Catholic Early EdCare
WATCH THEM GROW

SAFE USE OF TECHNOLOGIES AND ONLINE ENVIRONMENTS PROCEDURE

TABLE OF CONTENTS

POLICY AND PHILOSOPHY

This procedure operationalises CEEC's commitment to protecting children in digital and online environments. It provides practical steps for the safe and ethical use of devices, platforms, and digital content and outlines expectations for staff, children, and families in relation to privacy, supervision, consent, and online safeguarding.

Policy Sponsor: Operations
Document Type: Procedure
Applicable To: Catholic Early EdCare
Approved By: Director, Catholic Early EdCare
Last Updated: 29/08/2025
Due for Review: 29/08/2028
Version No. 2025.1

Catholic Early EdCare
WATCH THEM GROW

SAFE USE OF DIGITAL DEVICES IN SERVICES

CATHOLIC EARLY EDCARE WILL:

- ☐ Provide safe, secure, and clearly designated storage areas (e.g., locked cupboards or staff lockers) at every service location for staff to store their personal devices during work hours.
- ☐ Ensure service-owned digital devices are managed, updated, and monitored in accordance with CEEC's digital safety expectations and IT protocols.

EDUCATORS AND STAFF MUST:

- ☐ CEEC provides safe, secure and clearly designated lockable storage at each service for staff to store personal electronic devices, during work hours. All other personal belongings, such as bags, must be stored in separate lockable storage provided by the service.
- ☐ Service Leaders or Responsible Persons (RPs) may take service devices off-site when required for work-related duties including but not limited to:
  - ☐ Attending other CEEC Services or the Rosalie Support Office.
  - ☐ Participating in training sessions during work hours.
  - ☐ Emergency communication outside of operational hours (e.g. staff cancelling shifts, parents requesting care).
- ☐ Use only CEEC-authorised devices (e.g service tablets, cameras, laptops) for educational or documentation purposes. CEEC devices may be removed from the service licensed premises for approved excursions. Educators must ensure all devices are returned to the service after the excursion.
- ☐ No personal use of devices (including messaging, calls, or browsing) during contact with children unless on scheduled breaks or in emergency situations.
- ☐ Never take photos, videos, or voice recordings using personal devices at the service, including during excursions or events.
- ☐ Protect all CEEC devices with strong passwords and log out of applications when not in use and ensure devices are stored in a secure location.

- ☐ All service-issued devices must have a CEEC branded identification sticker applied in a clearly visable location. This requirement ensures that devices are easily recognisable as belonging to Catholic Early EdCare, helping to safeguard children and staff by preventing the unauthorised use or misidentification of CEEC equipment.
- ☐ Immediately report lost or stolen devices to the Nominated Supervisor who will report to the Rosalie Support Office.
- ☐ Adhere to the National Model Code in which any device that can take images or videos of children should not be worn when directly educating and caring for children. This includes:
  - ☐ Smart watches or any other electronic device that **CAN** take images are **NOT** to be worn.
  - ☐ Smart watches that **CANNOT** take images and videos including wearables **CAN** be worn, however should not be used to make calls, read notifications while educators are responsible for the supervision and care of children (e.g. an Apple Watch would be an approved device, as although it can trigger capturing on a mobile device, the device itself cannot capture images or video.
  - ☐ Smart watches must not be used to take photos or videos, make or receive phone calls, or send and receive messages while educators are responsible for the supervision and care of children.
  - ☐ If any wearable device is identified by the Nominated Supervisor as causing regular distraction or impacting the quality of supervision and engagement with children, appropriate performance support and management processes may be implemented.

EXEMPTION:

- ☐ An exemption may be granted where a staff member has requested to keep an electronic device on their person while providing education and care to students in certain instances, such as:
  - ☐ Personal health needs requiring device use (e.g. heart or blood monitoring). This may also include staff members own children with the above health needs.
  - ☐ Disability-related communication needs.
  - ☐ Urgent family matters (e.g. critically ill or dying family member).
- ☐ A medical exemption letter will be required and supporting documentation may be requested if further verification is required.

DEFINITION OF PERSONAL DEVICES

DEFINITION OF PERSONAL DEVICE:

A personal device refers to any personally owned electronic or digital device that can capture, store, transmit, or access data or communications.

This includes, but is not limited to:

- ☐ Mobile or cellular phones
- ☐ Tablets (e.g., iPads, Android tablets)
- ☐ Laptops or notebooks that can capture images/videos
- ☐ Smartwatches and fitness bands with messaging/camera/GPS/ recording capabilities
- ☐ Smart watches and fitness bands that can take images or videos
- ☐ Digital cameras or wearable cameras (e.g. GoPros)
- ☐ Smart wearables also include smart glasses and smart sun glasses
- ☐ USBs and external hard drives

These devices must be securely stored and not used during operational hours except as authorised.

