Safe Use of Digital Technologies and Online Environments Policy

POLICY STATEMENT

Lake Mac Newy OOSH is committed to a culture that creates and maintains a safe online environment, with support and collaboration from staff, families and the community. As a child safe organisation, the Service embeds the National Principles for Child Safe Organisations and continuously addresses risks so that children are safe in both physical and online environments. Digital technologies are integral to children's daily lives; educators must be familiar with their use and able to guide children's understanding of, and ability to safely interact with, digital technology in a child safe environment.

The safety, welfare and wellbeing of the child is paramount in every decision made under this policy — including decisions about device use, image consent, online safety concerns and any restriction of a family's or visitor's access to the Service. The Service will provide and maintain a safe and secure working and learning environment for staff, children, visitors and contractors, including online environments, consistent with the Service philosophy and applicable privacy and legislative requirements.

Where Closed-Circuit Television (CCTV) is installed at a Service, it is used to support site security, respond to visitors or unexpected activity, assist complaint-handling and investigations, and enhance child safety. CCTV supplements, and does not replace, active supervision. The Service complies with applicable privacy, workplace-surveillance and record-management requirements, including the *Privacy Act 1988* (Cth), the Australian Privacy Principles and the *Workplace Surveillance Act 2005* (NSW).

SCOPE

This policy applies to children, families, staff, educators, management, the Approved Provider, the Nominated Supervisor, students, volunteers and visitors of the Service.

DEFINITIONS

- **Personal device** – a device not owned or issued by the Service, including a mobile phone, tablet, smart watch, camera-enabled wearable device (e.g. smart glasses), digital camera, personal computer, gaming device, and personal storage or file-transfer media such as SD cards, USB drives, external hard drives and personal cloud, email, messaging or social-media accounts.
- **Service-owned device** – a device purchased, issued or approved by the Service for operational or educational use, including computers, tablets, mobile phones, cameras and gaming consoles provided for the program.
- **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.
- **Generative artificial intelligence (AI)** – a branch of AI that develops generative models capable of learning to generate novel content, such as images and text, with properties similar to their training data.

- **Cyberbullying** – using 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 or devices, including mobile phones and other devices.
- **Disclosure** – the 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.
- **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; and footage of real violence, cruelty or criminal activity.
- **Optical surveillance device** – has the same meaning as in section 6(1) of the *Surveillance Devices Act 2004* (Cth).
- **Online hate** – hateful posts about a person or group based on race, religion, ethnicity, sexual orientation, disability or gender.
- **Smart toys** – toys that generally require an internet connection to operate, as the computing task runs on a central server.
- **Sexting** – sending a sexual message or text, with or without a photo or video, by phone service or any platform allowing people to connect via an online message or chat function.
- **Unwanted contact** – any online communication that makes a person feel uncomfortable, unsafe or harassed.

Source: Glossary to the NQF Child Safe Culture and Online Safety Guides, ACECQA 2025.

DIGITAL TECHNOLOGY AND ELECTRONIC DEVICES USED AT THE SERVICE

The Service uses digital technology and electronic devices as a tool for learning with children, documenting learning and development, communicating with families and the wider community, supporting program planning and administration, and enhancing safety and security through systems such as sign in/out platforms. Educators ensure children can only access age-appropriate technology on a Service-issued device.

The Service follows the National Model Code and Guidelines for taking images or videos of children. The Approved Provider, Nominated Supervisor, staff, volunteers and students may use only Service-supplied devices to capture, store or transmit images or videos of children being educated and cared for by the Service, and must not use a personal device for that purpose under any circumstances. Families, visitors, contractors and allied health or inclusion-support professionals must not photograph, record audio or capture video of children at the Service unless the activity has been specifically authorised under this policy and the associated procedure.

Approved providers, nominated supervisors, staff, volunteers and students must not use, or have in their possession or control, a personal device while working directly with children. For this purpose, working directly with children means being physically present with a child or children at the Service while employed, engaged or appointed to provide education and care. A person on a genuine break who is not physically present with children is not working directly with children for this purpose but must continue to comply with the Service's storage and security requirements.

Service-owned devices must not be removed from Service premises except for an approved operational activity — such as an excursion, transportation, an authorised off-site meeting, compliance work, or an approved work-from-home arrangement. Any personal-device exception during an excursion or transportation applies only where the device is genuinely necessary for the safety of children or the provision of education and care, and must be used in accordance with the National Law, this policy and the associated procedure.

