SAFE USE OF DIGITAL TECHNOLOGIES & ONLINE ENVIRONMENTS PROCEDURE

Statement of Procedure

At Fun 4 U OSHC, we are committed to ensuring that all children, educators, staff, visitors, volunteers, students, and families engage with digital technologies and online environments in a safe, responsible, and respectful manner. In accordance with Education and Care Services National Regulation 168(2)(ha), our Service maintains and implements robust policies, procedures, risk assessments, and authorisations to ensure they address the safe use of digital technology and online environments, by outlining:

- How to take, use, store, and destroy images and videos of children in accordance with the National Model Code and Guidelines, privacy legislation, and service-specific authorisations.
- Obtain and document authorisations from families for digital technology use, image capture, storage, and sharing.
- Ensure transparency with families and staff regarding the use of digital devices, including clear signage and communication about service-issued devices and any recording or image-taking equipment.
- Establish expectations for appropriate and restricted use of all digital devices within the Service, including service-issued and personal devices, and ensure secure handling of all digital data.
- Implement age-appropriate and supervised technology use for children.
- Identify, assess, and manage risks related to digital technology and online environments, ensuring strategies are in place to protect children from harm while supporting their learning, creativity, and access to information.
- Maintain compliance with relevant state, territory, and federal legislation, including privacy, data security, and child protection requirements.

All staff, educators, and volunteers are responsible for following this procedure and for modelling safe and respectful use of digital technologies at all times. Families will be informed

of these procedures upon enrolment and whenever updates are made. This policy can be found on Fun 4 U's main computer desktop – files – policies and procedures, on our Facebook page and next to our sign in and out register we have a folder with a QR code to each policy.

Safe Use of Digital Technologies and Online Environments Procedure:

Education and Care Services National Regulations
Quality Area 2: 2.2, 2.2.1, 2.2.3 Quality Area 4: 4.2.2 Quality Area 5: 5.1, 5.1.2 Quality Area 7: 7.1.2 Regs: S.162A, S.165, S.167, 12, 73, 76, 84, 115, 122, 123, 149, 155, 156, 168, 168 (h), 170-172, 175, 176, 181, 183, 184
Outlines of how Fun 4 U's organisational culture priorities child safety throughout our services in reflection of legislation: Safe Use of Technologies and Online Environments
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? At Fun 4 U OSHC, we embed the National Principles for Child Safe Organisations into all practices, ensuring that digital technology is used in a way that upholds children's safety, dignity, and wellbeing. Staff are trained to actively supervise all online interactions, model safe and respectful digital behaviour, and encourage open conversations with children about online safety. Our organisational culture prioritises children's voices, ensuring they are consulted on how technology is used while reinforcing that safety always comes first.
How will you ensure you are safely using digital technologies and online environments? We use only secure, password-protected, service-issued devices for online activities that only the staff access at Fun 4 U. All apps, programs, and websites are pre-approved by management and regularly reviewed. Devices are configured with filtering and monitoring software to prevent access to unsafe or inappropriate content. Staff receive regular training in online safety, privacy protection, and incident response, ensuring consistent application of safe practices.

How do you intend to set up digital and online learning environments to support the safety and wellbeing of children?

All of our service issued devices are used in open, visible areas, never in isolated or unsupervised spaces. Digital activities are planned with educational intent and linked to "My Time, Our Place" learning outcomes. Equipment placement avoids "blind spots" and supports easy line-of-sight supervision by multiple educators. We integrate cyber safety education into our program, empowering children to make safe and informed online choices even though children are not permitted on their own digital devices at Fun 4 U.

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?

Risk assessments will be completed for all digital activities, including evaluating the suitability of apps, websites, and platforms. These assessments will address privacy risks, cyberbullying potential, data security, and exposure to inappropriate content. Action plans will outline steps to mitigate identified risks while maintaining children's access to safe and beneficial digital learning. Assessments will be reviewed annually, and sooner if a new technology is introduced, a security breach occurs, or an incident is reported.

What precautions may be necessary to protect the safety, health and wellbeing of children when using digital technologies and online environments?

Precautions include:

- Limiting screen time in line with Australia's Physical Activity and Sedentary Behaviour Guidelines
- Ensuring children's personal information (name, age, location) is never shared online
- Using content filters and disabling in-app purchases
- Supervising all online use to prevent access to harmful content or unsafe interactions
- Providing regular breaks to avoid eye strain and fatigue
- Having a clear procedure for responding to incidents such as exposure to inappropriate content or online abuse

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?

We provide families with our Safe Use of Technologies and Online Environments Policy during enrolment and discuss it during orientation, ensuring the language is clear, respectful, and culturally inclusive. For families who speak English as an additional language, we offer translated materials or visual guides where possible. Children are informed through group discussions and visual posters that encourage questions and input.

How will you monitor the amount and quality of screen time children have at the service?

Educators maintain a daily log of children's screen time to ensure it does not exceed recommended limits and is balanced with physical play, creative activities, and social interaction. We prioritise educational, interactive, and creative uses of technology over passive entertainment. Regular reviews of the program ensure technology use aligns with learning outcomes and supports children's wellbeing.

