been developed by the Office of the Australian Information Commissioner.

Services using surveillance devices must follow privacy laws for any personal information that is collected and it's important to talk to families and staff about how the service uses cameras. State and territory workplace surveillance rules may also apply.

If a security camera records people, services:

- must inform individuals, before they're recorded, that their personal information may be captured (see Australian Privacy Principle 5 for further obligations to notify individuals of the collection of personal information), not simply that their images may be captured
- must make sure any personal information is secure and destroyed or de-identified when it is no longer needed

- should put signs at all entrances and exits
- should make sure signs are easy to understand, with pictures and words.

Ensure only authorised people have access to recorded videos. Cameras and devices connected to the internet can be hacked, so it's important to keep them secure. For example, the connection of webcams and baby monitors to wireless networks adds extra privacy risks because of the increased possibility of data being intercepted by people using electronic hacking devices.

What does this look like in practice?

For approved providers

- Teach everyone why and how cameras are used at the service.
- Have clear and publicly available policies and procedures for collecting, accessing, using and storing footage.
- Keep footage safe and secure.
- Clearly identify who is authorised to view the videos and have measures in place to prevent unauthorised access.
- Check which state/territory and federal laws apply to using cameras.

Timeframe to store data

How long do I keep data for?

Data should be kept for a certain time and then destroyed properly. Under regulation 183, the NQF requires all records relating to a child enrolled at the service to be kept for 3 years from the last day they were educated and cared for by the service, unless the record:

- relates to an incident, illness, injury or trauma suffered by a child while being educated and cared for by the service or may have occurred following an incident whilst being educated and cared for by the service, in which case the record must be kept until the child is age 25, or
- is in relation to the death of a child while being educated and cared for by the service, in which case the record must be kept until 7 years after the death.

Australian Privacy Principles 11.1 and 11.2 require personal information to be protected then destroyed or de-identified when it's no longer needed. Make sure electronic records are completely removed, not just deleted.

The Royal Commission into Institutionalised Cases of Child Sexual Abuse recommended records relating to child sexual abuse should be kept for 45 years. For more information, see the ACECQA information sheet.

Keeping personal data safe

Services should have a plan to prevent and respond to cyber security problems. Check the Australian Cyber Security Centre for more information.

What to do if data is leaked or hacked

Approved providers and their services should ensure they are aware of their reporting obligations in case they are the victim of a data breach involving personal data. For example, all cyber security incidents should be reported to The Australian Signals Directorate's Australian Cyber Security Centre through the ReportCyber portal, or by calling 1300 292 371, regardless of the scale or impact of the incident. People affected by a data breach involving their personal information should also be made aware.

In relation to the personal information held by an organisation, they have a responsibility under Australian Privacy Principle 11.1 to protect that information from misuse, interference and loss, as well as from unauthorised access, modification or disclosure.

The Privacy Act also establishes the Notifiable Data Breaches scheme in which entities must notify affected individuals and the Office of the Australian Information Commissioner when an 'eligible data breach' occurs. An eligible data breach occurs when:

- personal information is lost or subjected to unauthorised access or disclosure
- this is likely to result in serious harm to any of the individuals whose information is impacted
- the business has not been able to prevent the likely risk of serious harm with remedial action

The Office of the Australian Information Commissioner recommends that organisations should follow four steps when dealing with a data breach:

- **Step 1:** Contain the data breach to prevent any further compromise of personal information.
- **Step 2:** Assess the data breach by gathering the facts and evaluating the risks, including potential harm to affected individuals and, where possible, taking action to remediate any risk of harm.
- **Step 3:** Notify individuals and the Commissioner if required. If the breach is an 'eligible data breach' under the Notifiable Data Breaches scheme, it may be mandatory for the entity to notify.
- **Step 4:** Review the incident and consider what actions can be taken to prevent future breaches.

These steps may be followed for any data breach.

For more information, visit the Office of the Australian Information Commissioner and The Australian Signals Directorate's Australian Cyber Security Centre websites.

Useful Tool available

You can access the ***How do I manage a data breach? (Office of the Australian Information Commissioner recommendations*** in the Tools section at the end of this chapter or use this link if you are using the web version of this PDF.

Case study - Collaborating to create service device rules

Collaborating to create service device rules

Aditya recently moved to Australia and has English as a second language. He works with children aged 3-5, and older children after school. His induction involved a lot of complex reading, and left Aditya with many questions.

Aditya is good with technology and doesn't mind sharing his personal information online. At the service, he read some factsheets from ThinkUKnow about children's safety online, and the key risks such as grooming, image-based abuse and preventing online child sexual exploitation. This raised questions for Aditya about how to keep the service's devices (tablets, and a smartboard, and some smart toys) safe.

Aditya talked to other educators to better understand the safety information, including how to choose safe apps for children at the service. They showed him the eSafety Commissioner's guidance on choosing appropriate apps.

Aditya looked at ABC Kids, CBeebies and PBS KIDS to find age and developmentally appropriate apps for the children. He asked a small group of children to help test the apps, and found that a 4 year old named Trevor was very familiar with one of the apps as he used it at home. Aditya encouraged Trevor to share his opinions with the group, and why he liked the app.

Aditya spoke with his room leader and suggested using different logins for the younger and older children, and talked to the children to create rules for using devices. They researched options together, and he showed them ideas from the eSafety website, which they adapted to use at the service. The children drew pictures of the steps they would take to keep them safe, so everyone could see what to do.