PERSONAL ELECTRONIC DEVICES FOR STUDENTS AND FAMILIES:

- ☐ Students enrolled at the OSHC are not permitted to bring personal electronic devices to the Service, unless an exemption has been granted with the Nominated Supervisor based on necessity due to a diagnosed medical condition or disability.
- ☐ If a student brings a personal electronic device to the Service without a written exemption, the device must remain in the student's bag until they are collected at the student's and their family's risk.
- ☐ The service does not take any responsibility for the personal device whilst the student is at the service.

CAPTURING AND USING IMAGES OF CHILDREN

BEFORE CAPTURING IMAGES:

- ☐ Confirm a current, signed Informed Image Consent Form is held for the child (usually obtained during enrolment).
- ☐ Ensure the child is given the opportunity to decline being photographed, even with prior parental consent, and respect this without question.

WHEN TAKING IMAGES:

- ☐ Use CEEC-owned devices only (no personal phones, tablets or cameras).
- ☐ Avoid capturing other children incidentally or unintentionally.
- ☐ Ensure children are always dressed and captured in a manner that maintains their dignity.
- ☐ Ensure no full names or identifying details are visible in the image or its metadata.

AFTER CAPTURING IMAGES:

- ☐ Store all images and digital content in secure CEEC platforms (e.g., Xplor) with restricted access only to authorised staff.
- ☐ Label files with first name initials only and the date (e.g., "J.S. Reading - 2025-06-18").
- ☐ Regularly delete outdated or unnecessary images in line with CEEC's record retention policy.

CCTV (CLOSED CIRCUIT TELEVISION)

Catholic Early Edcare is committed to the safe and responsible use of digital technologies to protect the privacy and wellbeing of children, families, and employees. As part of this commitment, CEEC acknowledges that many of its services are co-located on sites with Brisbane Catholic Education (BCE) schools.

In some instances, the school may have its own Closed-Circuit Television (CCTV) systems installed for security and safety purposes. These CCTV systems are wholly managed, operated, and maintained by the school not by CEEC.

CEEC does not have access to any footage, data, or systems associated with school-operated CCTV. The use, storage, and management of CCTV by the school are governed by the school's own policies and procedures, which are seperate from CEEC's systems and operations.

Any request for access to CCTV footage relating to CEEC operations or incidents must be submitted through CEEC Senior Leadership, who will liaise directly with Brisbane Catholic Education to manage the request in accordance with privacy and data governance legislation.

CEEC ensures that its own use of digital technologies including photography, digital recordkeeping, and electronic communication complies with all relevant privacy, data protection, and child safety legislation, as well as Catholic Early EdCare's policies and procedures.

PUBLIC SHARING AND SOCIAL MEDIA USE

ALL CONTENT SHARED PUBLICLY (E.G. CEEC WEBSITE, NEWSLETTERS, SOCIAL MEDIA) MUST:

- ☐ Be approved in writing by the Service Leader prior to posting.
- ☐ Comply with the Archdiocese of Brisbane Social Media Use Policy and CEEC branding standards.
- ☐ Exclude children's full names or locations.
- ☐ Avoid identifiers such as uniforms, logos, or visible addresses.
- ☐ Not show children in states of distress, toileting, swimming, or other vulnerable contexts.
- ☐ Be posted on official CEEC approved accounts only.

Families can request the removal of shared content at any time, and this must be actioned within 48 hours.

EDUCATORS' USE OF PERSONAL DEVICES DURING EXCURSIONS

Catholic Early EdCare recognises that educators may need to carry personal devices when accompanying children on excursions. To ensure children's safety and uphold CEEC safeguarding principles...

EDUCATORS MAY:

- ☐ Carry their personal device during excursions for emergency use only (e.g., urgent contact with emergency services, the Service Leader, or families).
- ☐ Keep their personal device stored securely (e.g., in a pocket, bag, or locked compartment) when not in use.

EDUCATORS MAY NOT:

- ☐ Use personal devices to capture photos, videos, or voice recordings of children at any time.
- ☐ Use personal devices for messaging, social media browsing, or personal calls during excursions, except during scheduled breaks away from the children or in an emergency situation.
- ☐ Share their personal device with children under any circumstances.

CEEC WILL:

- ☐ Ensure that service-owned devices (e.g., tablets, cameras) are provided and used for all educational, documentation, and communication purposes during excursions.
- ☐ Provide clear protocols for emergency communications, including who is responsible for carrying CEEC-owned phones/devices.

USE OF ONLINE PLATFORMS AND CLOUD-BASED SYSTEMS

SOME EXAMPLES OF ONLINE PLATFORMS AND CLOUD-BASED SYSTEMS INCLUDE XPLOR AND MICROSOFT TEAMS.

EDUCATORS AND STAFF MUST:

- ☐ Use only CEEC-approved platforms, supported and endorsed by the Governance and ICT teams.
- ☐ Never access these platforms from personal devices or via unsecured networks.
- ☐ Use unique login credentials, and never share passwords or devices with others.
- ☐ Log out of platforms after use and report any access issues or suspected breaches.
- ☐ All apps, software, or digital tools must go through a documented risk assessment before use.
- ☐ Only CEEC IT can approve downloads/ installation- staff cannot independently install apps on service devices.
- ☐ Risk assessments must capture safeguarding, data security, privacy and child wellbeing considerations.

