CatholicCare
DIOCESE OF BROKEN BAY

# Children's Services

# Safe Use of Digital Technologies and Online Environments

## Policy

Version: 6.0
Approved: 10 June 2026
Review due: June 2029
Document ID: 12011-049

# Contents


What do we believe? ..... 3
What are we going to do? ..... 3
How will it be done? ..... 3
- Authorisation to take images and videos ..... 3
- Taking images and videos of children ..... 3
- Storage and destruction of images and videos ..... 4
- Service issued devices ..... 4
- Staff – Personal devices, smart watches and wearable devices ..... 5
- Children – Personal devices, smart watches and wearable devices ..... 5
- Optical surveillance devices ..... 6
- Programming with devices for children ..... 6
- National model code ..... 7
- Device register ..... 7

Who is responsible? ..... 8
National Quality Standards (NQS) ..... 9
Related documents ..... 9
- CatholicCare policy ..... 9
- Children's Services Policies or Guidelines ..... 9
- Forms ..... 10

Resources ..... 10
- External ..... 10

Glossary ..... 10
Sign off and review ..... 11
Revision history ..... 11

# What do we believe?

At CatholicCare Diocese of Broken Bay, we are committed to the safety and wellbeing of children and hold this at the centre of our decision making and practice. We understand that technology can create challenges and threats to the safety, wellbeing and protection of children. Digital technology plays an important role in supporting children's learning, communication, and documentation; however, it must always be used in a way that prioritises children's safety, privacy, dignity, and wellbeing.

We are committed to ensuring the safe, ethical, and responsible use of digital devices across our services.

# What are we going to do?

CatholicCare Diocese of Broken Bay Children's Services will ensure that all digital devices are used safely, ethically, and in ways that prioritise the safety, privacy, dignity, and wellbeing of children. We will implement clear procedures for the appropriate use, storage, and management of digital devices, images, and information, ensuring all practices align with legislative requirements, organisational and community expectations. Educators and staff will be guided and supported to use digital technology intentionally to enhance children's learning while actively minimising risks, including unauthorised access, sharing, or misuse of content. We will ensure informed consent is obtained from families, maintain secure systems for storing digital information, and regularly review practices to uphold a strong child safe culture.

This policy outlines the expectations for the use of digital devices by educators, children, and families, including the capturing, storage, and management of images and information. It reflects our commitment to maintaining a child-safe culture and aligns with the National Quality Framework and the National Model Code for Taking Images or Videos of Children while Providing Education and Care.

Through this policy, we aim to ensure that digital technology is used intentionally and appropriately to enhance children's learning, while minimising risk and upholding the rights of every child.

# How will it be done?

## Authorisation to take images and videos

- Written authorisation must be obtained from a child's parent or authorised nominee before any images or videos are taken, used or stored by the service. Authorisation is obtained through the enrolment process and outlines how images may be used for educational documentation and service purposes.
- This authorisation can be found on the CatholicCare consent form attached to the Enrolment form.
- Families may withdraw their consent at any time, and the service will immediately action this request.

## Taking images and videos of children

- Educators are only permitted to take photographs or videos of children using devices issued by the service
- Personal devices must not be used to capture images or videos under any circumstances

- All images and videos must be respectful and appropriate, and must protect the privacy and dignity of children
- Photographs that clearly identify children, including identifiable facial features, must not be shared on online platforms, including the service's CRM system
- Images of children must not be sent to families via text message or email
- When images are used for documentation or communication, children must not be identifiable
- Educators may use printed photographs within the service for educational documentation, learning displays, or program reflection
- Hard copy photographs must remain within the service and must not be distributed externally.
- For days of significance (*for example Mother's Day, Father Day),* seek advice from the Practice Manager if unsure; services may provide a hard copy photo of an individual child in line with the programmed experience. This photo must not contain images of any other children.

## Storage and destruction of images and videos

- All images and videos captured on service issued devices must be stored securely and accessed only by authorised educators or staff.
- The Nominated Supervisor is responsible for ensuring that images stored on service issued devices are permanently deleted at least once per month. This includes all service devices such as phones, tablets, and laptops.
- This process supports the secure management of children's information and reduces the risk of unauthorised access.