Removal approval and security requirements

A Service-owned device may leave the premises only where its removal has been approved for an operational purpose, and the device is protected by appropriate security controls, including unique user access, password or biometric protection, automatic locking, encryption and — where technically available — an approved mobile device management solution and remote-wipe capability. The Service maintains dedicated IT administration responsible for configuring and securing all Service devices.

A Service-owned device that does not meet the required security controls must not leave the premises unless a documented risk assessment has been completed and the Operational Management Team has provided written approval. All approved removals are recorded on the removal-from-site schedule, including the device, responsible person, purpose, date removed, expected return date and confirmation of return.

Personal devices and exemptions

The Approved Provider may give a person prior written authorisation to use or possess a personal device while working directly with children only where the device is necessary for one of the grounds in section 175J(1) of the National Law:

- providing support or assistance with a disability or health need (e.g. heart or blood sugar monitoring);
- communicating with a family member (e.g. an urgent family matter, or a critically ill or dying family member);
- safety or the provision of education and care to children if a Service-supplied device ceases working;
- use in an emergency (e.g. lost child, injury, lockdown, evacuation, or a local emergency alert such as a bushfire warning); or
- work health and safety.

An authorisation under section 175J, or an exception applying during an excursion or transportation, does not permit a personal device to capture, store or transmit an image or video of a child under any circumstances.

All exemption requests must be submitted through the Service's designated exemption request form and approved in writing by the Approved Provider before the device is used or possessed while working directly with children. Where prior written authorisation is not practicable because of an emergency, the Approved Provider must document the authorisation as soon as practicable afterwards. Each authorisation is recorded in the Service's Exemption Register, including the authorised person's name and role, the person recording the authorisation on behalf of the Approved Provider, a description of the device, the authorised purpose, any conditions of use and the authorisation period. Records are retained for at least three years, and authorisations are reviewed regularly and cancelled when no longer necessary.

Any inappropriate or unauthorised use of a Service-owned or personal device — including photographing, video recording, accessing confidential information, or failing to comply with conditions of use — is a **breach of this policy**.

The Service maintains an *Electronic Device Register* of all electronic devices purchased for and used within the Service, including device type, date of purchase, intended use, assigned user (if applicable), security settings, and any connectivity, data-storage or recording features. Devices recorded may include computers, tablets, mobile phones, cameras, CCTV systems, audio recorders, smart toys, baby monitors and other internet-connected or data-enabled devices.

Children's own devices

Children are not permitted to bring or use personal electronic devices while attending the Service. This includes mobile phones, tablets, gaming devices, smartwatches, digital watches, and other wearable or electronic devices.

An exception may be approved only by the Approved Provider or Nominated Supervisor when a personal device is required for a documented health, disability, accessibility, communication, or safety need. Any approved arrangement must be documented and specify the purpose of the device, conditions of use, supervision arrangements, permitted functions and any storage or security requirements.

Where a personal device is approved for an identified need:

- the device must only be used for the approved purpose and in accordance with the documented arrangement;
- use must occur under appropriate educator supervision;
- the device must not be used to capture, store or transmit photographs, video or audio recordings unless specifically required for the approved health, disability, accessibility, communication or safety purpose and permitted by law;
- functions not required for the approved purpose must not be used; and
- the child must follow educator directions regarding the use and storage of the device.

Where a child brings a personal electronic device to the Service without an approved arrangement, the device will be switched off and stored securely, out of children's reach, until the child's departure or collection by an authorised nominee. Families will be reminded that personal electronic devices are not to be brought to the Service.

This restriction applies consistently to wearable digital devices, including smart watches and digital watches, regardless of whether the device has internet, communication, camera or recording capabilities. This supports effective supervision, privacy, child safety and a clear and consistent approach across the Service.

Any personal device brought onto Service premises remains the responsibility of the child and their family. The Service accepts no responsibility for loss, theft or damage.

Where a staff member becomes aware of content on a child's personal device that raises a child-safety concern, the device or its content must not be altered, deleted or further accessed beyond what is necessary to address the immediate safety concern. The matter must be reported immediately to the Nominated Supervisor or Responsible Person and managed in accordance with the *Child Protection Policy*, including any applicable reporting obligations.

Children with additional privacy restrictions

Where a child is in out-of-home care or subject to a court order restricting publication, no image of that child will be published to public channels. Consent conditions from the delegated authority will be followed and clearly flagged in the child's enrolment record. Footage or images in which that child appears will only be provided to relevant authorities, if requested.

