



DIGITAL TECHNOLOGIES & ONLINE ENVIRONMENTS POLICY

1. POLICY STATEMENT

Kilkenny Primary School OSHC is committed to providing a child safe digital environment where the safety, rights, best interests, privacy and dignity of every child are paramount.

Digital technologies are used only when they support children's education, care, wellbeing, communication or service operations and can be used safely under active supervision.

This policy is informed by and/or operates in accordance with:

- Education and Care Services National Law (South Australia)
- Education and Care Services National Regulations
- Education and Early Childhood Services (Registration and Standards) Act 2011 (SA)
- Children and Young People (Safety) Act 2017 (SA)
- National Quality Standard – QA2 and QA7
- ACECQA child safety and digital device guidance
- Education Standards Board (ESB) regulatory guidance
- Relevant Department for Education SA child safe and digital safety guidance

2. SCOPE

This policy applies to:

- Approved Provider and Nominated Supervisor
- Responsible Persons
- Educators, employees and administration staff
- Volunteers, students and work experience participants
- Contractors and service providers while engaged by OSHC
- Children attending Kilkenny OSHC
- Families, carers and visitors while at the service
- Digital activity during excursions and transport forming part of the service





3. LEGISLATIVE & REGULATORY OBLIGATIONS

Kilkenny OSHC will meet current National Law and Regulation requirements, including:

- Children's safety, rights and best interests are the paramount consideration (s2A)
- Adequate supervision is maintained at all times (s165)
- Reasonable precautions are taken to protect children from harm and hazards (s167)
- Digital device requirements in centre-based services are followed (ss175A–175J)
- A safe use of digital technologies and online environments policy and procedures are maintained (Reg 168)
- Policies and procedures are followed, available and updated as required (Regs 170–172)
- Personal-device authorisations contain prescribed information and are retained for at least 3 years (Regs 179A–179B)
- Confidentiality, storage and security of records are maintained (Regs 181 and 183)

From 27 February 2026, centre-based services must ensure personal digital devices are not used or possessed by relevant workers while working directly with children, except where a lawful limited exception applies.

4. CHILD SAFE DIGITAL PRACTICE

Kilkenny OSHC will:

- Place child safety ahead of convenience, documentation or communication
- Use the minimum technology necessary for the intended purpose
- Actively supervise children whenever digital technology or an online environment is used
- Respect children's privacy, dignity, cultural safety and age-appropriate choice
- Obtain and respect required parent/carer authorisations
- Support children to understand consent, privacy, respectful behaviour and online safety
- Respond immediately to unsafe content, contact, conduct or suspected online abuse
- Review digital risks when technology, platforms, equipment or service practices change



5. PERSONAL DIGITAL DEVICES

While working directly with children, the Approved Provider, Nominated Supervisor, staff, educators, volunteers and students must:

- Not use or have a personal device in their possession
- Store phones, image-capable smart watches, cameras, tablets and personal storage media securely in the allocated staff-only storage area
- Keep personal devices inaccessible to children and out of the education and care environment
- Not use personal accounts, personal cloud storage or personal file-transfer media for OSHC information
- Use a personal device only where a lawful exception has been approved
- Never use a personal device to capture, store or transmit an image or video of a child

A short break away from children is not considered “working directly with children”; personal devices may only be accessed in a staff-only area where children are not present.

6. AUTHORISED EXCEPTIONS & RECORDS

A personal device may only be authorised for a limited essential purpose, including:

- A genuine health or disability-related need
- Urgent communication with a family member where service contact arrangements are not practical
- Failure of a service-supplied device where a device is necessary for children’s safety or education and care
- An emergency, lockdown, evacuation or local emergency warning
- A work health and safety reason
- An excursion or transport situation where use is genuinely necessary for children’s safety or education and care
- Authorisation must be given by the Approved Provider in writing before use wherever practicable and an exemption form to be filled out and signed by the approved provider
- Where prior written authorisation is not practicable in an emergency, the approval and circumstances must be documented as soon as practicable.
- Records must include the authorised person, role, authoriser, device description, purpose and period of authorisation and be kept for at least 3 years.

