



SAFE USE OF DIGITAL TECHNOLOGIES AND ONLINE ENVIRONMENTS POLICY

Version 1.0
Date: 28/08/2026



POLICY

1. BACKGROUND

PCYC Out of School Hours Care (OSHC) Service is committed to fostering a culture that promotes and maintains safe, inclusive and supportive environments for children, both physically and online. As a child-safe organisation, we embed the National Principles for Child Safe Organisations and take a proactive approach to identifying, managing and reducing risks to children’s safety and wellbeing in all contexts, including digital environments.

Digital technologies are an increasingly integrated part of children’s daily lives, shaping how they learn, communicate and engage with the world. It is therefore essential that educators are not only confident in the use of digital technologies, but also able to guide children in developing the knowledge, skills and understanding needed to interact with these technologies safely, responsibly and respectfully.

Recent amendments to the *Education and Care Services National Law and Regulations*, including the introduction of strengthened child safety provisions (Part 6A) and the *Education and Care Services (Supply, Authorisation and Use of Devices) Order 2026 (NSW)*, have further reinforced the importance of robust practices in the safe use of digital technologies. Additionally, the National Model Code and Guidelines for taking images or videos of children highlight the need for strict controls around device use, privacy and data security.

This policy has been developed to reflect these legislative requirements and to ensure that the Service embeds best practice approaches to digital safety, privacy and child wellbeing. It provides a clear framework to support educators, families and the wider community to work collaboratively in creating a safe and responsible digital environment for all children.

2. PURPOSE

PCYC OOSH is committed to ensuring that the safety, wellbeing and rights of children are upheld at all times, including within digital and online environments. Guided by our Service philosophy and commitment to child-safe principles, we recognise our responsibility to provide and maintain an environment that is safe, secure, respectful and inclusive for children, educators, families, visitors and contractors.

This policy reflects our belief that children’s rights, voices and best interests are central to all decision-making. It supports the development of a proactive and reflective digital safety culture that aligns with our values, privacy obligations and legislative requirements, ensuring that the use of digital technologies enhances children’s learning and wellbeing without compromising their safety or dignity.

Document Number	POL-073	Document Owner	
Version	1.0	Business Unit	PCYC NSW OOSH

This policy establishes a consistent framework to guide:

- the safe, appropriate and intentional use of digital technologies and electronic devices within the Service
- the responsible capture, use, storage and deletion of images and video of children
- processes for obtaining informed written consent from parents/guardians
- the management and use of surveillance systems, where applicable
- the supervised, age-appropriate use of digital devices by children
- safe and ethical engagement with online environments, including emerging technologies such as artificial intelligence (AI) and digital platforms

PCYC OOSH Commitment to Children's Digital Safety:

At PCYC OOSH, we recognise that children have a fundamental right to be safe, respected and protected from harm, including within digital environments. This commitment is embedded within our Service philosophy, which values children as capable, competent and active participants in their own learning and wellbeing.

All educators have a professional and ethical responsibility to ensure that children's interactions with digital technologies are safe, secure and developmentally appropriate. We are committed to protecting children's personal information and ensuring that all images and videos are managed with respect, confidentiality and integrity.

Our approach to digital safety is informed by our strong commitment to children's rights, agency and voice. We actively support children to understand and navigate digital environments in ways that promote safety, confidence and positive engagement.

PCYC OOSH demonstrates this commitment through everyday practice by:

- creating a safe, inclusive and supportive environment where digital technologies are used intentionally to enhance learning while prioritising children's safety and wellbeing
- fostering a culture of respect, care and shared responsibility, where all children feel valued, supported and protected
- respecting children's agency and autonomy, including their right to make decisions about being photographed or recorded
- using digital technologies purposefully to support children's development, wellbeing, self-regulation and leisure experiences
- recognising digital technologies as meaningful tools that can extend children's creativity, engagement and connection to their world when used thoughtfully
- supporting children to develop the knowledge, skills and confidence to use digital technologies safely and responsibly

- engaging children in conversations about digital safety, encouraging them to express their views and contribute to decisions that affect them

3. SCOPE

This policy applies to all individuals involved in or accessing PCYC OOSH and outlines expectations for the safe and responsible use of digital technologies and online environments across all areas of Service operation.

It includes the use of digital devices, electronic systems and online platforms utilised for educational programming, communication, documentation, administration and any activity where children may be present or impacted.

This policy applies to:

- Children enrolled at PCYC OOSH
- Educators, staff and management
- Approved Provider and persons with management and control
- Students and visitors
- Families and external professionals (including ECIP practitioners)

This policy relates to all children, families, visitors and stakeholders accessing PCYC OOSH services and aligns with:

- National Quality Framework (NQF)
- Quality Area 2 – Children’s Health and Safety
- Quality Area 7 – Governance and Leadership
- Education and Care Services National Law and Regulations
- Education and Care Services (Supply, Authorisation and Use of Devices) Order 2026 (NSW)
- National Model Code and Guidelines for Taking Images or Videos of Children
- National Principles for Child Safe Organisations

4. RESPONSIBILITY

PCYC OOSH adopts a whole-of-service approach to digital safety, where responsibility is shared across leadership, educators, families and the wider community. All stakeholders are expected to actively contribute to maintaining a safe, respectful and secure digital environment that prioritises children’s safety, wellbeing and privacy.