IMAGES AND VIDEOS

The Approved Provider is responsible for determining who is authorised to take, use, store and destroy images and videos of children using Service-issued devices. Images and videos must be taken and used in accordance with Service policies, with careful consideration given to the purpose of the image or video. Educators will consider the intent, appropriateness, context and consent involved in capturing and using images and videos, so the process aligns with children's learning, wellbeing and right to privacy.

Parental consent for images and videos

The Service obtains written, purpose-based parental consent at enrolment for capturing, using, storing and sharing a child's images and videos. Consent identifies each intended purpose and allows families to opt in or out of each purpose separately. Where a family has not completed the consent agreement, the Service treats this as consent refused — the child's image will not be used until consent is given.

Where a family has permitted their child's image to be used, the child retains the final say on whether a particular image of them is used, even where a parent has already given permission; a child's decision not to have an image used will be respected, and children are told it is reasonable to say no.

A family may change or withdraw consent in writing at any time. Withdrawal ordinarily applies prospectively: optional displays and publications will be removed promptly where reasonably practicable, but withdrawal does not require destruction of a prescribed record, incident or safeguarding evidence, material subject to an investigation or legal hold, or another record the Service is required to retain. Backup copies are restricted and removed through the approved backup lifecycle. A group image forming part of another child's lawful record will be managed to prevent further optional use and unnecessary access.

Storage, retention and disposal

The Service uses an approved secure cloud storage platform for digital files, including images, videos and documents collected on Service-owned devices, configured — where available — with encryption in transit and at rest, role-based access, multifactor authentication, audit logging and secure backup arrangements.

- Images, videos and documents collected on a Service-owned device must be uploaded or synchronised to the approved secure platform as soon as practicable and, wherever technically possible, automatically. Where automatic synchronisation is unavailable, transfer must occur no later than the end of the staff member's shift when connectivity is available. Successful transfer must be verified before any local copy is removed.
- Access to the approved secure platform is restricted by role and operational need, using individual user accounts. Multifactor authentication is enabled where available. Access permissions are reviewed at planned intervals and removed or amended promptly when a person changes role, leaves employment or no longer requires access.
- Staff must not copy, share or store files on personal devices or unauthorised platforms.
- Service-owned devices use supported operating systems, current security updates, encryption where supported, automatic screen locking and secure authentication. Staff must not share credentials or use personal accounts on Service-owned devices.
- Loss, theft, unauthorised access, accidental disclosure or suspected compromise of a device or account must be reported immediately to the Nominated Supervisor or Approved Provider. A device used under an approved work-from-home arrangement must be stored securely and must not be accessed by household or family members.

- Regularly, Service-held images and videos will be reviewed and securely deleted where they are no longer required for an authorised Service purpose, unless they form part of a record required to be retained under legislation or regulation, e.g., programming, or are required in connection with an incident, complaint, child protection or safeguarding matter, investigation, insurance matter or legal hold.

Where an image or video forms part of any other prescribed record relating to a child, it is retained until the end of three years after the child's last date of attendance (Regulation 183(2)(d)). A record relating to an incident, illness, injury or trauma is retained until the child turns 25 (Regulation 183(2)(a)–(b)). A record relating to a child's death is retained until seven years after the death (Regulation 183(2)(c)).

Child-protection and safeguarding records are retained until the child turns 25 years of age, or longer where required by law, an investigation, insurer, legal advice or a legal hold. Images used only for optional displays, newsletters or social media are deleted when no longer required for that purpose, subject to withdrawn consent, backup and legal retention requirements. Digital records are otherwise retained in accordance with the *Privacy and Confidentiality* policy, the *Record Keeping and Retention* policy, applicable legislation, and any investigation, complaint, insurance or legal-hold requirement, and securely deleted or archived once no longer required for an authorised purpose. Routine deletion is suspended where a record may be relevant to an incident, complaint, investigation, litigation or regulatory process.

