



RISK MANAGEMENT TOOL – DIGITAL DEVICES

QUALITY AREA 2 & 7 | ELAA version 1.0

INTRODUCTION

Digital devices are now part of everyday practice in Early Childhood Education and Care (ECEC). While they provide opportunities for learning, documentation, and communication, they also bring risks. Services need a clear and consistent approach to identify, assess, and manage these risks. This tool supports services to integrate the National Model Code for Taking Images or Videos of Children while Providing Early Childhood Education and Care (National Model Code) into daily delivery, as well as the Occupational Health and Safety Act 2004 (OHS Act 2004) and industrial relations (IR) legislation requirements and ensure children's safety, privacy, and wellbeing remain the priority.

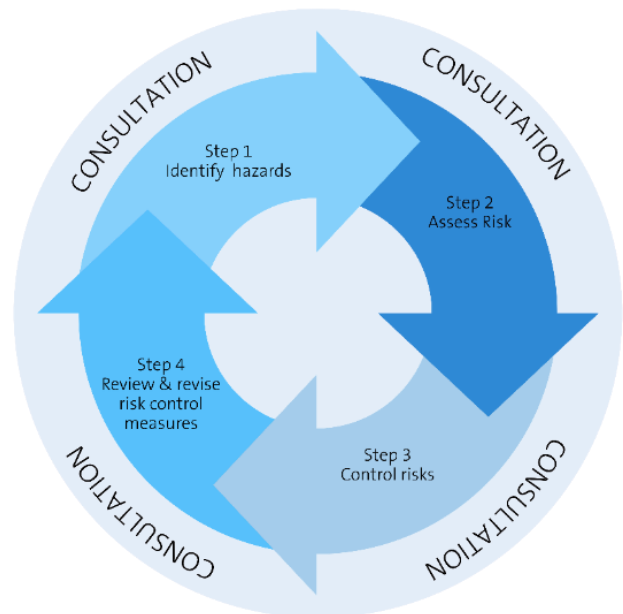
A clear risk management process helps services identify potential harms, gaps, and unintended consequences. By understanding risks, services can put safeguards in place, reduce liability, and protect children, staff, and families. Risk management also builds transparency, consistency, and continuous improvement across service delivery.

RISK MANAGEMENT

Risk management is a proactive process that helps services identify potential risks, assess, control and monitor the risks to reduce the chance or impact of something harmful happening. In the context of digital devices, this means planning how and why devices are used and considering a risk benefit analysis for their use. Other considerations can include how they are stored and accessed to prevent any harm occurring as a result of their use.

Services also need to consider concerns about hidden cameras and stealth recording devices. As technology becomes smaller and harder to detect, the risks to children, families, and staff increase. Strong risk management that keeps pace with these developments is essential. Services require clear procedures, regular reviews, and active monitoring to respond quickly when new technology emerges.

Risk Management Process Overview



Consultation

Consultation is the process of gathering feedback and information to guide decisions about how digital devices are used safely. It is a key part of child safety risk management process. Consultation is also a requirement under the OHS Act 2004.

Consulting leaders, teachers, educators, and staff is essential to understand the services' culture around identifying, monitoring, and managing risks linked to devices. When leaders treat device safety as a priority, it strengthens the whole risk management system.

Consulting with children helps you understand what makes them feel safe or unsafe when devices are used to capture or store their images. Their views can inform clear rules about photographing, recording, and sharing information.

Why is consultation important?

- It brings together expertise from different areas for every stage of risk management
- It ensures all views are considered when defining risks and setting controls for devices
- It ensures employees' perspectives are included, increasing the likelihood they will report hazards to employers.

Consultation provides the information needed for oversight and sound decision-making. It builds a sense of ownership among everyone affected by risks, encouraging shared responsibility for safe use of digital devices.

Identify the hazards

Services should prioritise identifying hazards before they use or introduce a new digital device. Preventing hazards is more effective than addressing problems after they arise.

In ECEC, identifying hazards involves more than recognising obvious risks. It also requires understanding the potential harm each hazard could cause to children, staff, or visitors.

Services should take a comprehensive approach to all potential risks across different scenarios involving the introduction and use of digital devices, ensuring each identified hazard is assessed and appropriately addressed.