7. SERVICE-SUPPLIED DEVICES

- Only service-supplied devices may capture, store or transmit images or videos of children
- Service-supplied devices are used exclusively for education and care purposes – never for personal use
- OSHC mobiles, iPads, laptops and other authorised devices are recorded in the service device/asset register
- Devices use secure passwords, screen locks, approved applications and appropriate filtering/security controls
- Personal accounts must not be logged into on service-supplied devices
- Lost, damaged, stolen or compromised devices must be reported immediately

8. IMAGES & VIDEOS OF CHILDREN

Images and videos may only be taken where there is a clear service purpose and child safe practice is maintained. Kilkenny OSHC will:

- Obtain written parent/carer authorisation before taking, using or storing images/videos
- Respect any withdrawal or change of authorisation
- Consider the child's assent or dissent and stop where a child indicates they do not want an image taken
- Use images primarily for learning documentation, participation, communication, service records or another approved purpose
- Take images only on service-supplied devices
- Avoid taking images in private or vulnerable situations including toileting, changing, undress, distress or dysregulation
- Ensure placement students do not use personal devices; any required practicum images must have specific consent and be taken/managed on a service-supplied device
- Ensure images are not altered, repurposed or shared beyond the authorised purpose

Families and visitors must not photograph, film or audio-record other children. Any photography at special events must follow service directions and family authorisations.



9. STORAGE, ACCESS, RETENTION & DESTRUCTION

Kilkenny OSHC will maintain strict controls over digital records and media:

- Store images/videos only on approved service or Department systems and locations
- Restrict access to authorised staff who require it for their role
- Not download or transfer children's images to personal devices, personal email, personal cloud storage or unapproved USB/storage media
- Use secure passwords, device locks and multi-factor authentication where available
- Back up official records to an approved secure location where required
- Retain and destroy images/videos in line with their purpose, service record-keeping procedures, applicable State Records/Department requirements and privacy obligations
- Remove access when staff leave or when families/children cease enrolment where access is no longer required
- Regularly audit storage locations, sharing permissions and device access

10. CHILDREN'S USE OF DIGITAL TECHNOLOGY

Digital technology is a planned learning and leisure resource, not a default activity. Children's use will be:

- Purposeful, age-appropriate and linked to the program, an observation, child voice or a planned experience
- Time limited and balanced with active, social, creative and outdoor experiences
- Actively supervised in an open shared area where educators can directly observe screens
- Restricted to service-supplied devices unless a child has an approved individual arrangement
- Protected by filtering, privacy settings and restrictions on downloads, purchases, chat and social media
- Recorded through the service device log where devices are allocated to individual children
- Used in a way that supports healthy posture, breaks and safe physical use
- Never used as a reward, behaviour management strategy, babysitting tool or routine response to weather





Children's personal devices, including image-capable smart watches, are not permitted unless approved for a documented medical, disability, communication or other individual need. Approved use must have clear limits, supervision and risk controls.

11. ONLINE SAFETY & ACTIVE SUPERVISION

- Educators must be able to see the screen and monitor what the child is accessing
- Children must not have unrestricted or unsupervised internet access
- Children are taught not to share names, images, passwords, locations or other personal information online
- Children are encouraged to tell an educator immediately if content, contact or behaviour feels unsafe or inappropriate
- Staff intervene promptly where there is unsafe content, cyberbullying, grooming, sexualised content, inappropriate messaging or other online harm
- Digital use is included in relevant risk assessments and reviewed after incidents or changes in technology

12. ARTIFICIAL INTELLIGENCE & EMERGING TECHNOLOGIES

- Only service/Department-approved AI or emerging technology may be used for OSHC work where access is permitted
- Children's names, images, videos, health information, enrolment information or other identifying/sensitive data must not be entered into public or unapproved AI tools
- Children will only use AI-enabled tools where the activity is planned, age-appropriate, supervised and does not require disclosure of personal information
- AI output must not replace educator judgement, supervision, child protection decisions or professional responsibility





13. CCTV & OPTICAL SURVEILLANCE

Where CCTV or another optical surveillance device is used, Kilkenny OSHC will:

