



These guidelines are part of a series intended to assist in the development of your service's policies and procedures required under regulations 168 and 169. They set out the main components to be included in your policies and procedures, and considerations for each component.

They should guide how you develop your policies and procedures, and are not an exact format to be followed.

SAFE USE OF DIGITAL TECHNOLOGIES AND ONLINE ENVIRONMENTS

POLICY GUIDELINES

Under the *Education and Care Services National Regulations*, an approved provider must ensure that policies and procedures are in place for the safe use of digital technologies and online environments at the service (regulation 168) and take reasonable steps to ensure those policies and procedures are followed (regulation 170).

It's important to keep children safe when using digital technologies and online environments as part of the educational program. Children have the right to quality education and care in a safe environment, including when using digital technologies and online.

Your policy and procedures must provide a clear set of guidelines that address the safe use of digital technologies and online environments at the service, including the following:

- The taking, use, storage and destruction of images and videos of children being educated and cared for by the service.
- Obtaining authorisation from parents to take, use and store images and videos of children being educated and cared for by the service.
- The use of any optical surveillance device at the service (e.g. closed-circuit television).
- The use of any digital device issued by the service.
- The use of digital devices by children being educated and cared for by the service.

Your policy and procedures for the safe use of digital technologies and online environments are to align with the [*National Model Code for Taking Images or Videos of Children while Providing Early Childhood Education and Care*](#) (National Model Code), and adopt its parts as follows:

- only service-issued devices are to be used to take images or videos of children while providing education and care
- personal electronic devices that can take images or videos, and personal storage and file transfer media, are not to be in the possession of any person while providing education and care and working directly with children, unless for authorised essential purposes such as emergencies, health and family needs
- strict controls are to be in place for appropriately storing and retaining children's images and recordings.

Your policy and procedures also need to address:

- how approved providers, nominated supervisors, and family day care (FDC) educators at a service meet their legislative obligations to ensure every reasonable precaution is taken to protect children from harm and hazard, including when using digital technologies and online environments
- the timely and effective identification of, and response to, children who may be at risk of or are experiencing abuse or maltreatment through digital technologies and online environments. This includes appropriate notification to the relevant regulatory authorities, where required.

When developing your policies and procedures for the safe use of digital technologies and online environments at the service, you will need to consider:

- the safety and security of the digital technologies and online environments being used by any individual at the service, including during excursions and transport that forms part of the service
- the physical environment in which these digital technologies and online environments are used
- staffing and supervision, including monitoring for any data transfers between devices issued by the service and any other devices and ensuring device use is authorised and/or for approved purposes as per the National Model Code
- staff training and competency in the safe use of digital technologies and online environments
- the use of digital devices by visitors while at the service, including families.

In addition to meeting your obligations under the *Education and Care Services National Law* and *Education and Care Services National Regulations*, you may need to consider other applicable requirements under state, territory or federal law. For example, privacy laws, child protection laws including mandatory reporting requirements, listening device laws, the National Principles for Child Safe Organisations, and Child Safe Standards may apply in your jurisdiction.

Your policies and procedures should address these requirements, as well as quality practices relating to the safe use of digital technologies and online environments at the service that align with the National Quality Standard.

Every service is different. It is not sufficient to apply generic policies and procedures to multiple services. You will need to contextualise your policies and procedures to your service's operations and its unique context.

1. Title

Safe use of digital technologies and online environments policy

2. Policy statement

The policy statement will reflect your service's philosophy about providing a child safe environment when it comes to the safe use of digital technologies and online environments.

For example:

Children's safety and wellbeing are paramount at our service, including the safe use of digital technologies and online environments, including for children's learning and development and maintaining records.

3. Background

Your policy needs to include a statement of why this policy is in place.

For example:

The *Education and Care Services National Regulations* require approved providers to ensure their services have policies and procedures in place for the safe use of digital technologies and online environments at the service.