PHYSICAL ENVIRONMENT AND ACTIVE SUPERVISION

The Approved Provider, Nominated Supervisor, management and educators will:

- Ensure children are always supervised and never left unattended while an electronic device is connected to the internet;
- Provide a child safe environment, reminding children that if they encounter anything unexpected, uncomfortable, scary or upsetting online, they can seek support from staff;
- Reflect on the Service's physical environment, layout and design to support child safe practices when children are using technology, including through regular audits to identify supervision 'blind spots';
- Position digital technology and equipment so that educators remain in line of sight of other staff, and only permit children to use devices in open areas that educators can monitor;
- Be alert to high-risk online behaviours — including uploading private information or images, engaging with inappropriate content, making in-app purchases, or interacting with unsafe individuals;
- Ensure administrative accounts, settings and Service records are restricted to authorised staff, and that any child access occurs only through supervised, age-appropriate applications or restricted profiles that prevent access to administrative functions and confidential information; and
- Apply this policy and the associated procedure where digital devices are used during transportation and excursions.

Ratios and general supervision requirements are set out in the *Supervision of Children* and *Staffing* policies and apply in full to activities involving digital technology.

SOFTWARE, PROGRAMS, APPS AND SCREEN TIME

The Service uses approved software programs and applications on Service-issued devices to support the educational program and administration. Applications are assessed for child safety, privacy, security, age-appropriateness, data location and operational need before approval, and reviewed regularly. Access to systems containing confidential information is protected through individual user accounts, secure authentication and multifactor authentication where available. Login details and passwords must not be shared.

Programs requiring additional background checks are accessed only by staff who have completed the necessary screening in accordance with Family Assistance Law. The Service's educational program software is used by educators to share observations, photos, videos, daily reports and learning portfolios with families through a secure, closed platform. The Service may also use accounting and payroll software, HR systems and compliance tools to support financial, staffing and administrative functions.

- Programs and apps are age-appropriate; only G and PG classified television programs and movies are shown at the Service.
- Programs depicting violence or inappropriate content, including graphic news reports, are not shown. Television and DVD use is kept to a minimum and limited to content with positive messages about relationships, family and life.
- Recreational screen time is planned and managed regarding the Australian OSHC Physical Activity and Screen Time Guidelines, which recommend no more than 30 minutes during Before School Care, 60 minutes during After School Care and 2 hours during Vacation Care. Recreational screen time includes activities such as television, movies, videos, electronic games and other screen-based entertainment. Screen use for approved educational, homework or operational purposes is not considered recreational screen time. Recreational screen time is balanced with opportunities for physical activity, play and other experiences and is not used as a reward or to manage challenging behaviour.
- Technology is used to extend the program, not to replace play-based experience or professional pedagogy, and children are supported to critically evaluate online information and to 'ask before they tap' on a device.

SOCIAL MEDIA USE

Only the Service's official social media account may be used to represent the Service, or to communicate with children or families on the Service's behalf, online. Staff must not use a personal social media account to post about the Service, its children, families or colleagues, or to interact with children or families in a Service capacity. A personal social media account must not be accessed on a Service-owned device (see *Storage, retention and disposal*, above).

Where the Service operates a social media platform, families engaging with it will not post spam, advertising or commercial content without the Service's prior consent, and will not post content that is abusive, profane or defamatory toward a person, entity, belief or symbol. The Service's social media platforms are not a channel for grievances or complaints — these are raised through the *Complaints & Grievance Handling* policy. The Service may remove content that does not comply with this policy.

Non-compliance is addressed under **Breach of policy**, below.

ARTIFICIAL INTELLIGENCE (AI) — USE AND GUIDELINES

AI may be used only as an assistive tool and does not replace professional judgement, legal obligations or human accountability. The Approved Provider or Operational Management Team approves the AI systems, organisational accounts and permitted use cases available to staff. Staff must recognise that AI outputs may be inaccurate, incomplete, biased, fabricated or out of date.

- Staff must use only Service-approved AI systems and organisational accounts for Service work. A personal AI account must not be used for Service information or documentation, and no AI system or account may be used for Service work without the Approved Provider's or Operational Management Team's prior approval.
- Personal, sensitive, confidential, legally privileged or security-sensitive information must not be entered into or uploaded to an AI system — including names, dates of birth, addresses, contact details, photographs, audio, health or disability information, NDIS information, court orders, attendance information, incident or child-protection records, family information and staff employment information. Removing a name alone does not necessarily de-identify information; the risk of re-identification must be assessed as low before information is used.
- Only Service-created content authorised for the intended use may be entered into an approved AI system. Staff must protect copyright, intellectual property, confidential business information and third-party material.
- AI-assisted content must be critically reviewed and fact-checked, and — where it concerns law, regulation, health, safety or child protection — verified against an authoritative source before use. The staff member approving or using the content remains responsible for its accuracy, relevance and outcome.
- AI must not make or determine decisions about mandatory reporting, child protection, medical treatment, medication, behaviour support, risk assessment, disciplinary action, employment, or any other matter materially affecting a child, family or staff member.
- Where AI materially contributes to a formal policy, report, assessment, communication or decision-support document, its use is reviewed and recorded in accordance with the Service's AI procedure.
- Children may use generative AI only as part of an approved, age-appropriate and actively supervised activity, and must not enter personal information, images, recordings or confidential Service information into an AI system.
- Any actual or suspected privacy, security or confidentiality incident involving AI is reported immediately and managed under the Service's Data Breach Response Procedure. The Approved Provider will assess whether the incident meets the threshold for notification under the Notifiable Data Breaches scheme or another legal or regulatory reporting requirement.