## Service issued devices

- Digital devices issued by the service such as tablets, phones, cameras or laptops must only be used for work related purposes. These devices must be listed on the Approved Device Register at each service and have authorisation from the person with management and control. These records must be kept for three (3) years.
- Educators and staff must ensure that devices are used in accordance with this policy and professional standards and that children's personal information and images are protected. Devices must not be used to access inappropriate content or used for personal purposes unless authorised.
- Where digital devices are used by children as part of the educational program, educators will ensure that device use supports learning, creativity and exploration. Children will be supervised when using digital devices and the content provided will be safe, age appropriate and balanced with other forms of play and learning.
- Educators will support children to develop an understanding of safe and responsible use of technology.
- Service-issued digital devices, including phones, tablets, cameras, and laptops, are provided to support the operation of the service and the delivery of the educational program. These devices must only be used for work-related purposes and as defined by this policy.
- Educators and staff will:
    - Use service-issued devices to support programming, documentation, communication, and administrative tasks
    - Ensure all use of devices is professional, appropriate, and aligned with policies and procedures

- Use only service-issued devices to take photos or videos of children
- Ensure children's information, images, and data are protected, stored securely, and accessed only by authorised persons
- Not use service-issued devices to access inappropriate and/or illegal content or for unauthorised personal use
- Ensure devices are stored securely when not in use and handled in a way that prevents loss, damage, or unauthorised access

- The use of service-issued devices will be monitored to ensure compliance with this policy and to always maintain the safety and privacy of children at all times.

## Staff – Personal devices, smart watches and wearable devices

- Educators must not wear smart watches or wearable devices capable of taking photos, recording video, or accessing communication platforms while working with children, unless authorised by the Nominated Supervisor with a completed and stored authorisation form.
- Personal digital devices may only be accessed during working hours with approval from the Nominated Supervisor and must remain stored with personal belongings and not accessible while working with children.
- Personal devices must never be used to take photographs or videos of children under any circumstances.
- Any approved access to personal devices must be supported by a completed authorisation form stored in the educator's staff file.
- The service must maintain and regularly update a register of authorised personal devices, with all authorisations and consent forms reviewed at least every three (3) months to ensure they remain current and appropriate.
- The written authorisation must be kept for a minimum of three (3) years and include the:
  - Service details
  - Personal details
  - Reason for authorisation
  - Duration of the authorisation

## Children – Personal devices, smart watches and wearable devices

- Children may only wear or carry a personal device, smart watch, or wearable technology where it is required for a diagnosed medical condition, and/or with written consent provided by a parent or guardian prior to use.
- Personal devices are not permitted for general communication and must only be used for approved medical purposes. Children are not permitted to make calls, send messages, access the internet, or use the device for non-medical reasons while in care.
- Educators must ensure the device and its use are documented within the child's medical risk minimisation plan, that all staff are aware of its purpose and required procedures, and that a service-level risk assessment has been completed.

- Educators are responsible for ensuring that:
    - The device and its approved use are documented within the child's medical risk minimisation plan.
    - All staff working with the child are aware of the device, its purpose, and any required responses for procedures.
    - Nominated Supervisors will ensure a risk assessment is completed in relation to personal devices being used at the service.
- Written authorisation must:
    - Include the service name and details
    - Include the child's details and parent or guardian authorisation
    - Clearly outline the reason for the device and how it will be used.
    - Be reviewed at least annually, or earlier if the child's needs change.
    - Be retained by the service for a minimum of three (3) years in accordance with record-keeping requirements.

# Optical surveillance devices

- Currently No CatholicCare Services have Optical Surveillance devices installed.
- If optical surveillance devices such as closed-circuit television are used at the service, families, staff and visitors will be informed.
- Surveillance devices will only be used for safety and security purposes and will not be installed in private areas such as bathrooms, toilets or change areas. Any recorded footage will be stored securely and accessed only by authorised personnel in accordance with privacy requirements.

