St Paul Lutheran School

St Paul Lutheran School- SPLASH

Safe Use of Digital Technologies and Online Environments

Policy and Procedures

March 2026

1. Policy Statement

In accordance with the Education and Care Services National Law (from 27 February 2026), the safety, rights and best interests of children are the paramount consideration in all decisions, actions and practices relating to the use of digital technologies and online environments at the service.

2. Background

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. In addition the State Government of South Australia has banned the use of personal mobile devices in early years services to strengthen safety and better protect young children.

3. Legislative Requirements

National Law & Regulations

Section/Regulation	Description
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 162A	Child Protection training
Regulation 165	Record of visitors
Regulation 165A	Offence relating to children being at risk of harm
Regulation 166	Children not to be alone with visitors
Regulation 168	Education and care services must have policies and procedures
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

4. Principles informing our Policy

All decision-making is carried out in accordance with the principles of our service's Safe use of digital technologies and online environments policy.

- 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
- only service-issued devices may be used when taking images or videos of children while providing education and care. Personal mobile devices capable of taking images or videos, personal storage, or file transfer media cannot be in possession of any person while they are working directly with children
- 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.

5. Key terms

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

6. Links to other Policies

- Administration of Medication Policy
- Delivery and Collection of Children Policy
- Excursion Policy
- Incident Injury Trauma and Illness Policy
- Staffing Policy
- Providing a child safe environment Policy
- The administration of first aid Policy
- Dealing with medical conditions in children Policy

7. Induction and ongoing training

7.1 Induction Training

- New staff orientation: Induction includes a thorough introduction to our Centre's Safe use of digital technologies and online environments Policy.
- National Model Code for Taking Images or Videos of Children while Providing Early Childhood Education and Care

- During induction new staff are made aware that this Code has been adopted by our service and addresses child safe practices for the use of electronic devices while providing our team with further support and understanding which promote a child safe culture.
- Staff will be trained in our policy and procedures for the safe use of digital technologies and online environments, including how to use our service-issued devices and platforms securely.

7.2 Ongoing Training

- Regular updates: Ongoing training via sharing of information from ACECQA and the ESB at staff meetings, to reinforce and update staff on all new developments in this area of child safety.

7.3 Specialised Training

Specialised training will be made available to staff in particular the eSafety Commissioner online learning. To support leaders', teachers' and educators' understandings of their legal responsibilities, other specific training will be considered as it becomes available online or provided by specialist consultants. Organisations providing training include ACECQA, the Department of Education, AISSA, Lutheran Education SA NT WA, or other acknowledged, reputable and recommended training organisations.

8. Evaluation, Monitoring and Review

The policy will be subject to ongoing review and also annually as a part of the policy review process.

In the event of a revision or change of policy, educators and families are made aware of the changes and the revised policy. We follow the appropriate record-keeping processes for each updated version of the policy.

9. Policy Review

St Paul Lutheran School

St Paul Lutheran School- SPLASH

Safe Use of Digital Technologies and Online Environments

Policy and Procedures

March 2026

Last reviewed: March 2026

Date for next review: March 2027

44 Audrey Avenue, Blair Athol, South Australia 5084
T 08 8260 2655 **E** admin@stpaulba.sa.edu.au
W stpaulba.sa.edu.au / ABN 84 648 346 828

St Paul Lutheran School

St Paul Lutheran School- SPLASH

Safe Use of Digital Technologies and Online Environments

Policy and Procedures

March 2026

Procedural Guidelines

1. Reference to Policy and Philosophy

Our Safe Use of Digital Technologies and Online Environments Policy is located our website and a printed copy is available in the policy folder in the SPLASH office. Our procedures reflect our service's overall philosophy which highlights that our commitment to children's safety and wellbeing are paramount at our service. The procedures also set out supervision and action plans, including where plans are in place for specific children.

2. Procedures

Our procedures are kept with the policy document on the website and hard copies are available in the SPLASH Office.

2.1 Use of Personal devices by staff

- The use of personal devices when working or volunteering with children in any capacity is banned at our service. This fulfills our responsibility to children and families in accordance with the requirements of the Education Standards Board of SA (August 2025) and the National Model Code for Taking Images or Videos of Children while Providing Early Childhood Education and Care.
- Staff personal devices can only be used when staff are in the SPLASH office on breaks and no children are present.
- The exception is for smart watches **that are not capable of capturing, storing or transmitting an image.** Staff can wear these devices for timekeeping only and therefore MUST switch the device to airplane mode before their shift begins, only switching airplane mode off when they have completed their shift. The mandate is to ensure there is no current connection with the staff member's personal phone which has been appropriately stored away.

2.2 Use of Service issued devices

- Only service-issued electronic devices can be used when taking images or videos of children while we are providing education and care.
- Staff are trained in this policy and procedure, including how to use service-issued devices and platforms securely.
- Staff sign an agreement to this requirement as part of our Code of Conduct Procedures.
- Access to our service devices and platforms are limited to authorized staff only, with strong passwords and two-factor authentication.
- Service-issued devices are audited periodically by the nominated supervisor or approved provider to ensure appropriate use and compliance with this policy.