Questions to guide reflection on practice

These questions help you think about what you're doing well and what you can improve.

- How do educators learn to choose safe toys, games, apps, or websites?
- Who maintains the service's devices and sets up parental controls?
- How does the service keep track of who uses the service's devices and how?
- Do educators share devices between rooms or have one per room? How does the service manage risks like shared logins and using images for planning?
- Has a risk assessment been carried out for using service-issued electronic devices, including during excursions or transporting children?
- How often does the service review the use of devices? What's the service's policy on taking, using, keeping, and deleting images and videos of children?
- What settings or restrictions are in place to prevent misuse of devices?
- If the service uses surveillance devices, is there a clear policy on their use, who can see the footage, and how it's stored and deleted? Is there signage about the use of cameras?
- How does the service keep devices safe when taken off-site, for example, on excursions? How do services protect devices from online risks, like using public Wi-Fi?

Useful Tool available

You can access the ***Questions to guide reflection on practice*** in the Tools section at the end of this chapter or use this link if you are using the web version of this PDF.

Resources

To access resources related to this chapter, please scan the QR code or click this link.

There are several tools available for this chapter. You can access these in the Tools section on the next page or select each link below if you are using the web version of this PDF.

Questions to guide reflection on practice

Using electronic devices safely - How do I manage a data breach?

Scan the QR code to access all the resources from this chapter

Chapter 5: Resource tools

To access tools related to this chapter, please scan the QR code or click this link.

Scan QR code to access Chapter 5 tools

Questions to guide reflection on practice

Australian Children's Education & Care Quality Authority

Using electronic devices safely

These questions help you think about what you're doing well and what you can improve.

- How do educators learn to choose safe toys, games, apps, or websites?
- Who maintains the service's devices and sets up parental controls?
- How does the service keep track of who uses the service's devices and how?
- Do educators share devices between rooms or have one per room? How does the service manage risks like shared logins and using images for planning?
- Has a risk assessment been carried out for using service-issued electronic devices, including during excursions or transporting children?
- How often does the service review the use of devices? What's the service's policy on taking, using, keeping, and deleting images and videos of children?
- What settings or restrictions are in place to prevent misuse of devices?
- If the service uses surveillance devices, is there a clear policy on their use, who can see the footage, and how it's stored and deleted? Is there signage about the use of cameras?
- How does the service keep devices safe when taken off-site, for example, on excursions? How do services protect devices from online risks, like using public Wi-Fi?

How do I manage a data breach?

The OAIC recommends that organisations should follow four steps when dealing with a data breach:

- **Step 1:** Contain the data breach to prevent any further compromise of personal information.
- **Step 2:** Assess the data breach by gathering the facts and evaluating the risks, including potential harm to affected individuals and, where possible, taking action to remediate any risk of harm.
- **Step 3:** Notify individuals and the Commissioner if required. If the breach is an 'eligible data breach' under the NDB scheme, it may be mandatory for the entity to notify.
- **Step 4:** Review the incident and consider what actions can be taken to prevent future breaches.

These steps may be followed for any data breach.

For more information, visit the OAIC and ASD's ACSC websites.

Chapter 6: Artificial Intelligence (AI) and online safety

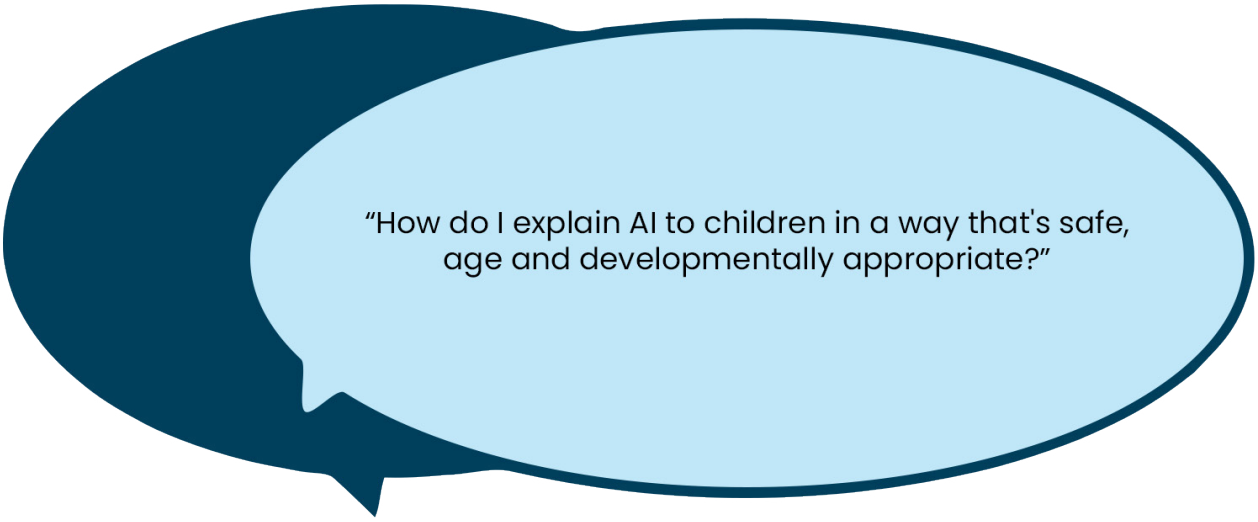
Chapter 6: Artificial Intelligence (AI) and online safety

Scan QR code to watch the video or use this link

Use of AI

It's important for services and children to understand AI as the technology becomes more easily available and embedded with other forms of digital technology. While AI has many benefits, it's also important to be aware of the risks and how it can introduce new, or amplify existing harms. Educators can help children learn about these issues as they become more curious about AI.

