



Springwood and District Preschool Kindergarten

SAFE USE OF DIGITAL TECHNOLOGIES AND ONLINE ENVIRONMENTS POLICY

Please note this policy comes into effect from 1 September 2025.

Our Preschool is committed to fostering a culture that creates and maintains a safe online environment with support and collaboration from staff, families and community. As a child safe organisation, our Preschool embeds the [National Principles for Child Safe Organisations](#) and continuously addresses risks to ensure children are safe in physical and online environments. Digital technologies have become an integral part of many children's daily lives. For this reason, it is important that our educators are not only familiar with the use of digital technologies, but are able to guide children's understanding of, and ability to interact, engage, access and use a range of digital technology in a child safe environment.

NATIONAL QUALITY STANDARD (NQS)

QUALITY AREA 2: CHILDREN'S HEALTH AND SAFETY		
2.2	Safety	Each child is protected
2.2.1	Supervision	At all times, reasonable precautions and adequate supervision ensure children are protected from harm and hazard.
2.2.3	Child Safety and Protection	Management, educators and staff are aware of their roles and responsibilities regarding child safety , including the need to identify and respond to every child at risk of abuse or neglect (effective Jan 2026 change of wording for this element in yellow)
QUALITY AREA 7: GOVERNANCE AND LEADERSHIP		
7.1.2	Management System	Systems are in place to manage risk and enable the effective management and operation of a quality Preschool that is child safe . (effective Jan 2026 change of wording for this element in yellow)

EDUCATION AND CARE PRESCHOOLS NATIONAL LAW AND NATIONAL REGULATIONS	
S. 162A	Child protection training
S. 165	Offence to inadequately supervise children
S. 167	Offence relating to protection of children from harm and hazards
12	Meaning of serious incident

73	Educational Program
76	Information about educational program to be given to parents
84	Awareness of child protection law
115	Premises designed to facilitate supervision
122	Educators must be working directly with children to be included in ratios
123	Educator to child ratios – centre-based Preschools
149	Volunteers and students
155	Interactions with children
156	Relationships in groups
168	Education and care Preschools must have policies and procedures
170	Policies and procedures to be followed
171	Policies and procedures to be kept available
172	Notification of change to policies or procedures
175	Prescribed information to be notified to Regulatory Authority
176	Time to notify certain information to Regulatory Authority
181	Confidentiality of records kept by approved provider
183	Storage of records and other documents
184	Storage of records after Preschool approval transferred

RELATED POLICIES

Behaviour Guidance Governance Policy Child Safe friendly Organisation Policy Child Protection Policy Code of Conduct Policy's Complaints Policy Management Policy Educational Program Policy Family Communication Policy Governance Policy	Incident, Injury, Trauma, and Illness Policy Communication with Families Policy Interactions with Children policy Cyber Policy Privacy and Confidentiality Policy Programming Policy Record Keeping and Retention Policy Staffing Arrangements Policy Student, Volunteer and Visitor Policy Indoor Outdoor Supervision Policy Social media Policy
---	---

PURPOSE

Children's safety and wellbeing is paramount, and our Preschool has the responsibility to provide and maintain a safe and secure working and learning environment for staff, children, visitors and contractors, including online environments. We aim to create and maintain a positive **digital safe culture that works in conjunction with our preschool philosophy**, and privacy and legislative requirements to ensure the safety of enrolled children, educators and families.

The use of Close Circuit Television (CCTV) installed outside of the Preschool grounds aims to address crime prevention strategies to reduce concerns, deal with complaints and support investigations. Our Preschool adheres to the Privacy Act 1988 (Privacy Act) and comply with the Australian Privacy Principles.

In NSW, Australia, the Privacy Act 1988 is a federal law that protects individuals' personal information by setting rules for how it can be collected, used, and shared. It applies to government agencies and many private organisations, and is enforced through the Australian Privacy Principles (APPs)—13 guidelines that ensure transparency, security, and fairness in handling personal data. These principles cover things like giving people access to their own information, keeping data accurate and secure, and limiting how it's used or disclosed

SCOPE

This policy applies to children, families, staff, educators, management, approved provider, nominated supervisor, students, volunteers and visitors of the Preschool.

