Sydney Catholic early childhood services

Policy Document

Child Safe Digital Technology Policy

Policy Hierarchy link	Education and Care Services National Law Act 2010: 161, 161A, 162,162A, 165, 167 Education and Care Services National Regulation 2011: 84, 117A, 117B, 117C, 161, 168, 170, 171, 172, 181, 183 Australian Child Protection Legislation Australian Privacy Principals Privacy Act 1988

Version	Approved by	Effective Date	Revision Date
2	COO	September 2025	September 2028

1. PURPOSE

In today's digitally connected world, the safe and responsible use of digital technologies in early childhood education and care is paramount. This policy outlines the service's commitment to ensuring the safety and well-being of children.

Key considerations for educators, students and volunteers utilising digital devices in the service context include:

- Supporting the implementation of child-safe practices when using electronic devices for the taking, use, storage and destruction of images or videos of children being educated and cared for by the service.
- Increasing awareness of educators, students, volunteers, and families regarding safety risks associated with using electronic devices in the service and implementing strategies to support child safety.
- Implementing child-safe practices regarding the use of electronic devices across the service context in preparation for the potential regulatory changes predicted by the Education and Care Services National Law 2010, in line with the National Model Code in response to the Review of Child Safety Arrangements under the NQF.
- Obtaining authorisation from parents to take, use and store images and videos of children being educated and cared for by the service.

2. SCOPE

Children have the fundamental right to be safe and protected from digital exploitation. All staff have a responsibility to ensure that children's interactions with digital technologies are secure and their personal information and any images or videos used in the service are safeguarded.

Our service is committed to exercising its duty of care, to do everything that is reasonably practicable to avoid potential digital threats and maintain children's right to digital safety and privacy. Our team members will exercise their duty of care by:

- Creating a safe, supportive, and informed environment where digital technologies can enhance learning whilst prioritising the safety and security of every child in care.
- Establishing a nurturing and secure environment prioritising every child's well-being, safety, and development.
- Committing to fostering a culture of vigilance and care in which all children feel protected, supported, and valued.
- Providing children with the opportunity to maintain their rights and dignity, express their autonomy, and have the right to say no if they do not want their photo or video taken.
- Using devices with purpose to enhance learning and support development.
- Recognising that digital technology is a valuable tool when used intentionally with children to extend and support active, practical, creative, and authentic engagement with their surroundings, the community and the world.
- Supporting children to use digital technology, when applicable, with intentionality to inform and educate children on how to safely use digital devices and support children's positive relationships with different forms of technology.

3. POLICY STATEMENT

The service adopts the National Model Code and the accompanying Guidelines developed by ACECQA (Australian Children's Education and Care Quality Authority). These resources will be used in the service to implement child-safe practices and enhance awareness of the associated risks and considerations when educators, students, and volunteers use personal and service devices.

To create a digitally safe environment for the children in care, the service will:

- Provide and enforce the use of centre-owned devices for all digital activities involving children.
- Regularly update and maintain these devices with the latest security software and firmware.
- Not permit personal devices for work-related tasks to minimise the risk of data breaches.
- Develop and enforce strict privacy policies that govern the collection, storage, and sharing of children's digital information.

- Ensure that all digital content, such as photos and videos, is stored securely and access is limited to authorised personnel only.
- Obtain consent from parents and guardians before sharing any digital media involving their children.
- Obtain consent from children, whenever possible, before capturing or sharing any digital media involving themselves.
- Do not share children's images and digital media in online platforms without parent/guardian permission.
- Provide specific training on the centre's privacy policies and the proper use of centre-owned devices.
- Keep staff updated on the latest trends and threats in digital safety to ensure they remain vigilant and informed.
- Implement audits of digital device usage to ensure compliance with established policies and procedures.
- Conduct regular digital content and storage audits to identify and address potential security vulnerabilities.

When children are supported to use digital technology, the service will:

- Ensure age-appropriate, active, and engaging use of technology accompanied by an educator.
- Service the interests of the children and their provocations identified through play.
- Encourage exploratory play and enhance children's learning using technology.
- Allow children to engage in multimodal use of technology such as images, text, video and audio.
- Offer insight into the role, use, and presence of technology in today's world.
- Educate children on how to use digital platforms safely. For example, tell children to always communicate with team members and educators if they feel unsafe using digital devices.
- Support a positive relationship with digital technologies and devices, avoiding glorifying and condemning its use in the program.