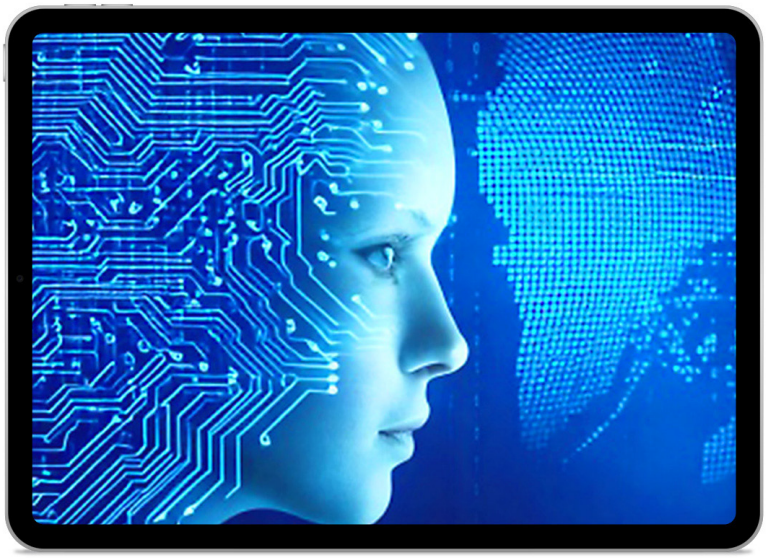
AI helps machines do things that usually need a human to complete. AI programs can make decisions, solve problems, understand and copy human language, and share information. AI keeps learning from the information it gets. This includes photos, which AI can collect, store, and use.



Generative AI can create new content, such as text, images, videos, audio, or code. People type in prompts (questions or instructions) and get AI-generated content. Generative AI has become more popular as tools, such as chatbots driven by large language models (for example, ChatGPT, Microsoft Copilot, and Google Gemini) have become more readily available. This technology is being used more frequently in schools and education and care services.

Using AI tools and AI-enabled toys with children

When interacting with a device by providing instructions or asking questions, it is possible the device may use AI capabilities to provide a response in the form of a text, image, video or voice response. Examples include Siri, Alexa, Cortana, Apple Intelligence, and Google Assistant.



AI tools have also been developed that children can interact with to engage in various activities including generating images and songs, remixing songs, and playing games such as rock, paper, scissors.

There are also internet-connected toys for children that use AI. These toys can record and analyse how children play to personalise their experience. However, this play data may also be used to personalise advertisements to children. This "datafication" can also threaten children's privacy by collecting and using their personal information.

Using generative AI can be helpful, but there are risks. This includes safety risks, such as spreading harmful content, cyberbullying, and image-based abuse. It also includes privacy risks, as Generative AI can use children's personal data from the internet, including a child's digital footprint. Generative AI may pose a higher risk to younger children because they:

- may not understand the difference between humans and AI
- may not understand what to do if AI chatbots respond inappropriately, causing strong emotions
- can be coerced by perpetrators using AI to groom, manipulate and exploit children.

Services considering using AI tools with children must be aware of and address the risks.

Case study - Purchasing a new smart toy

Purchasing a new smart toy

A service is thinking about buying some smart teddy bear toys that use AI. These smart toys can answer children's questions and talk with them. Children have started bringing their own teddy bears to the service and telling them secrets. Educators can see benefits for children and think that having a smart toy that talks would help children improve their language skills.

The educators know that today's learning toys are very different from the toys of the past. They think about the possible benefits and risks of the smart toys and how to reduce any risks, like turning off location services and supervising children's interactions with the teddy bears. They also talk to the families about their concerns and ask for their permission before buying the toys.

The use of AI tools as part of children's learning

The approved learning frameworks see digital technology as an important tool for teaching and learning. This requires the integration of digital literacy skills, so that children and young people learn about and use generative AI technology in age and developmentally appropriate ways, both in formal school settings and informally with their peers and families.

A strength-based education helps to build preventative strategies and resilience so that children and young people are equipped to safely use current and emerging technologies. But it's important to be careful, understand the risks, and if choosing to use AI, do so in a way that is appropriate for the age and developmental stage of the children.

Deciding whether to use generative AI tools with children for learning needs careful thought and risk assessment. Generative AI can create content that is not suitable for children, like violent or sexually explicit material and they may lack safeguards to prevent children from seeing harmful content. If used incorrectly, AI tools can produce harmful or misleading results. For example, AI might generate inappropriate material like online pornography for a child. It is possible that children may disclose experiences of abuse to AI chatbots. The chatbot may not be trained to appropriately handle disclosures and may provide the child with a harmful response.

AI chatbots are often designed to encourage ongoing interaction, which can lead to overuse and even dependency. Children and young people are particularly vulnerable to mental and physical harms from AI companions. Their age means they are still developing the critical thinking and life skills needed to understand how they can safely use computer programs, and what to do about it. This reinforces the need to support children to use AI safely.