4. Legislative requirements

Your policy must be consistent with, and refer to, legislative requirements for providing a child safe environment. Examples include, but are not limited to:

Section 162A	Child protection training
Section 165	Offence to inadequately supervise children
Section 167	Offence relating to protection of children from harm and hazards
Regulation 84	Awareness of child protection law
Regulation 115	Premises designed to facilitate supervision
Regulation 122	Educators must be working directly with children to be included in ratios
Regulation 123	Educator to child ratios – centre-based services
Regulation 123A	Family day care coordinator to educator ratios – family day care service

Regulation 124	Number of children who can be educated and cared for – family day care educator
Regulation 165	Record of visitors
Regulation 166	Children not to be alone with visitors
Regulation 168	Education and care services must have policies and procedures
Regulation 169	Additional policies and procedures – family day care service
Regulation 170	Policies and procedures to be followed
Regulation 171	Policies and procedures to be kept available
Regulation 172	Notification of change to policies or procedures
Regulation 175	Prescribed information to be notified to Regulatory Authority
Regulation 176	Time to notify certain information to Regulatory Authority

When writing your policy, you will need to break down what is required under each regulation and how your service will meet these requirements. How these work in practice will be contained in your procedures.

As you reflect on the *Safe use of digital technologies and online environments policy*, it might highlight the need to split its various areas into different policies and/or procedures that can be readily accessed by all staff members to follow. For example, you may wish to have separate procedures under your policy for *Online supervision*, *Reporting online child abuse*, *Using electronic devices safely*, and *Collecting, storing and sharing personal information*.

5. Principles to inform your policy

All decision-making should be carried out in accordance with the principles of your service's *Safe use of digital technologies and online environments policy*. Examples of principles could include, but are not limited to:

- all children attending our service are provided with a safe environment through the creation and maintenance of a child safe culture, and this extends to the safe use of digital technologies and online environments
- children's wellbeing is paramount and children will be actively involved in decision-making about the safe use of digital technologies and online environments at the service, including taking, using and sharing an image or video of them on a digital device, whether by an adult or a child
- management, educators, and staff are aware of their roles and responsibilities to identify and respond to every child at risk of child abuse or maltreatment, including abuse or maltreatment that may occur through digital technologies and online environments
- approved providers, nominated supervisors, educators, volunteers and students, take reasonable precautions and use adequate supervision to ensure children are protected from harm that may occur through digital technologies and online environments
- procedures to effectively manage incidents and disclosures are in place and regularly rehearsed
- in adopting the National Model Code, our service considers the purpose and use of electronic and digital devices across the service and communicates clear expectations for educators, other staff and volunteers, to ensure child safe practices are implemented for the use of electronic and digital devices while providing early childhood education and care.

Considerations for active supervision

Supervising children when they use digital devices, particularly when accessing an online environment, is very important to keep them safe. Even if an adult is in the same room, they need to actively supervise the child.

High-risk behaviours for children online include:

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

Active supervision helps prevent incidents and enables educators to step in if something goes wrong. It also creates a supportive environment where children feel comfortable making a disclosure or asking for help to learn how to use online programs, apps, etc, safely and appropriately, without fear of reprisal.

Additional supervision considerations may exist in outside school hours care (OSHC) and family day care (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.

Note that supervision is facilitated by the physical design and maintenance of the premises (regulation 115), the supervision practices of educators (section 165), and educator ratios (section 169, regulations 122-124).

Also be mindful that the *Safe use of digital technologies and online environments policy and procedures* are closely aligned with most of your policies, especially your *Providing a child safe environment policy and procedures*, as children's health and safety are paramount.

6. Key terms

To make it easier for your audience, provide definitions of key terms that may not be used every day. For example:

Term	Meaning	Source
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.	Glossary to NQF Child Safe Culture and Online Safety Guides
Cyberbullying	When someone uses the internet to be mean to a child or young person so they feel bad or upset.	
Disclosure	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. Non-verbal 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.	
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.	
Harmful content	Harmful content includes: <ul style="list-style-type: none"> • sexually explicit material • false or misleading information • violence • extremism or terrorism • hateful or offensive material. 	
Illegal content	Illegal content includes: <ul style="list-style-type: none"> • 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. 	
Online hate	Any hateful posts about a person or group based on their race, religion, ethnicity, sexual orientation, disability or gender	
Sexting	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.	

Term	Meaning	Source
Smart toys	Smart toys generally require an internet connection to operate as the computing task is on a central server.	Glossary to NQF Child Safe Culture and Online Safety Guides
Unwanted contact	Any type of online communication that makes you feel uncomfortable, unsafe or harassed. It can be with a stranger or someone you/the child knows.	

7. Links to other policies

Refer to related policies and procedures, for example:

- providing a child safe environment
- incident, injury, trauma, and illness
- interactions with children
- staffing
- visitors to FDC residences and venues while education and care is being provided to children.