TERMINOLOGY	
Artificial intelligence (AI)	An engineered system that generates predictive outputs such as content, forecasts, recommendations, or decisions for a given set of human defined objectives or parameters without explicit programming.
Cyberbullying	When someone uses the internet to be mean to a child or young person so they feel bad or upset
Cyber safety	Safe and responsible use of the internet and equipment/devices, including mobile phones and devices.
Disclosure	Process by which a child conveys or attempts to convey that they are being or have been sexually abused, or by which an adult conveys or attempts to convey that they were sexually abused as a child
Generative artificial intelligence (AI)	A branch of AI that develops generative models with the capability of learning to generate novel content such as images, text and other media with similar properties as their training data
ICT	Information and Communication Technologies
Illegal content	Includes: images and videos of child sexual abuse Content that advocates terrorist acts Content that promotes, incites or instructs in crime or violence Footage of real violence, cruelty and criminal activity
Optical Surveillance Device	Has the same meaning as in section 6(1) of the Surveillance Devices Act 2004 of the Commonwealth
Online hate	Any hateful posts about a person or group based on their race, religion, ethnicity, sexual orientation, disability or gender
Smart toys	Smart toys generally require an internet connection to operate as the computing task is on a central server
Sexting	Sending a sexual message or text, with or without a photo or video. It can be done using a phone Preschool or any platform that allows people to connect via an online message or chat function
Unwanted contact	Any type of online communication that makes you feel uncomfortable, unsafe or harassed.

Source: Glossary to NQF Child Safe Culture and Online Safety Guides- ACECQA 2025

IMPLEMENTATION

Our Preschool uses digital technology and electronic devices for communicating with families and the wider community, supporting administration tasks and enhancing safety and security through systems such as sign in/out platforms and outdoor CCTV monitoring and at limited times tool for learning with children. Our educators are diligent in ensuring children are only able to access age-appropriate technology on a Preschool issued device.

DIGITAL TECHNOLOGY AND ELECTRONIC DEVICES USED AT THE PRESCHOOL

Our Preschool follows the [National Model Code](#) and Guidelines for taking images or videos of children. *(refer to attached document)*. Currently optional however, legislation is expected to change regarding the banning of personal electronic devices in ECEC Preschools making this mandatory and consequent breaches resulting in fines. However, **our organisation has this embedded practise. In our Child Safe Standards Policy & Child Safe Risk Assessment** – it already states that no staff members can use their own devices and must not have access to them within the classroom environment.

Procedures & practises are in place whereby educators, visitors, volunteers and family members that the use of ***personal electronic devices*** used to take photos, record audio or capture video of children who are being educated and cared for at the Preschool is strictly prohibited. This includes items such as tablets, phones, digital cameras, smart watches, META sunglasses and personal storage and file transfer media (such as SD cards, USB drives, hard drives and cloud storage). These devices should not be in the possession of staff, educators or visitors (e.g. OT professionals) while working directly with children.

Exemptions need to be provided and may include:

- Emergency communication during incidents such as a lost child, injury, lockdown, or evacuation
- Personal health needs requiring device use (e.g. heart or blood sugar monitoring)
- Disability related communication needs
- Urgent family matters (e.g. critically ill or dying family member)
- Local emergency event to receive alerts (e.g. government bushfire or evacuation notifications)

Children enrolled at our Preschool are not permitted to bring electronic devices to the Preschool, discussed with the nominated supervisor where the device may be required to support a diagnosed medical condition or disability. If a child brings an electronic device to the Preschool, it will be switched off and stored in a locked cupboard.

IMAGES AND VIDEOS

The nominated supervisor is responsible for determining who is authorised to take, use, store and destroy images and videos of children using Preschool issued digital devices. Images and videos will be stored securely with password protection. Images and videos of children must only be taken and used in accordance with Preschool policies, and careful consideration given to the purpose of the image or video. Educators will engage in discussions that consider the intent, appropriateness, context and consent involved in capturing and using the images and videos, ensuring the process aligns with children's learning, wellbeing and right to privacy.

Our Preschool will regularly review how digital data, including images and videos of children, is stored. Back-ups of all digital data will be transferred each **term to an external Hard drive that is stored and locked** for long term storage. Digital data stored at the Preschool will be destroyed in accordance with the **Information & Record Keeping Policy (19)** and procedure. The nominated supervisor will ensure staff, educators, visitors and volunteers do not transfer images or videos from Preschool issued devices to personal devices, unauthorised transferring of digital data may result in disciplinary action.