If educators are using AI to help with programming and creating learning experiences, this should not be done while children are present. To avoid exposing children to inappropriate content, educators should check if the AI-generated content is appropriate before showing it to children. Children need to be adequately supervised at all times, and closer supervision is needed when children access devices with AI tools.

The use of AI tools by educators to create the curriculum

Some AI tools offer to help with creating documentation about children's learning and generating or deciding upon future learning experiences for children.

Considerations for Using AI in Children's Education and Care

If approved providers and service leaders decide to use AI, they need to determine the agreed parameters and how these are communicated within the service and with families. However, it is important to exercise caution and understand and manage the risks.

AI may complement an educator's skills, however it cannot replace educators' professional knowledge and understanding of children and families, including families' priorities for their children's learning and development. Any content created by AI should be checked by an educator to make sure it is accurate and appropriate.

Educators use their deep knowledge and understanding of children when planning and evaluating learning experiences. Using AI to document children's experiences can reduce educators' connections with children's play. Educators need to be aware that using AI can limit their ability to use their own knowledge and skills and refine their pedagogy to create tailored learning experiences for each child.

Interactions between adults and children are crucial for children's cognitive, social and emotional development. These in-person interactions constitute the core of high-quality early childhood education and care and cannot be replaced by AI tools.

The Limitations of AI in Documenting Children's Learning

There is also a risk of inaccurate or limited analysis if educators use generative AI to replace how they document and analyse children's learning and development. This risk is clear when comparing AI with the value of an educator's unique knowledge and skills, including their:

- knowledge of child development and pedagogical teaching strategies
- intentionality in designing, critically reflecting on and refining learning experiences for each child
- professional judgment
- understanding of each child's current knowledge, strengths, ideas, culture, abilities and interests.

Addressing AI Bias in Children's Education and Care

If using AI to create learning experiences, educators should be aware of AI bias and review all outputs to avoid using inaccurate information and reinforce discrimination or stereotypes. Examples of AI bias and the risks they pose include:

- AI systems are trained on large data sets that may not be accurate or inclusive, reflecting the online world but not the diverse offline world.
- AI models may give confident but wrong or harmful answers, called "hallucinations", so educators should always check the accuracy of AI generated content. For example, an approved provider uses AI to find links to the approved learning frameworks in their documentation app, and educators then double-check against the EYLF or MTOP (or VEYLDF in Victoria).
- AI bias can pose safety (including cultural safety) risks, especially for underrepresented and marginalised communities, such as Aboriginal and Torres Strait Islander people.
- AI models that only reflect English-speaking, Western values may not be safe or appropriate for diverse users.

The Importance of Human-Led Self-Assessment

There are also risks if using AI tools to replace human self-assessment. Engaging in self-assessment is key for services' continuous improvement and to ensure all views (including children, educators, families, and communities) are incorporated and reflected in prioritised areas for action. Using AI for self-assessment may not provide information specific to the service's unique circumstances and community views and so AI should not be used in the absence of human self-assessment.

What does this look like in practice?

For approved providers

- Talk regularly with service leaders and educators to understand if they are using AI tools. Discuss the risks and how to manage them.

- If using AI, give clear instructions to service leaders and staff about using AI tools for certain tasks. Be specific about when and how AI can and can't be used.
- Check if the service's online safety policy and procedures need updating to include the use or restriction of AI tools.
- Make sure any use of AI follows privacy laws.

For everyone

- Do not input personal information into an AI tool that could reveal personal details, including about children (like names, birthdates, or other identifying information).
- Understand how any information you put into an AI tool will be used, stored, and shared by the AI tool.
- Read eSafety's statement on generative AI to ensure online safety is at the forefront of all uses of AI.
- Manage your data by turning off your chat history and not allowing your data to be used to train AI models.
- Fact check content generated by AI tools and consider whether it has taken into account all relevant information.
- Assume any information being input into generative AI tools could become public and think about what is appropriate to include.

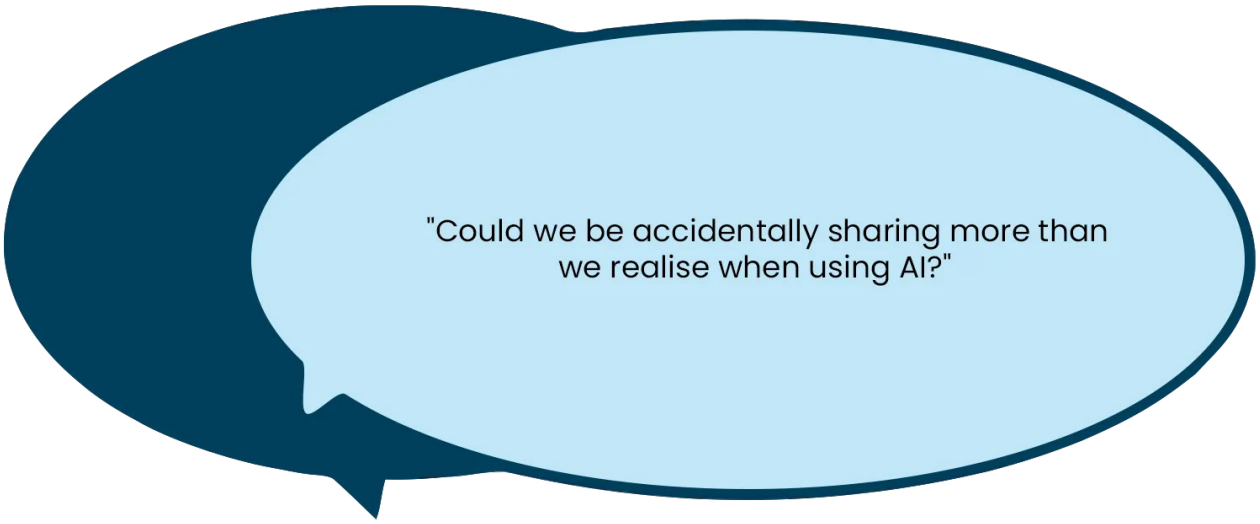
[14] Dr Kate Highfield, Associate Professor, Early Childhood Education, University of Canberra. CELA Amplify Blog Newsletter. (2023). AI and documentation: What are the ethical considerations? (https://www.cela.org.au/publications/amplify!-blog/jun-2023/ai-and-documentation-ethical-considerations)