4. ROLES AND RESPONSIBILITIES

The approved provider will:

- Apply the National Model Code and Guidelines for taking images or videos of Children while enrolled and providing education and care in the service.
- Ensure all educators, students and volunteers sign and adhere to the Child Safe Code of Conduct.
- Establish and maintain processes for the ongoing monitoring and review of any authorised use of service and personal electronic devices.

- Ensure that all related policies, including but not limited to privacy and confidentiality, child-safe environments, child protection, relationships with families and record keeping, are in line with this policy.
- Review and update digital safety policies and procedures to keep up with technological advancements and emerging risks.
- Establish procedures for the ongoing monitoring and review of centre-owned electronic devices to ensure their use aligns with authorised guidelines and remains appropriate.
- Provide educators, students, and volunteers, with training and professional development on digital safety practices, including recognising and mitigating risks associated with digital technologies.
- Communicate with families about digital safety practices, involving them in discussions about how digital devices are used within the service and any associated risks.
- Establish secure access controls used to manage who can use digital devices and access digital content, ensuring that only authorised individuals can access sensitive information and technology.
- Establish the process to obtain parent authorisations to take, use and store images and videos of children via the enrolment form.
- Establish protocols for safe online interactions, including supervision of children's online activities and the use of appropriate filters and monitoring software.
- Update software and security measures on all digital devices regularly to protect against viruses, malware, and other cybersecurity threats.
- Encourage responsible and respectful use of technology to promote a culture of digital responsibility among educators, students, and volunteers.
- Maintain clear documentation of any digital safety incidents and establish a protocol for reporting and addressing these incidents promptly, as part of the governance duty of care.
- Establish processes for safe digital record keeping, in line with the recommendations of the Royal Commission into Institutional Responses to Child Sexual Abuse; Section 175 of the National Law: Offence relating to requirement to keep enrolment and other documents; and Regulation 177 of the National Regulations: Prescribed enrolment and other documents to be kept by approved provider.

The nominated supervisor will:

- Support the approved provider in applying the National Model Code and Guidelines for taking images or videos of children while enrolled and providing education and care in our service.
- Ensure all educators, students and volunteers sign and adhere to the Child Safe Code of Conduct.
- Support the approved provider to develop and maintain service policies and procedures.

- Ensure that all digital safety policies and procedures are effectively implemented and adhered to within the service.
- Coordinate and provide ongoing training and education for educators, students, and volunteers on digital safety practices, including responsible use of electronic devices and recognising potential risks.
- Develop effective onboarding programs to ensure educators, students, and volunteers are informed about the safety and responsibility of using service digital devices safely in the centre.
- Keep families informed about digital safety measures, policies, and any updates or changes.
- Facilitate regular reviews and audits of digital device usage, ensuring that authorisations are current, and devices are used appropriately and safely.
- As part of the service's child-safe practices, encourage a culture of digital responsibility and safety among educators, students, volunteers, children, and families, fostering an environment where all stakeholders understand the importance of digital safety.
- Stay current with the latest developments in digital safety and cybersecurity and ensure this knowledge is shared with educators, students, and volunteers and incorporated into practice.
- Ensure that appropriate access controls, such as passwords and user permissions, are in place to protect sensitive information and limit access to authorised personnel only.
- Promptly address digital safety incidents, documenting them accurately and taking necessary actions to mitigate risks and prevent future occurrences.
- Provide feedback to educators, students, and volunteers who are found using personal devices during work hours and implement appropriate action for non-compliance of policies and procedures.
- Work closely with the approved provider to regularly review and update digital safety policies and procedures, ensuring they remain practical and relevant.
- Implement and monitor the processes for safe digital record keeping, in line with the recommendations of the Royal Commission into Institutional Responses to Child Sexual Abuse, Section 175 of the National Law: Offence relating to requirement to keep enrolment and other documents and Regulation 177 of the National Regulations: Prescribed enrolment and other documents to be kept by approved provider.

Educators will:

- Adopt the services implementation of the National Model Code and Guidelines for taking images or videos of children while enrolled and providing education and care in the service.
- Sign a Child-safe Code of Conduct that emphasises the importance of child safety in the service, including using digital technologies safely.
- Ensure digital safety when taking photos and video materials and documenting children's development while avoiding accessing centre information using personal devices during and outside work hours.