PHYSICAL ENVIRONMENT AND ACTIVE SUPERVISION

The approved provider, nominated supervisor, management and educators will:

- ensure children are always supervised and never left unattended whilst an electronic device is connected to the internet
- provide a child safe environment to children- reminding them if they encounter anything unexpected that makes them feel uncomfortable, scared or upset, they can seek support from staff
- reflect on our Preschool's physical environment, layout and design to ensure it supports child safe practices when children are engaged in using technology
 - perform regular audits to identify risks to children's safety and changes in room set-ups that can indicate areas of higher-risk and become supervision 'blind spots'
 - ensure location of digital technology/equipment allows educators to remain in line-of-sight of other staff members when working with children
 - only permit children to use devices in open areas where educators can monitor children's use
 - be aware of high-risk behaviours for children online, including uploading private information or images, engaging with inappropriate content (inadvertently or purposefully), making in-app purchases, and interacting with unsafe individuals
 - ensure all visitors and volunteers are supervised at all times
 - ensure all devices are password protected with access for staff only
- where digital devices are used during transportation and excursions, they must be used in accordance with practices outlined within this policy and associated procedure.

SOFTWARE PROGRAM (Hub works)

Our Preschool uses a secure software program Hubworks at preschool-issued devices to support administration of the Preschool. Any apps used by educators, are carefully selected, regularly checked and kept up to date with our computer support specialist who both managers and monitors our software and hard ongoing, Refer to our [Cyber Security Policy \(5.1\)](#). Access to software programs and apps are password protected to ensure the privacy of children, families and staff.

The nominated supervisor will ensure electronic which require additional background checks, such as Digital Hub works Software link, are only accessed by authorised staff who have completed necessary screening processes in accordance with Department of Education. At present the department mandate that every family and staff member sign a permission form to enable the Department (Digital Hub) to legally gather data on individuals. Our Preschool Administration side uses accounting systems and payroll software MYOB HR. These platforms assist in managing the Preschool's financial, staffing, and operational requirements.

ARTIFICIAL INTELLIGENCE (AI) INTERACTIONS AND GUIDELINES

*Educators or staff using AI are to be aware of limitations, privacy risks, and the potential for errors in the information it provides. AI can support and assist staff as a documentation tool; however, it is their responsibility to ensure the information's accuracy and not rely upon it as an authoritative source. Staff and educators should ensure they enter original work into the AI program and are required to monitor, verify, and check information obtained from AI to ensure specific details are contextually relevant. Data and privacy concerns must be addressed, and staff should not enter details which may identify individual children, such as names and date of birth. **This in September 2025 is emerging technology and will need to be assessed in the near future as this unpacks further.....***

CONFIDENTIAL AND PRIVACY GUIDELINES

Our *Privacy and Confidentiality Policy* & Cyber Policy applies to all use of digital technology and online environments. All staff, educators, and visitors must ensure that any information, images, or digital content related to children, families, and the Preschool is collected, stored, used, and shared in accordance with privacy legislation and Preschool procedures, to maintain confidentiality and protect the safety and wellbeing of children. The team will advise the nominated supervisor as soon as possible regarding any potential threat to security information and access to data sensitive information. Our Preschool will follow practices to protect personal and sensitive digital data.

The nominated supervisor will notify the Office of the [Australian Information Commissioner \(OAIC\)](#) in the event of a possible data breach by using the online [Notifiable Data Breach Form](#). This could include:

- a device containing personal information about children and/or families is lost or stolen (parent names and phone numbers, dates of birth, allergies, parent phone numbers)
- a data base with personal information about children and/or families is hacked
- personal information about a child is mistakenly given to the wrong person
- this applies to any possible breach within the Preschool or if the device is left behind whilst on an excursion
- ensure educators are aware of their mandatory reporting requirements and report any concerns related to child safety including inappropriate use of digital technology to the nominated supervisor or nominated supervisor.

IDENTIFICATION AND REPORTING OF ONLINE ABUSE AND SAFETY CONCERNS

Our Preschool will implement measures to keep children safe whilst using digital technology and accessing online environments.