- Use surveillance only for an identified lawful and child safe purpose
- Inform families and staff and display appropriate signage
- Never install cameras in toilets, bathrooms, changing or other private areas
- Ensure CCTV does not replace active educator supervision
- Restrict access to authorised personnel
- Store, access, disclose and destroy footage securely and in accordance with applicable law, privacy and service requirements

14. PRIVACY, CYBERSECURITY & DATA BREACHES

- Personal and sensitive information about children, families and staff is confidential
- Only approved systems, applications and accounts are used for service information
- Passwords are not shared and devices are locked when unattended
- Open/public Wi-Fi and unapproved storage services are not used for confidential service information
- Suspected unauthorised access, data loss, phishing, lost/stolen devices or privacy breaches are reported immediately to the Director/Nominated Supervisor
- The service will follow Department, governing council, regulatory and legal reporting requirements for any confirmed data or privacy breach

15. INCIDENTS, CONCERNS & REGULATORY NOTIFICATIONS

Any concern involving online abuse, unsafe digital contact, inappropriate images, device misuse or a breach of this policy must be acted on immediately.

- Protect the child and stop unsafe access or activity
- Notify the Responsible Person and Director/Nominated Supervisor immediately
- Preserve relevant evidence safely without forwarding or unnecessarily copying harmful material
- Follow mandatory reporting, child protection, incident and complaint procedures where required
- Notify SAPOL, the Department for Child Protection or eSafety Commissioner where required by the nature of the concern



- Notify the Education Standards Board within the prescribed timeframe for notifiable matters; serious incidents and allegations/incidents of physical or sexual abuse require 24-hour notification where applicable

16. RESPONSIBILITIES

Approved Provider / Nominated Supervisor will:

- Implement, communicate and review this policy and procedures
- Provide suitable service-supplied devices and secure personal-device storage
- Maintain device registers and personal-device authorisation records
- Ensure staff induction, training and understanding of current requirements
- Audit digital practice, storage, permissions and compliance
- Make required notifications and respond to breaches or incidents

Responsible Persons, educators and staff will:

- Follow this policy and all approved device procedures
- Store personal devices before working directly with children
- Use service-supplied devices only for authorised work purposes
- Maintain active supervision and protect children's privacy and dignity
- Check authorisations before taking or using images/videos

- Report concerns, breaches, lost devices or unsafe online activity immediately

Families, visitors, volunteers and students will:

- Follow service directions for personal devices, photography and online safety
- Not capture or share images/audio/video of other children
- Respect children's privacy and service confidentiality
- Report any digital safety concern to OSHC staff promptly

17. CONTINUOUS IMPROVEMENT

This policy will be reviewed:

- Annually
- Following legislative or regulatory change
- Following a serious incident, breach or complaint
- Following advice from ACECQA, the ESB or relevant Department for Education guidance

Families will be notified of policy changes in accordance with Regulation 172, including at least 14 days before changes that may have a significant impact unless an immediate change is required to address a risk to children's safety, health or wellbeing

18. RELATED POLICIES & GUIDANCE

- Child Safe Environment Policy
- Supervision Policy
- Child Protection / Mandatory Reporting procedures
- Code of Conduct
- Privacy and Confidentiality Policy
- Incident, Injury, Trauma and Illness Policy
- Excursion and Safe Transportation policies
- Complaints and Feedback Policy
- ACECQA – Safe Use of Digital Technologies and Online Environments: Policy and Procedure Guidelines (April 2026)
- ACECQA – Using Digital Devices in Centre-Based Education and Care Services
- ESB – National Child Safety Reform and Regulatory Changes / digital technology guidance
- Relevant Department for Education SA child safe and digital safety guidance

REVIEW DETAILS

POLICY REVIEWED BY	Graziella Panazzolo	OSHC DIRECTOR	
POLICY REVIEWED	August 2026	NEXT REVIEW DATE	August 2027
MODIFICATIONS	• Condensed into an easier-to-read dot point format • Updated to reflect 27 February 2026 National Law/Regulation digital device requirements • Updated against current ACECQA, ESB and relevant Department for Education SA guidance		
PREVIOUS MODIFICATIONS	• New policy developed following Regulation 168 digital technology changes effective 1 September 2025 • Merged Technology, Cyber Safety, Mobile Device Usage and CCTV policies		