What information can be used by AI tools

Some AI tools offer to help with creating documentation about children's learning and generating or deciding upon future learning experiences for children.

AI technologies are often made by companies (often based overseas) whose primary focus is not children's rights and welfare. This should be considered when deciding whether or not to use them. The OAIC provides Guidance on privacy and the use of commercially available AI products, stating that privacy laws apply to any personal information input into an AI system and the output generated by AI.

There is a risk that any data collected by an AI tool about a child could be hacked or misused, violating the child's right to privacy. For example, photos of children in Australia have been taken from the internet and used to train AI tools without the knowledge or consent of the children or their families.



What does this look like in practice?

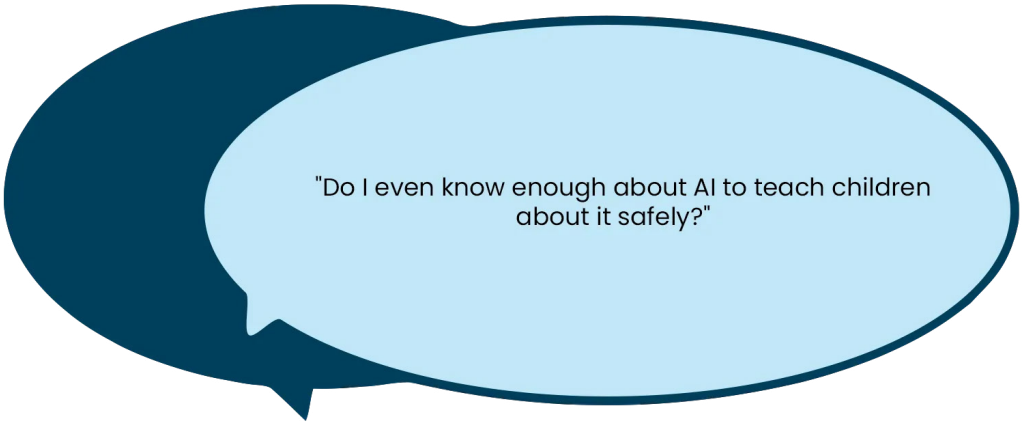
For educators

- If using AI tools, it is safer to use them to generate templates that do not involve personal or other sensitive information. For example, this might be to reference the requirements of the National Law and National Regulations and draw on publicly available guidance from authoritative sources.
- Never share personal information about children or others when using AI tools. For example, if using an AI tool to summarise a child's learning experiences, always remove any identifying details before entering them into the tool. Use random initials and birthdates to create generic profiles that can track children's progress without risking their privacy.

Educating children about AI and online safety

As AI becomes a bigger part of children's digital lives, it's important to teach them about the benefits and risks of AI in an age and developmentally appropriate way.

It's important to teach children about how AI works and the benefits and risks of AI systems from an early age.



What does this look like in practice?

For educators

- Engage children in fun and meaningful activities to help them understand AI concepts, such as:
  - AI is not a real person
  - AI can put your personal information on the internet
  - AI never forgets information and can use it repeatedly, even if it's no longer accurate
  - AI was created by humans and can be trained with examples like images and sounds. If taught bad or inaccurate things, AI will share that information, and opinions can look like facts
  - AI uses examples to get better at providing information
  - AI has limitations and can make mistakes
  - AI does not replace the need for talking to people or using our own minds to solve problems and learn new things.
- Discuss the importance of privacy with children, including how AI can collect and store personal information and why this can lead to safety risks.
- In an age and developmentally appropriate way, encourage children to be critical of the information they get from new technology and help them find answers from trustworthy sources.

- Teach children to question the writing, images, and posts that AI tools create. For example, ask:
  - How did AI come up with the answer?
  - What information did it use to find the answer?
  - Could the responses harm marginalised groups?
  - Are the answers making assumptions about race, gender, and other forms of identity?
- Consider if sensitive information about the service or personal information about any staff member could be identified because of the information input into the AI tool.

Case study - Using AI to reduce paperwork

Using AI to reduce paperwork

Sakura works with babies and toddlers and is the room leader. She uses AI tools to help create the educational program for children.

Sakura found an AI Tool that already includes the EYLF and other important documents such as the National Law and National Regulations. The AI tool has learned her style of creating programs because Sakura has been feeding it her own work for the last 6 months. She made sure not to include any personal information about specific children. She also told the AI tool about the educational theorists that influence her work.