The approved provider, nominated supervisor and management will:

- ensure all staff, educators, students and volunteers are aware of their mandatory reporting obligations and promptly report any concerns related to child safety, including inappropriate use of digital technology, to the nominated supervisor or nominated supervisor [See *Child Protection Policy*]
- support educators to:
 - encourage children to seek support if they encounter anything unexpected that makes them feel uncomfortable, scared or upset
 - listen sensitively and respond appropriately to any disclosures children may make relating to unsafe online interactions or exposure to inappropriate content, adhering to the *Child Protection Policy, Behaviour Guidance* and reporting procedures
 - respond to and report any breaches and incidents of inappropriate use of digital devices and online Preschools to management
- ensure all concerns are documented and responded to promptly and appropriately, with support provided to the child and their family as required
- *report any suspected cases of online abuse to the relevant authorities, including the eSafety Commissioner and Police, in accordance with legal requirements and child protection procedures*
- *notify the regulatory authority within 24 hours, via NQAITS, if a child is involved in a serious incident, including any unsafe online interactions, exposure to inappropriate content, or suspected online abuse.*

USE OF CLOSED-CIRCUIT TELEVISION (CCTV) MONITORING

Our Preschool uses Closed-Circuit Television (CCTV) to monitor the physical environment. Our Preschool will regularly review guidance on the use of surveillance devices, including information provided by the Office of the Australian Information Commissioner.

A sign is placed at the entrance of the Preschool to advise staff, families, and visitors about the surveillance. Closed-Circuit Television (CCTV) operates at the Preschool and comprises of:

- 8 fixed position cameras
- A monitor
- Digital Hard Drive Recorder
- Public Information Sign

CAMERA LOCATIONS The entrance and exit points

- Outside front door location
- Back of building behind wombat room
- Back of building where staff car park located
- Playground near garage focus along railway corridor
- Hill area outside playground
- Parent car park
- Doors to on veranda

The CCTV recording system operates in real mode, monitoring the site **continuously 24 hours a day**. Footage and information collected via the recording system will be governed by [Australian Privacy Principles](#). *In NSW, Australia, the Privacy Act 1988 is a federal law that protects individuals' personal information by setting rules for how it can be collected, used, and shared. It applies to government agencies and many private organisations, and is enforced through the Australian Privacy Principles (APPs)—13 guidelines that ensure transparency, security, and fairness in handling personal data. These principles cover things like giving people access to their own information, keeping data accurate and secure, and limiting how it's used or disclosed.* All relevant staff will be kept up to date with requirements under Australia's privacy law. CCTV footage is stored on a hard drive and is large enough to store back for 6 weeks before it over rights itself unless an incident is copied and stored for a specific incident.

Access to CCTV footage at the Preschool is strictly controlled and protected by secure, password-protected systems. Only authorised personnel are permitted to access the footage, in accordance with privacy laws and Preschool policies. The nominated supervisor is responsible for determining who is authorised to access CCTV footage. CCTV footage will not be accessible to external parties (e.g., staff members or families) without appropriate authorisation. Any requests to view CCTV footage will be managed in accordance with Australian Law.

Access to the recordings will only be disclosed to:

1. the NSW Ombudsman to assist with investigations on 'child protection' (e.g., risk of harm, abuse, neglect and ill treatment).
2. to a member or officer of a law enforcement agency e.g., Police for use in assisting with investigations.
3. the nominated supervisor or administrative person to investigate situations that may have occurred.

THE NOMINATED SUPERVISOR WILL ENSURE:

