SPCC Saints Academy

ACN 002 919 584
Administered by St. Philip's Christian Education Foundation Ltd.

SAFE USE OF DIGITAL TECHNOLOGIES AND ONLINE ENVIRONMENTS POLICY

Policy Statement
SPCC Saints Academy is committed to providing a safe, respectful, and inclusive environment for all children, families, and staff. This includes the responsible and secure use of digital technologies and online environments. We recognise the potential benefits of digital tools in supporting learning and communication, while also acknowledging the associated risks. This policy outlines our commitment to ensuring digital safety, privacy, and child protection in all digital interactions.

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.

Purpose
- Promote the safe and appropriate use of digital technologies and online environments.
- Protect children from harm, abuse, and exploitation in digital contexts.
- Ensure compliance with relevant legislation and regulatory requirements.
- Provide clear guidance on roles, responsibilities, and procedures for digital safety.

Scope
- All staff, educators, and volunteers.
- Children attending the service.
- Families and visitors.
- Contractors and external providers using digital technologies within the service.

Definitions
- Digital technologies: Devices and platforms such as computers, tablets, smartphones, cameras, and internet-based applications.
- Online environments: Any digital space accessed via the internet, including websites, apps, social media, and cloud-based platforms.
- Service-issued devices: Devices owned and managed by SPCC Saints Academy for educational or administrative use.
- The National Model Code for Early Childhood Education and Care (ECEC): National code recommending practices for using electronic devices, particularly when taking photos and videos of children, emphasizing using service-issued devices for these purposes and restricting personal device use to specific, authorized circumstances. The code also stresses the importance of obtaining consent, having strict controls for storing and sharing images, and regularly reviewing policies and procedures.

Roles and Responsibilities
Policy created: August 2025

Approved Provider	- Ensure this policy is developed, implemented, and regularly reviewed. - Allocate resources for secure digital infrastructure and staff training, ensuring all staff implement practices that align with the National Model Code and the services child safe practices for the use of electronic and digital devices for taking images or videos of children. - Ensure compliance with legal and regulatory obligations. - Respond to serious incidents involving digital technologies and notify authorities as required.
Nominated Supervisor	- Oversee the implementation of this policy and related procedures. - Ensure all staff are trained in digital safety and child protection. - Maintain records of parental consent for digital content. - Monitor the use of digital technologies and address any breaches. - Ensure secure storage and appropriate disposal of digital media.
Educators and Staff	- Use only service-issued devices for documentation and communication. - Supervise children's use of digital technologies and online platforms. - Promote safe, respectful, and age-appropriate digital engagement. - Report any concerns or incidents involving digital technologies. - Maintain confidentiality and adhere to privacy protocols. - Engage children in digital literacy and online safety education. - Families provide informed consent for the use of digital media involving their child. - Support the service's digital safety practices. - Refrain from using personal devices to capture audio, images or videos on site.

Procedures

1. **Use of Devices**

- Staff personal devices must be stored away during work hours unless authorised by Nominated Supervisor or Responsible Person.
- Service-issued devices are used for educational and documentation purposes only.
- Devices are password-protected and stored securely when not in use.
- Children with digital devices, including phones and computers, are asked to store away during service hours. Homework task completion is the only exception.
- Children with smart watches are requested to stow away or place the device in "flight" or "do not disturb" mode if required or appropriate.

2. **Audio, Image and Video Capture**

- Written consent is obtained from families before capturing or sharing audio, images/videos.
- Audio, Images/videos are used only for educational or documentation purposes.
- No audio, images/videos are shared on social media or public platforms without explicit consent.
- All media is stored securely and deleted when no longer required.
- Children are not permitted to use their own devices for audio, photo or video collection.

3. **Online Safety and Supervision**

- Children's online activity is actively supervised at all times. In the Saints Academy context, this is rare due to our intentional philosophical approach of "replacing screen-time with green-time". At times, Middle School children (Year 5 and 6) are given permission to complete homework tasks using their school-issued device, and this is done in a public space under staff supervision.
- Only age-appropriate, secure platforms are used for learning.
- Staff monitor for signs of cyberbullying, grooming, or exposure to inappropriate content.
- Children are taught to recognise and report unsafe online behaviour.

4. **Staff Training and Education**

All staff receive training both during induction and ongoing on:

- Digital safety and responsible use
- Privacy and data protection
- Identifying and responding to online abuse or grooming

5. **Incident Management**

- All incidents involving digital technologies are documented and reported.
- Serious incidents are escalated to the Approved Provider and relevant authorities.
- Families are informed of any incidents involving their child.
- The service follows mandatory reporting obligations where harm or abuse is suspected.

Communication and Review

This policy is reviewed annually or when significant changes occur.
Staff are informed on policy updates and expected to implement changes promptly.
Families are informed of the policy and invited to provide feedback.
A copy of the policy is available on request and QR code to policy displayed in the service.

Legislative and Regulatory Framework

- Education and Care Services National Law and Regulations, including:
  - Section 162A – Child protection training
  - Section 165 – Inadequate supervision
  - Section 167 – Protection from harm and hazards
  - Regulation 84 – Awareness of child protection law
  - Regulation 168 – Policies and procedures
  - Regulation 170 – Policies and procedures to be followed
  - Regulation 172 – Notification of changes
- National Quality Standard (NQS) – Quality Areas 2, 5, 6, and 7
- National Principles for Child Safe Organisations
- Privacy Act 1988 and relevant state-based privacy and child protection laws