8. Induction and ongoing training

State information about induction training and frequency of ongoing training and information sharing to assist managers, coordinators, educators and other staff to fulfil their roles effectively.

9. Policy created/reviewed

Include the date the policy was created, reviewed or changes were made.

10. Monitoring, evaluation and review

State when the policy will be reviewed and who will be responsible for this. All policies need to be monitored and reviewed regularly to ensure that they are up to date and compliant with the National Law and National Regulations.

Your policy should record the dates it has been reviewed or when changes were made, as well as the next review date. In the event of a revision or change of policy, you will need to ensure educators and families are made aware of the changes and the revised policy, removing access to electronic or hardcopies of the older versions.

Follow the appropriate record-keeping processes for each updated version of the policy.

11. Checklist

Have you referenced the relevant regulations and are these reflected in the policy?

How does your policy reflect the National Model Code and Guidelines for the taking of images and videos and use of electronic and digital devices at the service?

Does the title provide a clear and concise statement identifying the intent of the policy?

Have you checked the policy requirements and referenced related legislation that applies to your service type?

Does your policy statement provide a framework for child-safe decision-making and ensure consistent practice?

Does your policy statement reflect your service philosophy and child safe culture?

Is it clear why this policy exists?

SAFE USE OF DIGITAL TECHNOLOGIES AND ONLINE ENVIRONMENTS

PROCEDURES GUIDELINES

Under the *Education and Care Services National Regulations*, an approved provider must ensure that policies and procedures are in place for the safe use of digital technologies and online environments at the service. These guidelines are part of a series to assist in the development of your policies and procedures required under regulations 168 and 169. They are to guide how you develop your policies and procedures, and are not an exact format to be followed.

Your procedures should be written in clear and concise language, making them easy to read and understand. This makes it easy for anyone within your service to implement. Separate [Guidelines](#) have also been prepared to assist you to implement the National Model Code. These should be considered when preparing your procedures for the *Safe use of digital technologies and online environments*.

The steps and guidelines you document will not only guide your practice, but also inform regulatory authorities of roles and responsibilities at the service.

When thinking about your procedures for the safe use of digital technologies and online environments at the service, they need to be practical and achievable. For example, if your procedures state that you develop a culture where children feel safe to talk to a trusted adult about what they have seen online, you will need to make sure steps are in place for this to occur.

Procedures for the safe use of digital technologies and online environments at the service must consider, at a minimum:

- the taking, use, storage and destruction of images and videos of children being educated and cared for by the service
- obtaining authorisation from parents to take, use and store images and videos of children being educated and cared for by the service
- the use of any optical surveillance device at the service (e.g. closed-circuit television)
- the use of any digital device issued by the service
- the use of digital devices by children being educated and cared for by the service.

1. Title

Safe use of digital technologies and online environments procedures

2. Reference to policy and philosophy

Here you refer to *Safe use of digital technologies and online environments policy* as seen in your policy documents. You can reference where you will find the policy to help those looking for it.

Your procedure will also reflect your service's overall philosophy and any supervision and action plans for specific children.

3. Procedures

This is where you detail the way you will implement the *Safe use of digital technologies and online environments policy*.

It is the 'How to' in your service and includes specific step-by-step procedures for the safe use of digital technologies and online environments. Some areas that will be outlined here will include:

- where the procedures will be kept
- when they were last reviewed
- templates or documents that might be required and/or used as a part of the procedure (e.g. online safety self-assessment and risk assessment forms)
- systems to monitor the implementation of procedures.

When developing your procedures you will need to consider current legislation in your state or territory in relation to child protection and online safety, and ensure that all educators and staff, including volunteers and students, understand how to report their concerns about child protection issues and child abuse.

You may also need to consider other procedures and how they may need to be adjusted in relation to the *Safe use of digital technologies and online environments procedures*. For example, consider how procedures for staffing include measures for supervising visitors to ensure that they do not take images or videos of children without the appropriate authorisation by parents/carers.

As you reflect on the *Safe use of digital technologies and online environments procedures*, consider any need to split its various areas into different procedures, which will be displayed or accessed by educators and staff to follow. For example, you may wish to have separate procedures for Online supervision, Reporting online child abuse, Using electronic devices safely, and Collecting, storing and sharing personal information.