- that obligations under the *Education and Care Preschools National Law and National Regulations* are met
- educators, staff, students, visitors and volunteers have knowledge of and adhere to this policy and associated procedure
- new employees, students and volunteers are provided with a copy of the *Safe Use of Digital Technologies and Online Environments Policy* and procedure as part of **their induction** and are advised on how and where the policy can be accessed
- all staff, educators, volunteers and students are aware of current child protection law, National Principles for Child Safe Organisations and their duty of care to ensure that reasonable steps are taken to prevent harm to children
- families are aware of this *Safe Use of Digital Technologies and Online Environments Policy* and procedure and are advised on how and where the policy can be accessed
- they promote and support a child safe environment, ensuring adherence to the *Child Safe Organisation and Child Protection Policies*, including mandatory reporting obligations
- the National Principles for Child Safe Organisations is embedded into the organisational structure and operations.
- professional learning is provided to educators and staff relating to the safe use of digital technologies and online environments
- appropriate ratios and adequate supervision are always maintained for children including when using digital technology and accessing online environments
- students, volunteers and/or visitors are never left alone with a child whilst at the Preschool under any circumstances
- all staff, educators, volunteers and students are aware of the National Model Code and [Guidelines](#) and adhere to these taking images or video of children including:
 - personal electronic devices or personal storage devices, that can take images or videos, are not used by educators, staff, visitors or volunteers when working directly with children
 - staff and educators only use electronic devices issued by the Preschool for taking images or videos of children enrolled at the Preschool
 - Preschool issued devices are securely configured, monitored and maintained to prevent unauthorised access
- children, educators and parents are aware of our Preschool's complaints process to raise any concerns they may have about the use of digital technologies or any other matter (see: *Complaints Policy*)
- the Preschool *Privacy and Confidentiality Policy* is adhered to at all times by staff, educators, families, visitors, volunteers and students
- parents/guardians are informed of how the Preschool will take, use, store and destroy images and videos of children enrolled at the Preschool during enrolment and orientation
- written authorisation is requested from families to take, use, store and destroy digital documentation including images and videos of children
- images or videos of children are not taken, used or stored without prior parent/guardian authorisation
- written authorisation is obtained from parents/guardians for children to use electronic devices (See: *enrolment form*)
- written authorisation is obtained from parents/guardians to collect and share personal information, images or videos of their children online (Website, Facebook, press)
- digital data is stored securely, whether offline or online, using a cloud-based Preschool, and that data is archived regularly each term.

- images and videos are deleted or destroyed and removed from storage devices in accordance with the *Record Keeping Policy*, images and videos used for documenting children's learning and development must be held for 3 years after the child's last day of attendance
- external agencies or specialists are consulted if concerns are identified relating to online abuse, cyberbullying or digital safety risks
- policies and procedures reflect a commitment to equity and diversity, protect children's privacy, and empower children to be independent
- collaboration with relevant professionals, as required, to support equitable access to digital technologies for all children
- they remain informed of privacy legislation through monitoring of updated from relevant government authorities such as the Office of the Australian Information Commissioner (OAIC)
- a risk assessment is conducted regarding the use of digital technologies by staff and children at the Preschool, including accessing online environments
- risk assessments for digital technology and online environments (Child Safe Standards Risk Assessment) are reviewed annually or as soon as possible after becoming aware of any circumstances that may affect the safety, health or wellbeing of children
- policies and procedures are reviewed following an identification of risks following the review of risk assessments relating to the use of digital technologies and online environments
- staff, educators, families and children are informed of updates to policies, procedures or legislation relating to digital technologies and online environments
- a review of practices is conducted following an incident involving digital technologies or online environments, including an assessment of areas for improvement
- to install and maintain anti-virus and internet security systems including firewalls to block access to unsuitable web sites, newsgroups and chat rooms

EDUCATORS WILL:

- adhere to the *Safe Use of Digital Technologies and Online Environments Policy* and associated procedure
- ensure they are aware of current child protection law, National Principles for Child Safe Organisations and their duty of care to ensure that reasonable steps are taken to prevent harm to children
- ensure they promote and support a child safe environment, ensuring adherence to the *Child Safe Organisation* and *Child Protection Policies*, including mandatory reporting obligations
- participate in practical training related to digital safety, privacy protection and responsible use of technology
- understand the critical importance of implementing active supervision strategies when children are accessing online environments to keep children safe
- promote and contribute to a culture of child safety and wellbeing in all aspects of our Preschool's operations, including when accessing digital technologies and online learning environments
- not use, or have access to, any personal electronic devices, including mobile phones or smart watches used to take images or video of children at the Preschool, access social media (Facebook, Instagram or other) or breach children and families' privacy
- keep passwords confidential and log out of computers and software programs after each use
- ask permission before taking photos of children on any device and explain to children how photos of them will be used and where they may be published
- ensure children's personal information where children can be identified such as name, address, age, date of birth etc. is not shared online
- introduce concepts to children about online safety at age-appropriate levels
- support children's understanding of online safety by providing age-appropriate guidance, discussions and activities that help them to recognise safe and unsafe online behaviours

- consult with children about matters that impact them, including the use of digital technologies and online environments, to ensure their voices are heard and respected in a meaningful way.