4.1 Approved Provider / PCYC Management

The Approved Provider and PCYC Management are responsible for ensuring strong governance, compliance and leadership in relation to digital safety practices across the Service.

They will:

Governance and Compliance

- Ensure compliance with the *Education and Care Services National Law* (including Part 6A), National Regulations and the *Education and Care Services (Supply, Authorisation and Use of Devices) Order 2026 (NSW)*
- Establish, implement and regularly review policies, procedures and risk assessments relating to digital technologies
- Ensure all staff, students, volunteers and visitors understand and adhere to this policy
- Take reasonable steps to prevent and respond to breaches of this policy
- Ensure families are informed of this policy and able to access it
- Support families from diverse backgrounds to understand requirements, including consent processes
- Ensure all staff complete mandatory child safety training
- Embed child safe practices in line with the National Principles for Child Safe Organisations
- Remain informed of updates to privacy legislation and guidance
- Maintain clear complaint handling processes for digital safety concerns

Systems, Devices and Data Management:

- Provide and maintain secure, Service-supplied devices configured in accordance with Service requirements
- Implement systems for the secure storage, access and retention of digital information
- Maintain a register of all Service-issued devices, including allocation and usage
- Ensure devices are labelled, tracked, password-protected and securely stored when not in use
- Restrict access to authorised personnel only
- Ensure data is stored, backed up and destroyed in accordance with retention policies
- Notify the Office of the Australian Information Commissioner in the event of a data breach

Child Safety Leadership:

- Promote a strong child-safe culture across all digital and physical environments
- Ensure mandatory reporting obligations are understood and met
- Maintain appropriate educator-to-child ratios and active supervision
- Ensure students, volunteers and visitors are never left alone with children
- Conduct and review risk assessments relating to digital technologies
- Review practices following incidents or emerging risks and implement improvements
- Install and maintain appropriate internet filtering and security systems
- Ensure all concerns or incidents are documented, responded to promptly, and reported where required

Physical Environment and Supervision:

- Ensure the physical environment supports safe use of digital technologies
- Minimise supervision blind spots and maintain line-of-sight supervision
- Ensure children only use devices in open, supervised areas
- Monitor and manage risks such as inappropriate content, unsafe online interaction or sharing of personal information
- Conduct risk assessments for excursions and offsite use of devices

4.2 Personal Device Restrictions and Exemptions

PCYC OOSH enforces strict controls on personal electronic devices:

- Personal devices must not be used while working directly with children
- Personal devices must not be used to capture, store or share images or information about children
- Devices must be stored during shifts and only used in designated staff areas during breaks
- These requirements apply to staff, students, volunteers and visitors
- External professionals (e.g. NDIS or ECIP practitioners) may only use approved work-issued devices

Document Number	POL-073	Document Owner	
Version	1.0	Business Unit	PCYC NSW OOSH

Exemptions:

Exemptions may be granted in limited circumstances, including:

- Emergencies or critical incidents
- Medical or accessibility needs
- Emergency alerts (e.g. bushfires, floods, service lockdown etc)

All exemptions must:

- Be approved in writing
- Be reviewed every 3 months (NSW requirement)
- Never involve capturing images or videos of children
- Be documented and securely stored

4.3 Nominated Supervisor / Coordinator

The Nominated Supervisor/Coordinator is responsible for the implementation and oversight of this policy in daily practice and is required to adhere to the same standards, expectations and requirements as educators.

They will:

- Ensure consistent application of the policy across the Service
- Provide leadership, guidance and supervision to staff
- Ensure stakeholders understand their responsibilities
- Monitor use of digital technologies and address risks or non-compliance
- Manage and respond to incidents, complaints and concerns
- Support staff in maintaining safe and appropriate digital practices

4.4 Educators and Staff

Educators and staff are responsible for maintaining safe, respectful and compliant use of digital technologies.

They will:

- Adhere to this policy and all related procedures
- Not wearing a Smart Watch when rostered on and if visiting the service at anytime
- Lock personal devices (phones) away when rostered on

- Not to use personal devices to capture images or recordings of children
- Maintain active supervision when children use digital technologies
- Use only Service-supplied or approved devices
- Protect passwords and maintain confidentiality of all information
- Seek consent and respect children's privacy and preferences
- Ensure all content is age-appropriate and culturally respectful
- Avoid using screen time for behaviour management and self-regulate/calming time
- Promote and teach safe online behaviours to children
- Promptly report any concerns, incidents or breaches
- Participate in induction and ongoing training in digital safety and privacy
- Engage in discussions regarding emerging risks and best practice

4.5 Families

Families are expected to support the Service's approach to digital safety by:

- Adhering to this policy and associated procedures
- Not photographing or recording other children
- Providing consent for images and notifying any changes
- Respecting confidentiality and privacy requirements
- Not sharing Service-related images or content online without written permission
- Not allow their child to bring a phone, smart watch, talk to text watch to the OOSH service