4. Roles and responsibilities

This is where you will designate specific roles and responsibilities for the people who hold different positions within your service. This needs to align with the *Education and Care Services National Law* and *Education and Care Services National Regulations* (see below).

It is important to note that it is the legal responsibility of approved providers to ensure systems are in place to minimise risk, and that procedures are implemented by the responsible people in services, including family day care (FDC) environments (if applicable). This is required as a reasonable precaution to protect children from harm and hazards. Ultimate responsibility lies with the approved provider to ensure every service they operate is meeting the requirements under the *Education and Care Services National Law*.

- When developing this section consider the following questions:
- what are the roles and responsibilities of the approved provider, nominated supervisor, educators, other staff, volunteers, students and families in your service in relation to the safe use of digital technologies and online environments at the service?
 - how will you clearly define these roles and expectations and where will they be documented?
 - why are clear and robust procedures for the safe use of digital technologies and online environments at the service important for children’s safety, health and wellbeing?
 - how will you learn from the administration of these procedures to improve your practices?
 - how will you ensure that the necessary tools are available so the approved provider, nominated supervisor, educators and other staff members can follow the procedures? How will they be made aware of the procedures?
 - do the roles and responsibilities reflect your service type?
 - how do you ensure all involved in the service, including the approved provider, nominated supervisor, educators, other staff members, volunteers, students and families understand the National Model Code and the service’s expectations for the use of electronic and digital devices for taking images or videos of children at the service?

An example of roles and responsibilities could include, but is not limited to:

Roles	Responsibilities
Approved provider	<ul style="list-style-type: none">• ensure that obligations under the <i>Education and Care Services National Law</i> and <i>National Regulations</i> are met• ensure that the <i>Safe use of digital technologies and online environments policy and procedures</i> are implemented, the appropriate risk assessments and action plans are completed, and all identified actions are taken to minimise the risks to children’s health and safety• promote a culture of child safety and wellbeing that underpins all aspects of the service’s operations (including online learning environments), to reduce risk to children (including the risk of abuse)• ensure the safe use of digital technologies, including smart toys, and online environments at the service• ensure nominated supervisors, educators and staff implement practices that align with the National Model Code and the service’s child safe practices for the use of electronic and digital devices for taking images or videos of children• ensure policies and procedures promote equity and respect diversity for the safety and wellbeing of children and young people• take reasonable steps to ensure that nominated supervisors, educators and staff follow the <i>Safe use of digital technologies and online environments policy and procedures</i>• ensure that copies of the policy and procedures are readily accessible to nominated supervisors, coordinators, educators, staff, families, and are available for inspection• notify families at least 14 days before changing the policy or procedures if the changes will:<ul style="list-style-type: none">» affect the fees charged or the way they are collected or» significantly impact the service’s education and care of children or» significantly impact the family’s ability to utilise the service.

Roles	Responsibilities
Nominated supervisor	<ul style="list-style-type: none"> • implement the <i>Safe use of digital technologies and online environments policy and procedures</i> and ensure that any plans developed from risk assessments are in place for individual children and are carried out • ensure staff understand how to actively supervise children while using digital technologies • meeting staff to child ratios to ensure adequate supervision • ensure all educators and staff know where to access the <i>Safe use of digital technologies and online environments policy and procedures</i> • have ongoing communication with educators and staff about their responsibilities and any changes to policies, procedures and legislation, particularly as digital technologies evolve quickly • support educators and staff to uphold the service's culture of child safety and wellbeing, including when accessing digital technologies and online learning environments • support educators and staff to understand the National Model Code and manage the use of electronic and digital devices at the service, including the service's expectations around the use of personal and service issued devices • when required, work collaboratively with appropriate services and/or professionals to support children's access, inclusion and participation in the program, including their safe access to online learning environments..
Educators	<ul style="list-style-type: none"> • implement the <i>Safe use of digital technologies and online environments policy and procedures</i> and ensure that any action plans for individual children are carried out • implement the service's culture of child safety and wellbeing, including when accessing digital technologies and online learning environments • know the individual needs and action plans for the children in your care, and understand how they relate to the safe use of digital technologies and online environments • ensure active supervision of children when they are using digital technologies, including by monitoring and maintaining staff to child ratios • recognise and respond effectively to children and young people when discussing the use of digital technologies and online environments, considering diverse needs and interests • ensure children and young people participate in decision-making in matters affecting them regarding the safe use of digital technologies and online environments at the service • ensure you understand the National Model Code and the service's expectations around the use of personal and service issued devices while at the service, and seek guidance when needed from the nominated supervisor or approved provider.