CONFIDENTIALITY AND DATA BREACHES

The collection, storage, use and sharing of information, images and digital content relating to children, families, staff and the Service is governed by the *Privacy and Confidentiality* policy and applicable privacy legislation (see Considerations). Any actual or suspected data breach must be reported immediately to the Nominated Supervisor or Approved Provider, who will notify the Office of the Australian Information Commissioner where required, in accordance with the *Privacy and Confidentiality* policy and the Service's Notifiable Data Breaches procedure.

IDENTIFICATION AND REPORTING OF ONLINE ABUSE AND SAFETY CONCERNS

The Approved Provider, Nominated Supervisor and management will:

- Ensure staff, educators, students and volunteers are aware of their mandatory reporting obligations and promptly report any child-safety concern, including inappropriate use of digital technology, to the Approved Provider or Nominated Supervisor (see *Child Protection Policy*);
- Support educators to encourage a child who encounters anything unexpected, unsafe or upsetting online to seek support, and to listen sensitively and respond appropriately to any disclosure, in line with the *Child Protection Policy*, *Behaviour Guidance Policy* and reporting procedures;
- Ensure every concern is documented and responded to promptly, with support provided to the child and family as required;
- Report a suspected case of online abuse to the relevant authorities, including the eSafety Commissioner and Police, in accordance with legal requirements and child protection procedures; and
- Assess every online safety incident against the serious-incident definition and other notification requirements under the National Law and National Regulations. Where notification is required, the Approved Provider will notify the Regulatory Authority through NQA ITS within the applicable statutory timeframe — this is assessed against the statutory notification categories on the facts of the incident, not treated as an automatic 24-hour serious-incident notification in every case.

DIGITAL MONITORING FOR SUPERVISION AND SITE SECURITY — HILLSBOROUGH OOSH ONLY

Hillsborough OOSH is currently the only Lake Mac Newy OOSH service operating fixed digital cameras for supervision and site security. Two high-definition cameras are installed — one at the front entrance and one at the side of the building — connected to a dedicated on-site recorder. **This section applies to Hillsborough only.** No other service currently operates under this section; if any other service installs cameras in future, this section (or a schedule listing all five services) will need updating.

- Footage is recorded continuously and stored securely on-site on a dedicated recorder. The retention period is approximately 60 days, though this may vary with activity levels, recording settings and future changes to the system configuration; once storage capacity is reached, the oldest footage is automatically overwritten.
- The cameras enhance site security and support educators to respond promptly to visitors, families or unexpected activity, and assist complaint-handling or investigations where required. Camera monitoring supplements, and must never replace, active supervision, required staffing arrangements or educator-to-child ratios, and is never used for staff performance monitoring or behaviour management.
- The cameras will never be installed in a private area such as a bathroom, nappy-change area or staff room.

Access to live or recorded footage is limited to staff specifically authorised by the Nominated Supervisor or Approved Provider, for an approved purpose only. Viewing, exporting, copying, or disclosing footage is limited to what is reasonably necessary, and exported footage is stored securely; a record is kept of access to or export of footage relating to an incident, complaint, investigation, or external request.

Families are informed of the monitoring and recording system at enrolment and orientation. Cameras or camera casings are clearly visible, and signage stating that security cameras and video recording are in use is displayed at each Hillsborough entrance. Employees must receive written notice in accordance with the *Workplace Surveillance Act 2005*

(NSW) — generally at least 14 days before surveillance commences, or before a new employee starts where surveillance is already operating — stating the type of surveillance, how it is carried out, when it commenced or will commence, and whether it is continuous or intermittent and ongoing or time-limited.