Sakura regularly talks with the educational leader, who helps all the educators use the same AI tool. They discuss what to do if the AI tool suggests learning experiences that are not age and developmentally appropriate or culturally safe. For example, the AI tool might not suggest activities that include Aboriginal and Torres Strait Islander ways of knowing, and sometimes the information it gives is wrong. Sakura knows she must check any suggestions from the AI tool for accuracy and appropriateness before using them.

Sakura understands that letting the AI tool create the entire program is not appropriate because it takes away from her professional judgment and teaching style. She knows that building strong, respectful relationships with children and their families is essential for planning the program.

Sakura knows the AI tool is still learning, and she works with other educators to find more ways to use it. She has started using the AI tool to create learning stories from her observations of the children. However, she is not fully confident that the AI tool is documenting the learning accurately, so she adds her own professional assessment and evaluation. She notices that the AI tool suggests future activities that do not match her teaching style, but she still reads them to get new ideas.

Sakura is open to using the AI tool to improve her documentation and expand her ideas for the children's learning. However, she remains in control of deciding what the educational program looks like. She uses her knowledge and experience to analyse the AI tool's suggestions and adapt them to fit her service's context. Sakura is willing to share her experiences with other educators and learn from them about how they use AI and manage risks in their daily practices.

Questions to guide reflection on practice

These questions help you think about what you're doing well and what you can improve.

- What ethical issues need to be considered before using AI at the service?
- How do the service's policies and guidelines make it clear when AI can and cannot be used?
- What training is available for staff to understand the risks and opportunities of AI?
- How can staff keep learning about new AI tools and technologies to address new risks and benefits?
- How does the service manage any personal and confidential information that should remain private and ensure it is properly de-identified if using AI?
- How does the service talk to families about the use of AI?
- How can families be asked for their consent when their children interact with AI or have their information used by AI?
- How can AI be used to help educators while protecting children's safety and privacy?
- How are children's digital footprints protected and minimised when using AI?

Useful Tool available

You can access the ***Questions to guide reflection on practice*** in the Tools section at the end of this chapter or use this link if you are using the web version of this PDF.

Resources

To access resources related to this chapter, please scan the QR code or click this link.

There are several tools available for this chapter. You can access these in the Tools section on the next page or select each link below if you are using the web version of this PDF.

Questions to guide reflection on practice

Explore definitions of terms from the NQF Online Safety Guide. Select letter groups below to reveal corresponding lists of terms and their definitions.

A – B

Active citizenship: is about displaying values of respect, inclusion and helping others, as well as appreciating diversity in all its forms. It involves helping out and being connected to your local community. (Adapted from Be an active citizen, Australian Government 2022).

Active learning environment: an active learning environment is one in which children

Scan the QR code to access all the resources from this chapter

Chapter 6: Resource tools

To access tools related to this chapter, please scan the QR code or click this link.

Scan QR code to access Chapter 6 tools

Questions to guide reflection on practice

Australian Children's Education & Care Quality Authority

Artificial Intelligence (AI) and online safety

These questions help you think about what you're doing well and what you can improve.

- What ethical issues need to be considered before using AI at the service?
- How do the service's policies and guidelines make it clear when AI can and cannot be used?
- What training is available for staff to understand the risks and opportunities of AI?
- How can staff keep learning about new AI tools and technologies to address new risks and benefits?
- How does the service manage any personal and confidential information that should remain private and ensure it is properly de-identified if using AI?
- How does the service talk to families about the use of AI?
- How can families be asked for their consent when their children interact with AI or have their information used by AI?
- How can AI be used to help educators while protecting children's safety and privacy?
- How are children's digital footprints protected and minimised when using AI?

Glossary

are encouraged to explore and interact with the environment to make (or construct) meaning and knowledge through their experiences, social interactions and negotiations with others. In an active learning environment, educators play a crucial role of encouraging children to discover deeper meanings and make connections among ideas and between concepts, processes and representations. This requires educators to be engaged with children's emotions and thinking. (Adapted from South Australian Curriculum Standards and Accountability (SACSA) Framework, General introduction).

Active listening: is concentrating on more than what is being said (such as gestures, facial expression and body language) and involves listening to and acknowledging what is being said in ways that enhance mutual understanding.

Additional needs: the term used for children who require or will benefit or be able to participate more fully from specific considerations, adaptations or differentiation of any aspects of the curriculum, including resources and the environment.

Agency: being able to make choices and decisions, to influence events and to have an impact on one's world.

Artificial Intelligence (AI): An engineered system that generates predictive outputs such as content, forecasts, recommendations, or decisions for a given set of human-defined objectives or parameters without explicit programming. AI systems are designed to operate with varying levels of automation.

Body safety awareness: Teaching children, from a young age, that they are the boss of their body and what they say goes is incredibly empowering. It includes exploring body boundaries, respect, consent, feelings and emotions, choices, recognizing bullying behaviours and body safety. Learning these important and life-long skills are crucial in developing children's confidence and will help them to recognise their rights — especially in regards to their body.