Psychosocial hazards

A psychosocial hazard is anything in the workplace that could cause staff to have a negative psychological response. This can lead to mental or physical harm, or both.

In ECEC, staff may experience stress from workload, challenging behaviours, or workplace culture. Stress is not a psychological injury on its own, but frequent, prolonged, or severe stress can cause harm.

Some examples the teachers and educators can experience can include but not limited to:

- Fear of making mistakes when storing or sharing children's images or personal data.
- Anxiety over privacy breaches or unauthorised access to children's information.
- Reduced work-life balance if work-related messages are expected to be answered outside hours.
- Pressure to learn new systems and keep up with technology changes.

Risk assessment

Risk is the possibility of harm when children, educators, or visitors are exposed to a hazard. In ECEC, digital devices can pose risks to privacy, wellbeing, and safety. Risk assessment involves identifying:

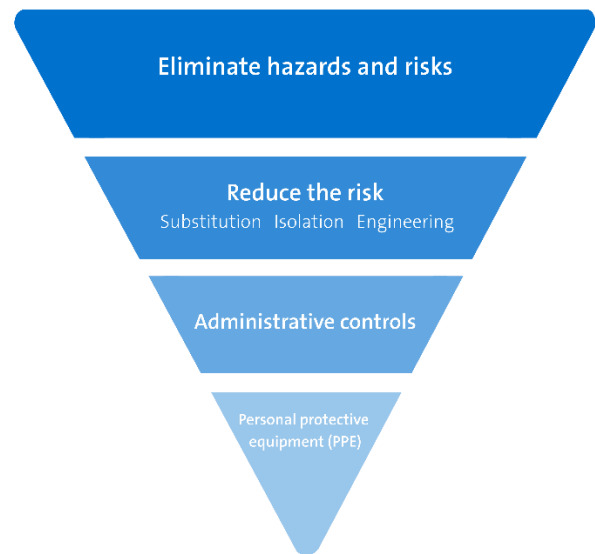
- What harm could occur (e.g., data breaches, inappropriate content exposure, device misuse).
- How harm could occur (e.g., unsupervised use, unsecured devices, sharing of images).
- How likely the harm is to occur.

Control risks

Once hazards and risks have been identified and assessed, the next step is to implement control measures. Control measures are actions or strategies that eliminate or reduce the risks to children, staff, and visitors. This step ensures the service actively manages risks and creates a safer environment for everyone. When implementing control measures, the service should prioritise actions by considering how severe and immediate the risk is, who is affected, how easily it can be controlled, and any additional benefits of managing the risk.

Hierarchy of control

When considering hazards and their risks in ECEC services, the hierarchy of control provides a clear approach to managing risks. The most effective step is to eliminate hazards, such as removing unsafe or unnecessary digital platforms. If **elimination** is not possible, risks can be reduced by **substituting** high-risk platforms with secure alternatives, **isolating** access so only authorised staff use devices, or applying **engineering** controls like password protection and firewalls. **Administrative controls**, such as policies on screen time, data use, and supervision, help minimise exposure but are less reliable on their own. The lowest level of control is **personal protective equipment**, such as using device filters or protective cases, which may help but do not address the core risks. This structured approach ensures digital devices used supports children's learning while keeping safety and privacy a priority.



It is important for service to identify as many risk control measures as possible. Reducing the risk might involve a single risk control measure or a combination of different control measures that work together to provide the highest level of protection.

At the end of the risk control process, the service should have:

- Identified as many risk control measures as possible that eliminate or reduce risks
- Reviewed any risk controls currently in place and assessed their effectiveness at controlling the risks
- Put those practical measures in place to manage the risks.

Services must keep staff informed of any changes to work practices, including new controls from the risk plan. Staff should receive the information, instruction, and training needed to work safely. Records of training should be maintained, and work practices reviewed regularly.

Staff and health and safety representatives must be consulted when:

- Identifying or assessing hazards and risks
- Deciding how hazards and risks will be controlled.

Monitor and review

The service must monitor and review health and safety controls to ensure they are effective. Monitoring should be ongoing, and reviews should be scheduled. When issues arise, risk controls should be revised promptly with processes to identify and address problems quickly.