Strategies for Monitoring and Implementing Procedures

- 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.

Related Policy and/or Procedures
• Child Protection Policy & Procedure • Governance and Management of the Service Including Confidentiality of Records • Incident, Injury, Trauma and Illness • Providing a Child Safe Environment • Staffing Code of Conduct

Outlines of how Fun 4 U's organisational culture priorities child safety throughout our services in reflection of legislation: <u>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.</u>
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? At Fun 4 U, all images and videos of children will only be taken on service-issued, password-protected devices. The purpose of each image or video will be directly linked to educational documentation, service promotion (if consent is provided), or safety and compliance requirements. Images and videos will be stored securely on encrypted, access-controlled systems and backed up in secure, cloud-based storage. When images or videos are no longer required, they will be deleted in line with the *Governance and Management of the Service Including Confidentiality of Records Policy*, ensuring permanent removal from all devices, storage drives, and backup systems.
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? Only authorised staff, approved by the nominated supervisor or approved provider, will have access to stored images and videos. User accounts are password-protected, access permissions are regularly reviewed, and any staff leaving the service will have access immediately revoked. Transfers of files are prohibited to personal devices or storage systems. All devices are set to lock automatically when unattended.

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? Families are required to complete and sign a Photography and Video Consent Form upon enrolment, specifying whether they grant permission for their child's image or video to be taken, the purposes for which it can be used, and the methods of storage and destruction. This consent form is reviewed annually or when a change in circumstances occurs. No images or videos will be taken or used without prior written authorisation from the child's parent/guardian.
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. Educators will explain to children—in age-appropriate language—why their photo or video is being taken, where it might appear, and who might see it. Children will be asked for their verbal consent before taking an image or video, even if parental consent is on file. We encourage children to voice their preferences and respect their decisions, supporting their independence and teaching online safety principles.
How will you help children and families understand that consent can be withdrawn at any stage? Families are informed in writing, both on the consent form and in the parent handbook, that they may withdraw consent at any time by providing written notice to the service. Children are regularly reminded that if they no longer want their photo or video used, they can tell an educator, who will inform the nominated supervisor to remove or delete the material immediately.
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? During enrolment and orientation, families are given a clear explanation of how images and videos are captured, where they are stored, how they are accessed, and the process for eventual destruction. This information is also included in the Safe Use of Digital Technologies and Online Environments Policy, available on our parent communication platform and at the service. Families are shown examples of secure storage practices and are reminded they may

change or revoke their consent at any time, in which case all relevant images or videos will be removed from the service's storage systems.

Strategies for Monitoring and Implementing Procedures

- 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.

Related Policy and/or Procedures

- Child Protection Policy & Procedure
- Governance and Management of the Service Including Confidentiality of Records
- Providing a Child Safe Environment
- Staffing Code of Conduct

RISK ASSESSMENT

1. The approved provider and nominated supervisor will conduct a comprehensive risk assessment regarding the safe use of digital technology and online environments by children and staff, identifying potential risks, implementing appropriate controls and ensuring supervision and protective measures are in place
2. The risk assessment will be developed in consultation with educators, families and, where possible, children
3. The approved provider and nominated supervisor will review the risk assessment for safe use of digital technology and online environments is reviewed at least once every 12 months

4. The approved provider and nominated supervisor will review the risk assessment following any incident or circumstance where the health, safety or wellbeing of children may be compromised
5. If a risk concerning a child's safety and wellbeing is identified during the risk assessment, the approved provider and nominated supervisor will update the *Safe Use of Digital Technologies and Online Environments Policy* and procedure as soon as possible
6. The approved provider and nominated supervisor will ensure the *Safe Use of Digital Technologies and Online Environments Risk Assessment* is stored safely and securely and kept for a period of 3 years

Images and Videos – Authorisation and Use

1. Photos/videos will only be taken on service-issued devices.
2. Parent/guardian authorisation will be obtained prior to capturing or using children's images/videos.
3. Children's consent will also be sought in an age-appropriate way.
4. Images/videos will be stored securely and deleted when no longer required.
5. Families will be informed if images are used for learning documentation, displays, or promotional purposes.
6. No images or videos will be transferred to personal devices or unauthorised platforms.
7.

Security Measures

1. Access to service systems will be password-protected.
2. Staff must not share login details.
3. Data will be stored securely, either on cloud systems with password protection or on service-issued hard drives/USBs.
4. Regular updates, antivirus protection, and security checks will be maintained.
5. Privacy Audit will be conducted annually or after any data breach.

RESIGNATION/EXIT PROCEDURE

1. Educators and staff who provide resignation are informed of their responsibilities and obligations in relation to the *Staff Code of Conduct* and *Governance and Management of the Service Including Confidentiality of records Policies.*
2. Management will remove access immediately to email address, SharePoint and/or cloud storage [Google Drive, Dropbox, OneDrive] and folders to an educator or staff member who has ended employment
3. Departing staff must sign to confirm they will not access or misuse service data.
4. An Exit Checklist will be completed to ensure digital security is maintained.