The following table will assist you in developing procedures specific to your service's needs and context. Referring to the *Education and Care Services National Regulations* when you are writing your procedures will assist you to ensure that you are meeting your obligations. More information and tools, including the NQF Online Safety Self-assessment and risk assessment tool, are available in the NQF Online Safety Guide.

Areas to include in your procedures	Things to consider and outline in each area (this will be specific to the context of your service)	Strategies for monitoring and implementing procedures	Related policy and/or procedures
Safe use of digital technologies and online environments Act: 165, 167 Regs: 168, 169, 170, 171, 172, 175, 176 QA2: 2.2.1, 2.2.3 QA3: 3.1.1, 3.1.2 QA5: 5.1.1, 5.2.2 QA7: 7.1.1, 7.1.2	<ul style="list-style-type: none"> • How will you ensure your service's organisational culture prioritises children's safety through the safe use of digital technologies and online environments for children's learning? • How will you ensure you are safely using digital technologies and online environments? • How do you intend to set up digital and online learning environments to support the safety and wellbeing of children? • How will you undertake risk assessments and action plans that will identify potential risks with digital technologies and online environments, and minimise any risks without compromising a child's right to privacy, access to information, social connections and learning opportunities? How regularly will you undertake these assessments and renew action plans? • What precautions may be necessary to protect the safety, health and wellbeing of children when using digital technologies and online environments? • How do practices and procedures inform children and their families in culturally appropriate ways, about the use of digital technologies and online environments at the service? • How will you monitor the amount and quality of screen time children have at the service? 	<ul style="list-style-type: none"> • Ensure your policy and procedures are available for all to access. • Ensure cyber security procedures are kept up to date and followed. • Ensure self and risk assessments are carried out, reviewed and updated as required. • Develop and implement plans as a result of self and risk assessments. • Consider using a safety checklist for digital technologies and online environments. • Provide educator and staff induction training on the safe use of digital technologies and online environments, and include regular updates and reviews at team meetings. • Provide guidance on the use of electronic and digital devices in the service for all staff using the National Model Code, including the reflection questions within the Guidelines. • Regularly reflect on supervision strategies to ensure they are effective for the use of digital technologies and online environments at your service. • Review current guidance on screen time and speak to families about the amount and nature of screen time their children have at home and at the service. 	<ul style="list-style-type: none"> • Incident, injury, trauma and illness • Interactions with children • Staffing • Governance and management

Areas to include in your procedures	Things to consider and outline in each area (this will be specific to the context of your service)	Strategies for monitoring and implementing procedures	Related policy and/or procedures
<p>The taking, use, storage and destruction of images and videos of children being educated and cared for by the service, and obtaining authorisation from parents to do so</p> <p>Act: 165, 167</p> <p>Regs: 168, 169, 170, 171, 172, 175, 176</p> <p>QA2: 2.2.1, 2.2.3</p> <p>QA3: 3.1.1, 3.1.2</p> <p>QA5: 5.1.1, 5.2.2</p> <p>QA7: 7.1.1, 7.1.2</p>	<ul style="list-style-type: none"> • How will you ensure you are safely taking, using, storing, and when required, destroying images and videos of children being educated and cared for by the service? • What procedures and security practices are in place to ensure only the appropriate staff at the service have access to the relevant images and videos of children? • How will you ensure you are obtaining authorisation from parents to take, use, store and destroy images and videos of children being educated and cared for by the service? • What practices and processes are in place for involving children in decisions about their images and provide information about consent in ways they understand? This helps teach online safety practices, builds their independence, and respects their rights. • How will you help children and families understand that consent can be withdrawn at any stage? • What practices and process are in place for explaining to families how children's images will be used, accessed, stored and destroyed, and explain to families how they can change or revoke their consent? 	<ul style="list-style-type: none"> • Ensure your policy and procedures are available for all to access. • Provide educator and staff induction training on the taking, use, storage and destruction of images and videos of children being educated and cared for by the service, and include regular updates and reviews at team meetings. • Provide guidance on when it is appropriate to take an image or video of a child and how to consider the purpose for why it is being taken. For example, use the reflective questions within the Guidelines of the National Model Code to consider how often and when to take relevant images of a child. • Ensure policies respect children's privacy and support their independence. • Get written consent from families for taking or recording images of their child. • Review any relevant state, territory or federal privacy laws that apply in your jurisdiction. 	<ul style="list-style-type: none"> • Interactions with children • Staffing • Governance and management