Regular checks should identify failures or faults in control measures. Reviews should be carried out with staff and any health and safety representatives before significant changes, after injuries or near misses, and when new information about hazards or risks becomes available

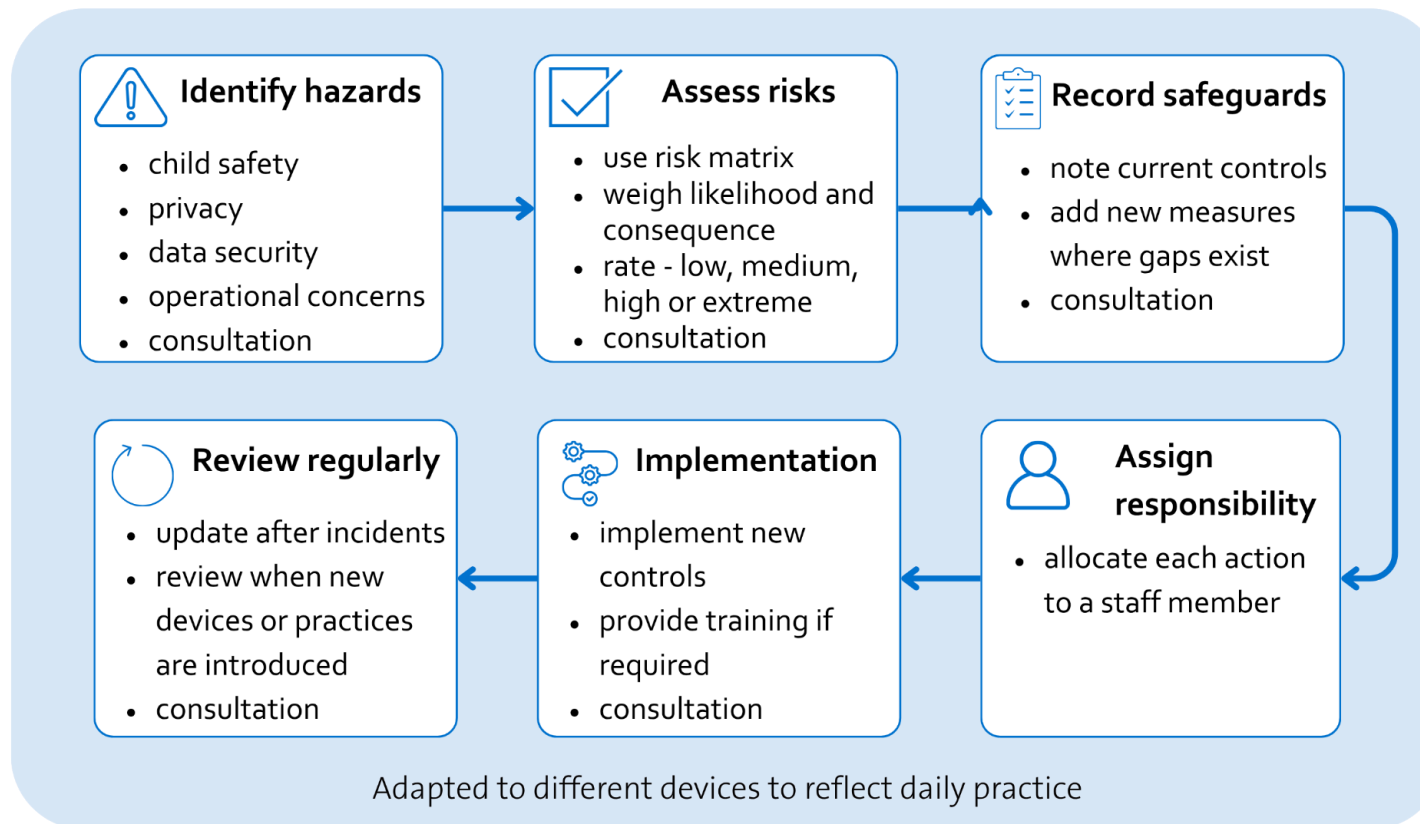
KEY POINTS TO REMEMBER

Risk assessment and management are ongoing parts of daily practice. This tool is designed as a starting point to guide your service but should be adapted to fit your own context. By embedding the process into everyday operations, services can ensure digital device use supports children's learning while keeping them safe. Each digital device that can take or store images of children must have its own risk management plan. Consultation with staff is essential when developing and reviewing these plans. Regular review and monitoring will ensure the plans remain effective and relevant.