Roles and Responsibilities

Approved Provider & Nominated Supervisor will:

1. Review this procedure and the Safe Use of Digital Technologies and Online Environments Policy annually in collaboration with educators, staff, families, and children.
2. Inform families of this policy and procedure during the enrolment process.
3. Inform educators and staff of their responsibilities during orientation and induction.
4. Keep records of staff induction and ongoing training relating to technology use.
5. Identify staff training needs and provide professional development, including resources from the eSafety Commissioner – Early Years Program.
6. Provide regular training on safe technology use, mandatory reporting, and child-safe practices.
7. Ensure all staff sign a Cyber Safety Agreement and complete a Data Security Checklist as part of induction.
8. Maintain an Electronic Device Register for all service-owned devices.
9. Provide parents with information about apps, software, or programs used with children.
10. Ensure images/videos of children are managed in line with privacy law, parent authorisations, and service guidelines.

11. Ensure any breaches or incidents involving technology are investigated, recorded, and reported to the appropriate authority if required.

Educators and Staff will:

1. Use only service-issued devices for work purposes.
2. Never use personal devices (e.g., mobile phones, smart watches, USBs) while directly supervising children.
3. Supervise children at all times when using digital devices or online environments.
4. Use only approved apps, programs, and search engines.
5. Limit children's screen time to no more than 2 hours per day in line with Australia's Physical Activity and Sedentary Behaviour Guidelines.
6. Encourage children to use technology safely, respectfully, and responsibly.
7. Report any unsafe or suspicious online behaviour to the Nominated Supervisor immediately.
8. Follow the Administration of First Aid Policy and Child Protection Policy if a child is exposed to unsafe or harmful online interactions.

Children will:

- Be supported to develop digital literacy and safe online behaviours.
- Be encouraged to report anything that makes them feel unsafe or uncomfortable online.
- Not be permitted to bring personal devices to the service. If a device is brought in, it will be stored securely until collection by a parent/guardian.

Learning from Implementation to Improve Practice

We will regularly review incidents, feedback, and audits to identify trends or gaps in our procedures. Staff meetings, reflective practice sessions, and team debriefs will be used to discuss what worked well and where improvements can be made. We will also encourage feedback from children, families, and staff to ensure our procedures remain practical, effective, and aligned with current regulations and best practice. This continuous improvement approach ensures that our child safe practices evolve with the needs of our community

Providing Tools and Promoting Awareness

We ensure all relevant individuals at Fun 4 U can follow procedures by:

We ensure all relevant documents—such as checklists, risk assessment templates, supervision plans, and the Code of Conduct—are easily accessible. These tools are introduced during staff induction and revisited during regular team meetings, training sessions, and professional development. Policies and procedures are displayed in our staff area and stored in a central policy folder. Updates are communicated through newsletters, emails, and team briefings to ensure everyone remains informed and equipped to follow them with confidence.

Monitoring Evaluation and Review

Fun 4 U, we proactively monitor updates from ACECQA and Childcare Centre Desktop to ensure our *Safe Use of Digital Technologies and Online Environments Procedure* remains current and compliant. The policy is reviewed at least annually, in consultation with families, staff, educators, and management, to reflect best practices and evolving regulatory requirements. In addition to this, our policies are made readily available to families on our Facebook page and next to our sign in and out register we have a folder with a QR code to each policy. (Reg 171 & 172)

Sources

- Australian Children's Education & Care Quality Authority. (2025). *Guide to the National Quality Framework*
- Australian Children's Education & Care Quality Authority. (2023). *Embedding the National Child Safe Principles*
- Australian Children's Education & Care Quality Authority. (2024). *Taking Images and Video of Children While Providing Early Childhood Education and Care. Guidelines For The National Model Code*.
- Australian Government eSafety Commission (2020) www.esafety.gov.au
- Australian Government Department of Education. *Child Care Provider Handbook (2025)*
- Australian Government. eSafety Commissioner Early Years program for educators
- Australian Government, Office of the Australian Information Commissioner. (2019). Australian Privacy Principles: https://www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/
- Australian Government Department of Health and Aged Care. (2021). Australia's Physical Activity and Sedentary Behaviour Guidelines
- Australian Human Rights Commission (2020). *Child Safe Organisations.* https://childsafe.humanrights.gov.au/
- Australia's Physical Activity and Sedentary Behaviour Guidelines
- Early Childhood Australia Code of Ethics. (2016).
- Education and Care Services National Law Act 2010. (Amended 2023).

- Education and Care Services National Regulations. (Amended 2023).
- NQF Online Safety Guide_1.pdf
- *Office of the Australian Information Commissioner (OAIC)*
- *Privacy Act 1988.*

Date Created: August 2025
Date Reviewed by Fun 4 U: 12/08/2025
Childcare Centre Desktop Procedure Update: July 2025
This Procedure Follows the ACEQA: Child Safety | ACECQA, Digital technology and children | ACECQA & Chapter 2: Using digital technologies safely | ACECQA