Areas to include in your procedures	Things to consider and outline in each area (this will be specific to the context of your service)	Strategies for monitoring and implementing procedures	Related policy and/or procedures
<p>The use of any optical surveillance device at the service (e.g. closed-circuit television)</p> <p>Act: 165, 167</p> <p>Regs: 168, 169, 170, 171, 172, 175</p> <p>QA2: 2.2.1, 2.2.3</p> <p>QA3: 3.1.1, 3.1.2</p> <p>QA5: 5.1.1, 5.2.2</p> <p>QA7: 7.1.1, 7.1.2</p>	<ul style="list-style-type: none"> • What type of optical surveillance devices are used at the service? E.g. closed-circuit television, baby monitors, etc. • What practices and procedures are in place for safely using the service's optical surveillance devices? • What processes are in place for ensuring optical surveillance devices are not in places where people expect privacy, like children's bathrooms? • How do you intend to ensure compliance with privacy laws and workplace surveillance rules for any personal information that is collected? • How will you decide who within the service needs access to the footage collected by a device and how long it will be retained for? 	<ul style="list-style-type: none"> • Provide educator and staff induction training on the use of optical surveillance devices, and include regular updates and reviews at team meetings. • Review guidance about the use of optical surveillance devices (including security cameras), such as information that has been developed by the Office of the Australian Information Commissioner. • Teach everyone why and how optical surveillance devices (including security 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 footage and have measures in place to prevent unauthorised access. • Check which state/territory and federal laws apply to using optional surveillance devices, including security cameras. 	<ul style="list-style-type: none"> • Interactions with children • Staffing • Governance and management

5. Procedures created/reviewed

Include the date the procedures were created or reviewed.

6. Monitoring, evaluation and review

Your service, in consultation with educators and other key staff, families and other stakeholders, should review the effectiveness of this procedure within a set timeframe or earlier if there is a change in relevant legislation.

State when the procedure will be reviewed and who will be responsible for this. All procedures need to be monitored and reviewed regularly to ensure that they are up to date and compliant with the National Law and National Regulations. Your procedures should record the dates they have been reviewed or when changes were made, as well as the next review date. In the event of a revision or change of procedure, you will need to ensure educators and families are made aware of the changes and the revised procedure, removing access to electronic or hardcopies of the older versions. Follow appropriate record-keeping processes for each updated version of the procedures.

7. Checklist

Do the *Safe use of digital technologies and online environments procedures* align with your *Safe use of digital technologies and online environments policy*?

How do your procedures reflect the National Model Code and Guidelines for the taking of images and videos and use of electronic and digital devices at the service?

Have your procedures been written in plain English and can they be easily implemented by an educator or staff member new to your service?

Have your policy and procedures been communicated to families? Is it clear who is responsible for the implementation of the procedures?

Are all educators and other staff aware of the procedures and can implement them if required?

Do you need to develop any resources to monitor and record the procedure?

REFERENCES AND RESOURCES

Include links to useful resources that have helped inform the development of your policy. Be mindful of any state or territory specific content.

Some examples include, but are not limited to:

- [ACECQA Guide to the National Quality Framework](#)
- [ACECQA – NQF Child Safe Culture Guide](#)
- [ACECQA – NQF Online Safety Guide](#)
- [ACECQA – National Model Code – Taking images in early childhood education and care](#)
- [ACECQA – Children’s rights in their digital footprints](#)
- [ACECQA – The endless possibilities of using digital devices in OSHC safely](#)
- [ACECQA – Using digital touch technologies to support children’s learning](#)
- [ACECQA – Digital documentation for families – quality or quantity?](#)
- [ACECQA – Digital technology in educational program and practice](#)
- [eSafety Commissioner](#)
- [Office of Australian Information Commissioner](#)
- [PlayingITSafe](#)
- [ThinkUKnow](#)
- [Digital Child](#)
- [Young Children in Digital Society](#)
- [The Alannah & Madeline Foundation](#)
- [The Carly Ryan Foundation](#)