FAMILIES MUST:

- ☐ Be informed of how their child's digital documentation is stored and shared.
- ☐ Be provided with secure login credentials if applicable.
- ☐ Have the option to opt-out of digital portfolios or request removal of specific content.

RISK ASSESSMENTS FOR DIGITAL TECHNOLOGIES

A risk assessment must be completed before the introduction, download, or use of any:

- ☐ Apps
- ☐ Programs
- ☐ Platforms
- ☐ Digital Devices
- ☐ Hardware
- ☐ Online Practices (e.g. video conferencing, livestreaming, digital portfolios).

The risk assessment must consider:

- ☐ Child Safety and Wellbeing
- ☐ Safeguarding and Supervision
- ☐ Privacy
- ☐ Data Storage and Information Sharing
- ☐ Reputational and Compliance Risks

All app and software downloads must be approved and installed by CEEC IT. Educators and staff must not download or install apps independently.

The Nominated Supervisor is responsible for ensuring risk assessments are completed, signed and filed before requesting Technology Support approval.

Risk Assessments must be reviewed and updated:

- ☐ Annually as part of CEEC's compliance audit cycle; and
- ☐ Following any incident or breach.

CYBER SAFETY FOR CHILDREN

EDUCATORS WILL:

- ☐ Supervise all use of digital technologies by children.
- ☐ Introduce concepts of cyber safety and digital respect using developmentally appropriate language (e.g., "always ask before taking a photo," "tell an adult if something doesn't feel right").
- ☐ Use screen time as a collaborative and purposeful activity, not passive or background entertainment.
- ☐ Limit digital use to content that is educational, inclusive, and values-aligned.

EDUCATIONAL PROGRAM:

- ☐ Catholic Early EdCare believes that safe technology use has a place in children's learning. Technology can make learning more interactive and engaging for students and support in the process of interest-based learning by providing powerful research tools.
- ☐ Images and videos can be used by staff to capture evidence of learning that may be shared with families and allow children to re-visit their learning. These images are shared via the XPLOR platform which parents can access their individual accounts via a secure login process.

RESPONDING TO DIGITAL BREACHES OR INCIDENTS

If a breach or concern is identified (e.g. inappropriate content, unauthorised image capture, lost device):

EDUCATORS MUST:

- ☐ Notify the Nominated Supervisor immediately.
- ☐ Complete a Guardian incident report within 24 hours.
- ☐ Not attempt to delete or alter evidence.

NOMINATED SUPERVISORS WILL:

- ☐ Secure the device and gather all related documentation.
- ☐ Notify:
  - ☐ Safeguarding
  - ☐ CEEC Governance and ICT (if technical risk)
  - ☐ Families of children involved
  - ☐ Regulatory Authority if the event meets notifiable criteria (e.g., Reg 175(2)(d) or (e)).
- ☐ All incidents will be logged and reviewed during compliance audits.

ROLES AND RESPONSIBILITIES

ROLE	RESPONSIBILITIES
Approved Provider	• Ensure all CEEC services comply with NQF digital safety requirements. • Provide infrastructure and support for digital compliance.
Director, CEEC	• Approve policies and oversee risk and compliance related to digital technology.
Service Leaders	• Maintain consent records. • Monitor educator practice and enforce safe storage of devices. • Approve media and communications prior to publication.
Educators and Staff	• Follow all safe use protocols. • Store personal devices appropriately. • Supervise children's use of digital tools and ensure informed consent for images. • Report incidents promptly.
Families	• Provide consent or opt-out for digital use. • Raise concerns or request image removal at any time.
Safeguarding and Governance	• Provide advice, risk review, and manage escalations and reporting to external authorities.

CONNECTION TO CEEC MINDSETS

MINDSET	APPLICATION
Safety First	Proactively preventing harm through secure storage, privacy, and active supervision.
Compassion	Respecting children's dignity and preferences regarding their image and identity.
Collaboration	Working with families on consent, image use, and digital transparency.
Accountability	Ensuring all staff are trained, compliant, and aware of reporting obligations.
Inclusion	Considering diverse needs in technology access, representation, and safety measures.

MONITORING, EVALUATION AND REVIEW

THIS PROCEDURE WILL BE REVIEWED EVERY 3 YEARS OR EARLIER IF REQUIRED DUE TO:

- ☐ Legislative changes (e.g. ACECQA NQF updates)
- ☐ Incident trends
- ☐ Family or staff feedback

ANNUAL AUDITS WILL CHECK:

- ☐ Image consent register accuracy
- ☐ Device use logs
- ☐ Staff compliance with personal device storage

Catholic **Early EdCare**

WATCH THEM GROW