4.6 Visitors and External Professionals

Visitors and external professionals must:

- Always comply with this policy at all times
- Do not wear a Smart Watch (you will be asked to remove your smart watch when you enter the service and sign in as a visitor)
- Not to use a personal electronic device to capture images or recordings of children
- Report any concerns regarding child safety or digital practices
- Obtain written authorisation before capturing images where applicable

4.7 Images, Video and Authorisation

PCYC OOSH will:

- Obtain written parent/guardian consent before capturing images or videos (enrolment form, vacation care booking form, during a PCYC OOSH promotional activity)
- Respect children's preferences and right to refuse
- Maintain a confidential list of children without photo consent
- Only use Service-supplied devices for capturing images
- Ensure images are appropriate, respectful and purpose-driven
- Prevent transfer of images to personal devices
- Obtain consent for external photographers or professionals
- Provide alternative arrangements for children without consent

4.8 Software, Applications and Artificial Intelligence (AI)

The Service will:

- Use only approved, secure digital platforms and applications
- Ensure all systems are password protected and access is restricted
- Regularly review and update software

Artificial Intelligence Use (AI):

- AI may be used as a support tool for planning or administration
- Educators must verify accuracy of AI-generated content
- Personal or identifying information must not be entered into AI systems

4.9 Closed Circuit Television (CCTV) - if applicable

Where CCTV is used in a PCYC Club that PCYC OOSH & Vacation Care attend or operate from, PCYC OOSH will:

- Inform families and display clear signage
- Ensure cameras are visible and not installed in private areas
- Restrict access to authorised personnel
- Store footage securely
- Only release footage in accordance with legal and regulatory requirements

Document Number	POL-073	Document Owner	
Version	1.0	Business Unit	PCYC NSW OOSH

4.10 Breach of Policy

Failure to comply with this policy may result in:

- Disciplinary action for staff
- Termination of engagement for visitors and external professionals
- Review or termination of enrolment for families

Serious breaches will be reported to regulatory authorities and child protection agencies.

4.11 Device Use and Restrictions in PCYC OOSH Services:

Device Type	Permitted in Program Areas?	Can Be Used While Working Directly With Children?	Conditions / Reason
Personal mobile phones/smartphones	✗ No	✗ No	Personal devices capable of taking, storing or transmitting images, video or communications are prohibited while working directly with children.
Smart watches (Apple Watch, Samsung Watch, etc.)	✗ No	✗ No	Smart watches can send messages, make calls, access the internet and store information and are considered personal devices.
Talk-to-text watches	✗ No	✗ No	Prohibited under PCYC policy as they can send voice messages, dictate text messages, make calls, record audio, or communicate with others.
Children's communication watches (e.g. Spacetalk, SyncUP Kids, Gizmo Watch)	✗ No	✗ No	These devices can call, message, track location and transmit information. Their use is restricted to support child safety and supervision.
Personal tablets/iPads	✗ No	✗ No	Personal devices capable of capturing, storing or transmitting images are restricted.
Personal cameras or video cameras	✗ No	✗ No	Personal image-capturing devices are prohibited.
GoPro or action cameras	✗ No	✗ No	Personal recording devices are not permitted.
Smart glasses with camera or recording capability	✗ No	✗ No	Devices capable of recording or transmitting images pose a child safety risk.
Personal USB drives/external hard drives	✗ No	✗ No	Personal storage devices may store or transfer children's information and images
Personal audio recorders	✗ No	✗ No	Recording devices are not permitted without authorisation.
Service-owned mobile phones	✓ Yes	✓ Yes	Must be supplied by the service and used only for approved service purposes.
Service-owned tablets/iPads	✓ Yes	✓ Yes	Used for programming, communication, documentation and approved educational activities.
Service-owned cameras	✓ Yes	✓ Yes	Used in line with service policies, procedures and image consent requirements.
Service-owned computers and laptops	✓ Yes	✓ Yes	Used for service operations, record keeping and educational purposes.

5. Document Information

Version History

Version	Date	Document Number	Created By	Role	Reason
1.0	28 th August 2026	POL-073	Renee Murray	State Children's Services Manager	- This policy incorporates content from the former "PCYC Guiding Principles: Electronic and Social Media Policy", consolidating requirements into a single, comprehensive document. - A substantial revision of this policy has been undertaken to ensure alignment with recent amendments to the Education and Care Services National Law, including the introduction of Part 6A and strengthened child safety provisions such as the principle of paramount consideration. - Updated guidance and definitions relating to personal electronic devices, as provided by ACECQA (2026), have been integrated to ensure compliance with current regulatory expectations. - Clear subheadings have been introduced to improve structure, particularly in relation to the roles and responsibilities of the Approved Provider and Service Management. - Practical examples and supporting tables have been incorporated to enhance understanding of key terms and expectations for educators, families and other stakeholders.

Reviewed By

Version	Date	Reviewed By	Role	Reason
1.0				

Acceptance Signoff

Version	Date	Name	Role	Signature
1.0	02/09/2026	Craig Becroft	PCYC CFO	

Document Number	POL-073	Document Owner	
Version	1.0	Business Unit	PCYC NSW OOSH