# Programming with devices for children

- A limited number of digital devices may be used within the educational program to enhance learning, creativity, and engagement, ensuring use is intentional and aligned with children's interests, development, and the service program
- Educators will use digital technology to support research, problem solving, creativity, and exploration, ensuring all experiences are age appropriate, meaningful, and linked to the planned program
- Children will be actively supervised at all times when using digital devices and supported to develop safe, respectful, and responsible use of technology
- Technology will be used to enhance, not replace, play-based learning and social interactions
- Digital media such as videos, music, or online content will only be used where it supports children's learning or wellbeing, is age appropriate, and has been reviewed by educators for suitability
- Children may use technology for creative purposes such as storytelling, research, or project work, ensuring compliance with copyright and ethical use requirements
- Any digital program, post, communication, or newsletter will not include images that identify children, including facial features, to maintain privacy and safety
- The use of digital devices within the program will be regularly reflected on and evaluated to ensure it remains purposeful, balanced, and in the best interests of children.

# National model code

- The service aligns with the National Model Code for Taking Images or Videos of Children while Providing Education and Care to support child safe practices when using digital devices
- Only service-issued devices are used to take images or videos of children
- Personal electronic devices must not be used or accessible while educators are working with children, unless formally authorised for essential purposes
- Any approved use of personal devices must be limited, justified, and must not impact supervision or child safety
- Images and videos of children must be managed in a way that protects their privacy, dignity, and safety
- Parents are encouraged to remain off their phones while at the service or attending service-based events.

# Device register

- Each service must have a current device register. This register must:

  a) Record the supply of the device in writing

  b) Include the following information in the written record:

    - The date the supply of the device;
    - The type of device that is supplied;
    - If available, the make, the model, and serial number of the device;
    - A declaration that the device is configured to operate in accordance with the service's policies and procedures that relate to child safety or the security of devices;
    - The name and signature of the approved provider or authorised delegate of the approved provider supplying the device;
    - If applicable, the date of any revocation of the supply of the device and the name and signature of the approved provider or authorised delegate authorising the revocation;

  c) Keep a record of the supply of the device and any revocation of the supply of the device in a safe and secure place at the service premises for a minimum period of three (3) years from the date the record was made.

- When a device is broken or no longer required, it must be returned to the IT team. The date the device is removed from service must be recorded in the device register.
- Where a new device is required, the Nominated Supervisor is responsible for arranging this through the IT team to ensure appropriate software and security requirements are met. Once issued, the device must be recorded in the device register.
- Educators and services are not permitted to independently purchase devices. All devices must be approved and supplied through the IT team to ensure compliance with organisational requirements, including security, software, and compatibility standards.

# Who is responsible?

| Roles | Responsibilities |
|---|---|
| **Approved Provider** | • Ensure the service has policies and procedures in place that align with legislation, the National Quality Framework, and the National Model Code<br>• Ensure systems are in place for the safe use, storage, and monitoring of digital devices<br>• Provide approved digital devices and ensure all devices meet organisational IT, security, and child safe requirements<br>• Ensure appropriate training, guidance, and oversight are provided to staff<br>• Monitor compliance and respond to any breaches of this policy |
| **Practice Manager** | • Support services to implement this policy consistently across all locations<br>• Monitor compliance through visits, audits, and practice review<br>• Provide coaching and guidance to Nominated Supervisors and Educators<br>• Ensure risks relating to digital device use are identified and managed<br>• Escalate concerns or breaches in line with organisational procedures<br>• Ensure device registers are approved.<br>• Ensure phone registers are up to date for their cluster. |
| **Nominated Supervisor** | • Ensure this policy is implemented within the service on a day-to-day basis<br>• Maintain and monitor the device register, ensuring all devices are recorded, approved, and managed appropriately<br>• Ensure all required authorisations and consents are obtained and stored<br>• Monitor the appropriate use of devices, including storage, deletion, and access of images and videos<br>• Ensure Educators supervise children when using digital devices and that device use aligns with the program<br>• Conduct risk assessment and manage any authorised use of personal devices or children's devices<br>• Address and respond to any breaches of this policy<br>• Ensure Educators do not have personal devices on them unless appropriate authorisation has been granted<br>• Must ensure that if personal devices are brought on excursions, they are stored in the excursion bag when required. |
| **Educators / Volunteer / Student** | • Follow this policy and all related procedures at all times<br>• Use only service-issued devices for work-related purposes, including taking images or videos of children<br>• Ensure children's privacy, dignity, and safety are maintained when using digital devices<br>• Actively supervise children when using digital technology and support safe and responsible use<br>• Use digital devices intentionally to support the educational program<br>• Ensure images and information are handled securely and not shared inappropriately<br>• Seek approval where required for any authorised use of personal devices.<br>• Ensure personal devices are locked away.<br>• When on excursions, if personal devices are not left at the service, they must be stored in the excursion bag. |