C

Child maltreatment, abuse and neglect: The term Child maltreatment is often used interchangeably with the terms 'child abuse and neglect'. This guide uses child maltreatment, abuse and neglect and defers to the definition provided by the World Health Organisation (2006) and includes:

> *All forms of physical and/or emotional ill-treatment, sexual abuse, neglect or negligent treatment or commercial or other exploitation, resulting in actual or potential harm to the child's health, survival, development or dignity in the context of a relationship of responsibility, trust or power.*
>
> *(https://aifs.gov.au/resources/policy-and-practice-papers/what-child-abuse-and-neglect)*

Child grooming: Grooming, through manipulative behaviours, is when an adult prepares a child for sexual abuse. Perpetrators may sexually abuse children by using manipulative behaviours or strategies as part of a process commonly involving prosocial behaviours violating personal boundaries, to obtain sexual contact with children in the periods prior to, during and following sexual contact. Grooming can happen in person or online. It is a sexual offense and must be reported.

Child protection: means responding to and dealing with cases of child abuse or neglect that have already happened.

Child safeguarding: means taking steps to prevent harm from happening in the first place.

Child sexual exploitation: when a child is manipulated or coerced to participate in a sexual activity in exchange for, or the promise of, an incentive. This can include incentives such as food, accommodation, clothing, drugs, alcohol, cigarettes or money. It can also include incentives such as love, affection, or safety. Child sexual exploitation is a distinct form of child sexual abuse because of this notion of exchange or reward.

Children: refers to each baby, toddler, three to five year old and school age child and means children as individuals and as members of a group in the education and care setting, unless otherwise stated.

Children who have displayed harmful sexual behaviours: includes a broad range of sexual behaviours in children and young people. This includes behaviours that affect their own development, as well as behaviours that are coercive, sexually aggressive or predatory to others.

Children living with disability: disability is part of human diversity. There are many different kinds of disability and they can result from accidents, illness or genetic disorders. Disability may affect mobility, ability to learn, ability to communicate, or ability to engage with others and with experiences. Some children may have more than one type of disability. A disability may be visible or hidden, may be permanent or temporary and may have minimal or substantial impact on a child's abilities.

Citizens: participating members of local, national, and global communities.

Code of Conduct: A child safe Code of Conduct is a document outlining expected behaviours from all members of an organisation, and behaviours that are unacceptable, when interacting with children and young people.

Communities: social, cultural or geographic contexts, groups or networks that share a common purpose, heritage, rights and responsibilities and/ or other bonds. 'Communities' is used variously to refer, for example, to the community within early childhood settings, extended kinships, the local geographic community and broader Australian and global society.

Cyberbullying: Cyberbullying is when someone uses the internet to be mean to a child or young person so they feel bad or upset.

D - K

Disclosure: is a process by which a child conveys or attempts to convey that they are being or have been sexually abused, or by which an adult conveys or attempts to convey that they were sexually abused as a child. This may take many forms, and might be verbal or non-verbal. Nonverbal disclosures using painting or drawing, gesticulating, or through behavioural changes, are more common among young children and children with cognitive or communication impairments. Children, in particular, may also seek to disclose sexual abuse through emotional or behavioural cues, such as heightened anxiety, withdrawal or aggression.

Enforceable undertaking: is a written undertaking from a person, in which the person sets out what they will do or refrain from doing, to comply with the National Law and Regulations.

Family/Family member: In relation to a child, family/family member means:

- a parent, grandparent, brother, sister, uncle, aunt, or cousin of the child, whether of the whole blood or half blood and whether that relationship arises by marriage (including a de facto relationship) or by adoption or otherwise; or
- a relative of the child according to Aboriginal or Torres Strait Islander tradition; or
- a person with whom the child resides in a family-like relationship; or
- a person who is recognised in the child's community as having a familial role in respect of the child.

Fitness and propriety: describes a person's suitability to be involved in the operation of an education and care service. More information on the meaning of fitness and propriety is available in the National Law and Guide to the NQF.

Generative artificial intelligence (AI): A branch of AI that develops generative models with the capability of learning to generate novel content such as images, text, and other media with similar properties as their training data.

Geotag: A piece of electronic data that shows where someone or something is and can, for example, be attached to a photograph or comment on social media.

Halo effect: The halo effect can occur during recruitment if the recruiter hires a person primarily because they were personable and likeable. Instead, individuals should always be selected based upon their demonstration of child safe skills, values and behaviours. When the 'halo effect' occurs, the approved provider and/or the service leader may ignore any concerns, comments or behaviours that may indicate an applicant is not right for the position, instead choosing to employ them because they seem 'nice'.

Harmful content: Harmful content includes:

- sexually explicit material
- false or misleading information
- violence
- extremism or terrorism
- hateful or offensive material.

Illegal content: Illegal content includes:

- images and videos of child sexual abuse
- content that advocates terrorist acts
- content that promotes, incites or instructs in crime or violence
- footage of real violence, cruelty and criminal activity.

Image-based abuse: Sharing, or threatening to share, an intimate image or video without the consent of the person shown. AND Restricted content/Restricted access system - A Restricted Access System aims to limit the exposure of children and young people under 18 to pornography and other age-inappropriate online content.

Kinships systems: a kinship system is an aspect of Aboriginal and Torres Strait Islander social organisation. It is a complex system that determines the relationships, roles, responsibilities, and obligations to one another and includes ceremonial business around land, lore, births, marriages and deaths. There are different structures and relationships that are not necessarily biological and covers more than people. Kinship includes a connection to Country: animals, places, ancestors, weather systems and plants.