2.3 Taking Images or Videos of Children

- Parental consent is obtained during the enrolment process and must be documented and signed before taking and storing any images of children.
- The wishes of any parents who refuse authorisation, are made clear to all staff involved with their child/children.
- Before filming or taking any photographs, we ask our educators to consider the following
    - Educational purpose – images should support documentation of children's learning and development.
    - Intentional documentation – educators should avoid taking excessive numbers of photos.
    - Privacy and confidentiality – images must comply with the service's Privacy Policy and Acceptance and Refusal of Authorisations Policy.
    - Respect and dignity – the dignity and wellbeing of children must be upheld at all times.
    - Children's voice – children have the right to object to being photographed or filmed and their wishes must be respected.
    - Legal and policy compliance – all educators must follow relevant legislation and service policies regarding digital technologies.

2.4 Storage and Access to Digital Images

- Images taken on service devices are stored only on the approved service digital platform (insert platform name) with restricted access and appropriate data protection measures.
- Access to images is restricted to authorised staff and the families of the children included in the images.
- Images and videos are only accessed for communication with families and for documentation of children's learning.
- Staff must not transfer images or files to personal devices, storage media, or platforms not approved or monitored by the service.

2.5 Image Retention and Deletion

- Images or videos of children will only be retained while required for documentation or communication with families.
- Images will be securely deleted when:
    - a child leaves the service, or
    - they are no longer required for educational documentation.
- Deletion must occur from:
    - service devices
    - cloud storage

2.6 Visitors and Digital Devices

- When visits are organised with the service, visitors are informed that digital devices are not permitted in areas where children are being educated and cared for.
- All personal devices must be left in the staff room or office.
- Visitors are always accompanied and supervised by the nominated supervisor or a designated staff member and are never left alone with children.
- It is acknowledged that laptops used by contractors and allied health providers will be owned by that particular organisation and the user is abiding by all relevant codes of conduct. They will be informed that they must not:
    - Take photos or videos of children
    - Record audio
    - Store images or recordings of children

- Access personal social media while onsite
- Connect to unsecured networks

2.7 Children's Use of digital technologies

- Digital technologies may be used in the educational program where they support learning and development.
- Educators ensure:
  - active supervision
  - age-appropriate content
  - restricted internet access or filtered platforms
  - time limits appropriate for OSHC use
- Children will be supported to develop safe and respectful online behaviours.

2.8 Children bringing personal devices

- If a child brings an electronic device to the service, it will be switched off and stored in a locked cupboard.
- Parents or caregivers will be informed of this procedure.

2.9 CCTV and optional surveillance

- If CCTV or other optical surveillance devices are used at the service, they must only be used for child safety, security, or regulatory purposes.
- Cameras must not be placed in bathrooms, change areas or private spaces.
- Families will be informed if surveillance devices are in use.
- Recorded footage will be stored securely and accessed only by authorised personnel.

2.10 Reporting Child Safety concerns and incidents

All educators, staff, volunteers and students have a responsibility to respond to and report concerns about children's safety, including concerns arising from the use of digital technologies or online environments.

Any suspected child abuse, harm, inappropriate digital contact, or misuse of images or recordings involving a child must be reported immediately to the Nominated Supervisor or Approved Provider. Educators must also fulfil their obligations as mandatory reporters under South Australian child protection legislation.

If an incident involving digital technologies places a child at risk of harm, constitutes a serious incident, or involves a breach of child safety obligations under the Education and Care Services National Law, the Approved Provider will notify the Regulatory Authority, the Education Standards Board, within 24 hours in accordance with Regulation 176 of the Education and Care Services National Regulations.

All incidents, actions taken, and notifications made will be documented and stored in accordance with the service's record-keeping and privacy requirements.

We ensure that all educators and staff, including volunteers and students, understand how to report their concerns about child protection issues and child abuse. If there is any doubt or confusion, we provide training using the ACECQA online safety tool which supports their understanding and ensures children remain safe.

3. Roles and Responsibilities

Roles	Responsibilities
Approved provider	• ensure that obligations under the Education and Care Services National Law and National Regulations are met • ensure that the Safe use of digital technologies and online environments policy and procedures 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 Safe Use of Digital Technologies and Online Environments Policy and Procedures
	• 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:
	  ○ 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.

Nominated Supervisor	• implement the Safe use of digital technologies and online environments policy and procedures 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 Safe use of digital technologies and online environments policy and procedures

	• 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	• implement the Safe use of digital technologies and online environments policy and procedures 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 our 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.

4. Procedures Created/Reviewed

Created: March 2026
Review: March 2027

5. References and Resources

- 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
- eSafety Commissioner online learning for early years
- Office of Australian Information Commissioner
- PlayingITSafe
- ThinkUKnow
- Digital Child
- Young Children in Digital Society
- The Alannah & Madeline Foundation
- The Carly Ryan Foundation