FAMILIES WILL:

- adhere to the *Safe Use of Digital Technologies and Online Environments Policy* and associated procedure
- *not use personal electronic devices, such as mobile phones, smart watches or META sunglasses, to take photos, record audio, or capture video of children being educated and cared for at the Preschool*
- be aware that sometimes other children in the Preschool may feature in the same photos, videos, and/or observations as their children. In these cases, families are never to duplicate or upload them to the internet/social networking sites or share them with anyone other than family members.

VISITORS AND VOLUNTEERS WILL:

- adhere to the *Safe Use of Digital Technologies and Online Environments Policy* and associated procedure whilst visiting the Preschool
- not use personal electronic devices, such as mobile phones smart watches or META sunglasses, to take photos, record audio, or capture video of children being educated and cared for at the Preschool
- report any concerns related to child safety, including inappropriate use of digital technology, to the nominated supervisor or nominated supervisor
- obtain written authorisation from parents/guardians to capture images or video of a child for observation/documentation purposes only. This applies to visitors who are supporting children at the Preschool (NDIS funded support professionals, Inclusion Support professionals)

BREACH OF POLICY

Staff members or educators who fail to adhere to this policy may be in breach of their terms of employment and may face disciplinary action. Visitors or volunteers who fail to comply to this policy may face termination of their engagement. Family members who do not comply with this policy may place their child's enrolment at risk and limit the family members access to the Preschool.

RESOURCES

Australian Children's Education & Care Quality Authority. [National Model for Early Childhood Education and Care.](#)

[Australian Government Office of the eSafety commission](#)

[eSafety Early Years Program for educators](#)

[eSafety Early Years Program checklist](#)

[eSmart Alannah & Madeline foundation](#)

[Family Tech Agreement. eSafety Early Years Online safety for under 5s](#)

Kiddle is a child-friendly search engine for children that filters information and websites with deceptive or explicit content: <https://www.kiddle.co/>

Office of the Australian Information Commissioner (OAIC)

CONTINUOUS IMPROVEMENT/REFLECTION

Our *Safe Use of Digital Technologies and Online Environments Policy* will be reviewed on an annual basis in consultation with children, families, staff, educators and management. Families will be notified of

changes to policies within 14 days to ensure they remain informed and can provide feedback or ask questions as needed.

SOURCES

Australian Children's Education & Care Quality Authority. (2025). [Guide to the National Quality Framework](#)

Australian Children's Education & Care Quality Authority. (2023). [Embedding the National Child Safe Principles](#)

Australian Children's Education & Care Quality Authority. (2024). [Taking Images and Video of Children While Providing Early Childhood Education and Care. Guidelines For The National Model Code.](#)

Australian Children's Education & Care Quality Authority. (2025). [NQF Online Safety Guide](#)

Australian Government eSafety Commission (2020) www.esafety.gov.au

Australian Government Department of Education.(2025). [Child Care Provider Handbook](#)

Australian Government. [eSafety Commissioner Early Years program for educators](#)

Australian Government, Office of the Australian Information Commissioner. (2019). Australian Privacy Principles: <https://www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/>

Australian Government Department of Health and Aged Care. (2021). [Australia's Physical Activity and Sedentary Behaviour Guidelines](#)

Australian Human Rights Commission (2020). *Child Safe Organisations*. <https://childsafes.humanrights.gov.au/>

Early Childhood Australia Code of Ethics. (2016).

Education and Care Preschools National Law Act 2010. (Amended 2023).

[Education and Care Preschools National Regulations](#). (Amended 2023).

Office of the Australian Information Commissioner (OAIC)

Privacy Act 1988.

REVIEW

POLICY REVIEWED BY	Name	Management Committee	Date
POLICY REVIEWED	Name:	Management Committee	Date
MODIFICATIONS			
POLICY REVIEWED	New policy developed following changes to National Regulations effective from 1 September 2025 Merger of the following policies: Cyber Safety Policy		