- Implement locking systems and passcodes on their personal devices for centre applications.
- Use centre-provided cameras or devices to take photos and document children's development, not personal devices.
- Ensure that written consent is obtained from parents or guardians and children, when applicable, before sharing any photos or videos of children using the centre devices.
- Adhere to the centre's privacy policies when documenting children's development, ensuring that images and videos are stored securely and shared only with authorised individuals.
- Store all photos, videos, and documentation on secure, password-protected devices or cloud services provided by the centre. Regularly back up data and ensure it is accessible only to authorised personnel.
- Be prohibited from using personal devices to obtain, access or store centre information. Be prohibited from using personal applications (Apps) and programs in their personal devices to obtain, store or access centre information. *(service to adjust according to centre procedures)*
- Utilise only secure, centre-approved platforms and applications for accessing and sharing information. Ensure that these platforms are used exclusively on centre-owned devices. *(if applicable to the centre)*
- Comply with regular reminders from your nominated supervisor about the importance of not using personal devices for work-related tasks and the potential risks involved.
- Follow clear rules and guidelines that personal devices should not be present in areas where children are being cared for.
- Have designated areas where educators, students, and volunteers can use their devices during breaks.
- Be provided with secure storage for personal devices during work hours to minimise distractions and prevent unauthorised use.
- Lead by example by not using personal devices in the presence of children and encourage a culture of full engagement and attention while interacting with children.
- Provide feedback to staff who are found using personal devices during work hours and will face disciplinary action for repeated non-compliance.
- Inform nominated supervisor of non-compliance with this policy.
- Not be permitted to document or record conversations and information that is private and confidential using personal devices.
- Not be permitted to obtain, access and store images and videos relating to educators, students, volunteers, children and families from personal devices.
- Educate children in acceptable and unacceptable behaviours (from adults and children) when children use digital devices and engage in digital platforms.
- Support children using digital devices to enhance their skills and development while cultivating a positive relationship with digital devices and platforms.

5. Resources / References

- ACECQA's Guide to the National Quality Framework – www.acecqa.gov.au/nqf/about/guide
- Australian Children's Education and Care Quality Authority (ACECQA) – www.acecqa.gov.au
- Policy and procedure guidelines – GUIDELINES FOR THE NATIONAL MODEL CODE - www.acecqa.gov.au/sites/default/files/2024-07/Guidelines%20for%20the%20National%20Model%20Code%20Taking%20Images%20and%20Videos.pdf
- National Model Code - www.acecqa.gov.au/sites/default/files/2024-07/National%20Model%20Code%20FAQS%20-%20Final.pdf
- ECA Code of Ethics (2016) Early Childhood Australia – www.earlychildhoodaustralia.org.au
- eSafety Commissioner - www.esafety.gov.au/educators/community-education
- ECA - eSafety early years program - learninghub.earlychildhoodaustralia.org.au/esafety-early-years-program
- NSW Office of the Children's Guardian - https://ocg.nsw.gov.au/
- NSW Dept of Education: Guide on the Child Safe Standards for early childhood education and outside school hours care services - education.nsw.gov.au/content/dam/main-education/early-childhood-education/working-in-early-childhood-education/media/documents/Guide_Child_Safe_Standards.pdf
- (NSW specific) Child Safe Standards: Key messages for early childhood education sector - Fact Sheet - education.nsw.gov.au/content/dam/ main-education/early-childhood-education/working-in-early-childhood-education/media/documents/Child_Safe_Standards_ECE.pdf
- United Nations Convention on the Rights of the Child - www.unicef.org.au
- Australian Human Rights Commission – www.humanrights.gov.au
- Australian Centre for Child Exploitation - www.accce.gov.au/help-and-support/what-is-online-child-exploitation
- SCECS Privacy Policy, Providing a Child Safe Environment Policy, Enrolment and Orientation Policy and Participation of Volunteers and Students Policy

6. Monitoring, evaluation, and review

Version	Authorised by	Date	Sections modified
1	Operations Manager	February 2025	New Policy
2	COO	SEP 2025	Policy contains information regarding the taking, use, storage and destruction of

			images and videos of children being educated and cared for by the service and obtaining authorisations from parents.