RISK MANAGEMENT TOOL VIDEO GUIDE

This video shows you how to use the Risk Management Tool in practice. It walks you through each step of the process and explains how to identify, assess, and manage risks within your service. The video was created to support the tool and help committees, leaders, and staff apply risk management in a clear and practical way - <https://elaa.org.au/training/video-library/risk-management-for-early-childhood-services>

HOW TO USE THIS TOOL



Risk Management Plan

Type of digital device:

Date:

What will the digital device to be used:

Who will be using the digital device?

Identify hazards – *What are the potential hazards (including psychosocial hazards) and scenarios in the use of this device which could cause harm?*

-

Assess risks – Likelihood and severity – *Refer to the risk matrix*

Hazard	Likelihood	Severity of harm	Risk rating

Consultation has been undertaken ☐ Yes ☐ No Date/s:

Risk Management Plan

Manage risks – *Detail how the risk of harm will now be managed?*

Hazard	Risk level	Applying hierarchy of controls	Controls to manage harm	Responsible person
		☐ Elimination ☐ Substitution ☐ Isolation ☐ Engineering ☐ Administrative controls		
		☐ Elimination ☐ Substitution ☐ Isolation ☐ Engineering ☐ Administrative controls		
		☐ Elimination ☐ Substitution ☐ Isolation ☐ Engineering ☐ Administrative controls		
		☐ Elimination ☐ Substitution ☐ Isolation ☐ Engineering ☐ Administrative controls		
		☐ Elimination ☐ Substitution ☐ Isolation ☐ Engineering ☐ Administrative controls		
		☐ Elimination ☐ Substitution ☐ Isolation ☐ Engineering ☐ Administrative controls		
		☐ Elimination ☐ Substitution ☐ Isolation ☐ Engineering ☐ Administrative controls		

Consultation has been undertaken ☐ Yes ☐ No Date/s:

Training of the controls

Risk Management Plan

Implementation of the controls

Evaluation and review – Risk management – *How effective were the controls for managing the risk of harm? What were the positive and negative outcomes of the device use?*

Developed by (full name and signature):

In consultation with (full name and signature):

Evaluated by (full name and signature):

Date of evaluation:

Risk Matrix

Consequences	Likelihood					
		Rare	Unlikely	Possible	Likely	Almost Certain
	Major	Moderate	High	High	Critical	Critical
	Significant	Moderate	Moderate	High	High	Critical
	Moderate	Low	Moderate	Moderate	High	High
	Minor	Very low	Low	Moderate	Moderate	Moderate
	Insignificant	Very low	Very low	Low	Moderate	Moderate

RISK LIKELIHOOD

The Likelihood Rating table is used to determine the chance of a risk event occurring.

Rating	Description	Frequency
Almost Certain	The event is expected to occur	Multiple times per year
Likely	The event will probably occur	Once per year
Possible	The event might occur	Once every 5 years
Unlikely	The event is unlikely to occur	One every 10 years
Rare	The event may occur in exceptional circumstances	Once every 20 years

Below is a list of examples for you to consider when developing your risk management plan. This list is provided as a guide only and does not cover every possible risk.