| Roles | Responsibilities |
|---|---|
| **Parents / Guardians** | • Provide written consent for images or videos of their child as part of the enrolment process and may withdraw this consent at any time<br>• Support the service by following expectations regarding children's personal devices and wearable technology<br>• Engage in communication with the service regarding the use of digital technology in the program<br>• Respect service policies regarding privacy, including the use and sharing of images.<br>• Ensure personal devices are not used while in the service premises unless required for service-related purposes, such as accessing QR codes or completing enrolment documentation. |

# National Quality Standards (NQS)

| Quality Area 2: Children's Health & Safety | | |
|---|---|---|
| 2.2 | Each child is protected. | Each child is protected. |
| 2.2.1 | Supervision | At all times, reasonable precautions and adequate supervision ensure children are protected from harm and hazard. |
| 2.2.2 | Incident and emergency management. | Plans to effectively manage incidents and emergencies are developed in consultation with relevant authorities, practises and implemented. |

| Education and Care Services National Law and National Regulations | |
|---|---|
| S. 167 | Offence relating to protect of children from harm and hazards |
| S. 165 | Offence to inadequately supervise children. |
| 168 (ha) | The safe use of digital technologies and online environments at the service, including - |
| 170 | Policies and procedures to be followed |
| 181 | Confidentiality of records kept by approved provider |
| | Education and care services (supply, authorisation and use of devices) order 2025 |
| | National Model Code |

# Related documents

## CatholicCare policy

- *Agency – Child Safe Policy*

## Children's Services Policies or Guidelines

- *Child Safe Environment Policy*
- *Confidentiality and Privacy Policy*
- *Excursion and Incursions Policy*
- *Family Participation and Collaboration Policy*
- *Supervision Policy*

## Forms

- *Authorisation for Use of Staff's Personal Electronic Device*
- *Authorisation for Use of Child's Personal Device*
- *Before and After School Care Enrolment Form*
- *Safe Digital Technologies and Online Environments Risk assessment*
- *Risk Minimisation Plan for Children with Diagnosed Medical Conditions*

# Resources

## External

- *Education and Care Services National Regulations 2011 (current version as of 1 January 2025)*
- *Education and Care Services National Law Act 2010*
- *Education and Care Services (Supply, Authorisation and Use of Devices) Order 2025*
- *Safe use of devices in education and care services | ACECQA – National Model Code*

# Glossary

**ACECQA – Australian Children's Education and Care Quality Authorities**

The independent national authority that works with all regulatory authorities to administer the National Quality Framework, including the provision of guidance, resources and services to support the sector to improve outcomes for children.

**OSHC**

Out of School Hours Care

**Practice Manager**

A practice manager oversees and supports a cluster of services within a local area. They work with the Nominated supervisor to ensure services operate safely, meet legal and quality requirements, and follow organisational policies. They do not work directly with children day to day.

**Personal Device**

A personal device is any privately owned electronic device that belongs to an individual, rather than the service or organisation. This includes items such as: mobile phones, smart watches, tablets or iPads, and other personal devices.

**Risk Assessment**

A systematic process of evaluating the potential likelihood and consequences of risks that may be involved in a projected activity or undertaking.

# Sign off and review

This document remains valid until it is either superseded by a new version or officially revoked.

CatholicCare values your input and welcomes feedback on this policy. Your suggestions help us improve and better support your work. Please send any feedback to policy.updates@catholiccaredbb.org.au.

| Version | Authorised by | Approved date | Review cycle | Review due |
|---|---|---|---|---|
| 6.0 | General Manager Children's Services | 10 June 2026 | 3 years | June 2029 |

# Revision history

| Version | Description | Author | Amendment date |
|---|---|---|---|
| 6.0 | Policy – supersedes Use of Media and Technology policy | Practice Manager Quality, Compliance and Business Development | 15 May 2026 |