L – P

LGBTIQA+: Lesbian, gay, bisexual, transgender, intersex, queer, asexual, and other identities not fully represented in the acronym.

Mandatory reporter: A person who is required by either state or territory law to report known and suspected cases of child abuse and neglect to a nominated government department or agency. Usually, they need to report to a child protection authority.

National Law: Unless otherwise specified, the Education and Care Services National Law Act 2010 or, in Western Australia, the Education and Care Services National Law (WA) Act 2012. This applied law system sets a national standard for children's education and care across Australia. See the ACECQA website for the Application Act or legislation that applies in each jurisdiction.

National Principles: National Principles for Child Safe Organisations are a set of ten principles that guide organisations in developing child safe cultures and practices.

National Regulations: The Education and Care Services National Regulations 2011. The National Regulations support the National Law by providing detail on a range of operational requirements for an education and care service.

Offender: is generally used for a person who is found by a court to have done something unlawful.

Online hate: Online hate can be defined as any hateful posts about a person or group based on their race, religion, ethnicity, sexual orientation, disability or gender.

Organisational culture: Organisational culture is the set of collective actions, values, beliefs, attitudes, systems, and rules that outline and influence employee behaviour within an organisation.

Parent: in relation to a child, includes— (a) a guardian of the child; and (b) a person who has parental responsibility for the child under a decision or order of a court.

Pedagogy: is the art, craft and science of educating. Pedagogy is the foundation for educators' professional practice, especially those aspects that involve building and nurturing relationships, curriculum decision-making, teaching and learning.

Perpetrator: an adult who has sexually abused a child or young person, but who may or may not have been convicted of this crime.

Persons with Management or Control: person with management or control means a person referred to in section 5A of the National Law. It relates to the approved provider.

Prosocial behaviour: is doing something to benefit, help or care for someone else because you believe that other people's feelings and experiences are important.

R - Z

Reconciliation: "At its heart, Reconciliation is about strengthening relationships between Aboriginal and Torres Strait Islander peoples and non-Indigenous peoples, for the benefit of all Australians." (https://www.reconciliation.org.au/reconciliation/what-is-reconciliation/)

Reportable conduct: is conduct that must be reported under legislation that obliges designated institutions to report allegations of institutional child sexual abuse to an independent statutory body.

Royal Commission into Institutional Responses to Child Sexual Abuse: The Royal Commission presented a final report to the Governor-General in December 2017 after a 5 year inquiry and made many recommendations about national, state and territory mechanisms for working with children checks (WWCC), mandatory reporting and child safety obligations, teacher registration/accreditation, Reportable Conduct Schemes and Child Safe Standards. Each jurisdiction has responded to the recommendations and is at different stages of maturity and have different

obligations, requirements, thresholds and information sharing mechanisms for inter-related child protection mechanisms.

Serious detrimental action: cannot be taken against a person for making a disclosure. Serious detrimental action includes dismissal, involuntary transfer, loss of promotion or demotion (National Law, section 296)

Sexting: means sending a sexual message or text, with or without a photo or video. It can be done using a phone service or any platform that allows people to connect via an online message or chat function.

Smart toys: Smart toys generally require an internet connection to operate as the computing task is on a central server.

Staff member: in relation to an education and care service, means any individual (other than a volunteer) employed, appointed or engaged to work in or as part of an education and care service, whether as a family day care coordinator, educator or otherwise (National Law).

Staff misconduct: In an early education and care setting, refers to when a staff member's behaviour breaches the code of conduct or they act in a way that is unacceptable when interacting with children and young people, or other staff and families.

Technologies: includes much more than computers and digital technologies used for information, communication and entertainment. It involves the development of new objects or tools by people that help them in their lives. There are 3 broad types of technology: mechanical (e.g. wheels, blocks, levers and gears) analogue technology (e.g. film-based photography, drawing, painting); and digital technology (e.g. mobile phones and computers) (ECA 2018).

Technology toys: Technology toys usually need to be connected to a phone, tablet or computer via Bluetooth connection but generally do not require an internet connection to work the device.

Trauma: children may be exposed to four different types of trauma:

1. Single incident trauma which can result from experiencing a time-limited and often unexpected traumatic event (e.g. a car accident, bushfire, loss of a loved one)
2. Complex trauma which can result from exposure to severe, sustained and harmful interpersonal events (e.g. physical, emotional or sexual abuse, profound neglect, domestic and family violence)
3. Historical trauma which refers to multigenerational trauma experienced by a specific cultural group (e.g. the intergenerational impacts of the European colonisation and forced removal of children from families and communities on Aboriginal and Torres Strait Islander communities)
4. Intergenerational trauma which can result when unresolved complex trauma impacts on the next generation's capacity to parent and leads to intergenerational harm. When exposed to traumatic events at a young age, children may not have developed or will have lost their sense of safety, trust and belonging.

Trauma informed practice: responsive practice made possible by awareness of the impact of trauma on children's learning, development and wellbeing. This includes recognising the signs and symptoms of trauma in children, responding by making places and relationships feel safe and supportive to children, and helping children to develop their capacity for emotional regulation.

Unwanted contact: Unwanted contact is any type of online communication that makes you feel uncomfortable, unsafe or harassed. It can be with a stranger or someone you know.

Victim and survivor: Victims and survivors are terms used for those who have experienced child sexual abuse. It should be recognised that not all people with lived experience of child sexual abuse will identify with these terms.