Digital devices	Hazards	Risks
Mobile devices - Smartphones (iPhone, Samsung Galaxy, Google Pixel, etc.) - Tablets (iPad, Samsung Galaxy Tab, Lenovo, etc.) - Smartwatches with cameras (Apple Watch with camera bands, specialised children's watches) Computers and laptops - Desktop computers with webcams - Laptops with built-in webcams - External webcams connected to PCs 2-in-1 laptops with cameras (Microsoft Surface, Chromebooks, etc.) Cameras and video recorders - Digital cameras (DSLR, mirrorless, point-and-shoot) - Video cameras and camcorders - Action cameras (GoPro, DJI Osmo, Insta360) - Compact handheld video recorders Storage media and accessories - USB flash drives - External hard drives - Network attached storage (NAS) devices - SD cards and microSD cards - CDs, DVDs, Blu-ray discs Online and cloud-based storage - Cloud platforms (Google Drive, Dropbox, OneDrive, iCloud)	Privacy and security hazards - Unauthorised access if devices are not password-protected - Hacking or malware compromising devices - Data breaches exposing stored images - Cloud storage leaks or misconfigurations - Loss or theft of device leading to unauthorised use of images - Weak or shared passwords on devices and apps - Auto-backups to personal accounts without consent - Insecure Wi-Fi connections during uploads Misuse and inappropriate sharing hazards - Unauthorised sharing on social media - Staff or visitors using personal devices to take images - Accidental posting or sending of images to the wrong person - Misuse of messaging apps where images are forwarded without consent - Use of images for unintended purposes (e.g. advertising without permission) - Lack of control once images are shared outside the service Storage and retention hazards - Images stored longer than required - Images stored on personal devices instead of secure service systems - Images stored on unencrypted USBs, SD cards, or hard drives	Privacy and security risks - Children's personal information and images accessed by unauthorised people - Identity theft if images are linked with names or details - Families losing control of how their child's image is used - Service breaching privacy laws and facing fines or investigations Misuse and inappropriate sharing risks - Images posted on public platforms without consent - Images used in contexts that could embarrass or distress children - Photos distributed beyond the intended audience (e.g. parents only) - Images accessed or exploited by individuals with harmful intent Storage and retention risks - Accumulation of large, unmanaged image libraries with sensitive data - Insecure storage leading to leaks or data loss - Old staff retaining access to children's images after leaving the service - No way to confirm if images have been permanently deleted Operational risks - Inconsistent practices across staff creating uneven protection levels

• Photo storage services (Google Photos, Amazon Photos, Flickr) • Messaging apps storing images (WhatsApp, Messenger, Signal, Telegram, WeChat) • Social media platforms (Facebook, Instagram, TikTok, Snapchat, X/Twitter) Educational and service-based platforms • Storypark • Seesaw • Xplor • Educa	• Forgotten images left in device galleries, recycle bins, or caches • Automatic syncing between personal and work devices Operational hazards • Staff confusion about policies on device use • No clear procedure on which devices are approved for use • Inconsistent use of service-owned vs personal devices • Difficulty tracking where images are stored across multiple platforms • Lack of audit trail on who accessed or used images Legal and compliance hazards • Breach of the Privacy Act or relevant child protection laws • Breach of service policies or agreements with families • Lack of parental consent for image use • Use of images beyond agreed purposes (e.g. educational vs promotional) • Exposure to complaints, investigations, or penalties Child safety hazards • Images falling into the hands of individuals with harmful intent • Geotagging or location metadata exposing children's whereabouts • Video or livestream functions showing sensitive environments • Risk of images being altered, misused, or distributed in unsafe ways Psychosocial Hazards	• Staff unintentionally breaching policy by using personal devices • Gaps in training leading to unsafe handling of images • Time and resources wasted trying to locate or recover images Legal and compliance risks • Non-compliance with National Law, National Regulations, or the Privacy Act • Regulatory action from ACECQA or state/territory authorities • Legal claims from families for misuse of images • Breach of service agreements with families Child safety risks • Children's locations revealed through geotagged images • Photos shared outside the service placing children at risk of grooming or exploitation • Children made identifiable in sensitive contexts (e.g. toileting, accidents) • Risk to vulnerable children in protective custody if images are exposed Psychosocial risks • Reduced concentration leads to lower quality work. • Heightened stress affects decision making. • Feelings of surveillance reduce trust. • Uncertainty with systems increases anxiety. • Exposure to online aggression damages confidence. • Rushed decisions increase error rates. • Fear of mistakes creates ongoing stress.
---	---	---

	• Staff face constant notifications that interrupt focus. • Staff manage high email volume that creates pressure to respond quickly. • Monitoring tools make staff feel watched. • Limited training leaves staff unsure how to use required systems. • Staff receive online aggression from parents or stakeholders. • Staff face pressure to approve image use quickly for events or marketing. • Staff fear making an error when managing consent. • Staff experience conflict with colleagues about when images can be used. • Confusing privacy requirements increase mental load. • Staff manage emotional strain when parents disagree about image use. • Staff worry about legal consequences if an image is shared without consent. •	• Conflicts with colleagues impact workplace culture. • Confusion about requirements leads to inconsistent practice. • Tense interactions with parents affect wellbeing. • Worry about legal outcomes reduces confidence in daily tasks.
--	--	---