- Footage that may be relevant to an incident, complaint, child-safety concern, employment matter, insurance claim, legal request or regulatory investigation must be preserved before it is automatically overwritten and retained securely until the matter is finalised and all applicable retention requirements are met.
- A request to access or obtain footage is referred to the Approved Provider and assessed under applicable privacy, employment, child-safety, law-enforcement and legal obligations. Footage must not be provided informally or used for a purpose inconsistent with this policy, unless required or authorised by law.

ROLES AND RESPONSIBILITIES

The Approved Provider, Nominated Supervisor and management will:

- Meet obligations under the National Law and National Regulations, and ensure educators, staff, students, visitors and volunteers know of and adhere to this policy and the associated procedure;
- Provide new employees, students and volunteers with a copy of this policy and procedure as part of induction, and ensure families are advised how and where it can be accessed;
- Promote and support a child safe environment consistent with the *Providing a Child Safe Environment* and *Child Protection* policies, and embed the National Principles for Child Safe Organisations, reflected through the NSW Child Safe Standards;
- Provide professional learning to educators and staff on the safe use of digital technologies and online environments, and identify related training needs for professional development;
- Develop and monitor the *Electronic Device Register* for all electronic devices purchased and used at the Service;
- Ensure a review of practice follows any incident involving digital technologies or online environments, including an assessment of areas for improvement; and
- Maintain anti-virus, internet-security and content-filtering systems on Service devices to block access to unsuitable sites, newsgroups and chat rooms.

Child-safe recruitment and screening (WWCC), ratios, supervision and training-completion obligations — including the *National Model Code and Guidelines for Taking Images and Videos of Children*, the ECA *Statement on Young Children and Digital Technology*, and Geccko child safety training — are owned by the *Staffing*, *Supervision of Children* and *The Participation of Volunteers and Students* policies and apply in full to work covered by this policy.

Educators will:

- Adhere to this policy and the associated procedure, and participate in training on digital safety, privacy protection and responsible technology use;
- Implement active supervision when children are accessing online environments;
- Not use, possess or control a personal device while working directly with children, except where a lawful exception or prior written authorisation applies — and never use a personal device to capture, store or transmit an image or video of a child, including where an exception or authorisation is in place;
- Keep passwords confidential and log out of computers and software after each use;

- Ask a child's permission before taking their photo on a Service device, and explain how the photo will be used and where it may be published;
- Ensure a child's identifying personal information — name, address, age, date of birth and similar — is not shared online; and
- Introduce online-safety concepts at age-appropriate levels and consult with children about the use of digital technology and online environments so their voices are heard.

Families will:

- Adhere to this policy and the associated procedure;
- Not use a personal electronic device — including a mobile phone, smart watch or camera-enabled wearable device — to photograph, record audio of, or video any children being educated and cared for at the Service, including their own; and
- Not copy, download, duplicate, upload, publish, distribute or otherwise share any photo, video or observation provided by the Service, regardless of whether the content features their own child, another child, or both.

Visitors and volunteers will:

- Adhere to this policy and the associated procedure while at the Service;
- Not use a personal electronic device to photograph, record audio of, or video children being educated and cared for at the Service;
- Report a child-safety concern, including inappropriate use of digital technology, to the Approved Provider or Nominated Supervisor; and
- Where supporting a child at the Service (e.g. an NDIS-funded support professional or Inclusion Support Professional), obtain written parental authorisation before capturing an image or video of a child, for observation or documentation purposes only (see the *ECIP Confidentiality Agreement*).

BREACH OF POLICY

A staff member or educator who fails to adhere to this policy may breach their employment obligations, the National Law or other applicable requirements and may be subject to disciplinary action. A visitor, volunteer or contractor who fails to comply may have their engagement or access to the Service restricted or ended. A family member's non-compliance is addressed through the Service's complaints, visitor management, and child safety procedures. Any restriction on a family member's access, or impact on enrolment, will be proportionate to the risk, consistent with applicable law and procedural fairness, and will prioritise the child's safety, wellbeing and continuity of care.

CONSIDERATIONS

Education and Care Services National Law & Regulations	National Quality Standard & Child Safe Standards	Links to other Service Policies	Other Documentation / Evidence
National Law ss165, 167, 175A–175J Regulations 84, 115, 165–166, 168(2)(ha), 170–172, 179A–179B, 181, 183	QA2: 2.2.1, 2.2.3 QA3: 3.1.1, 3.1.2 QA5: 5.1.1, 5.2.2 QA7: 7.1.1, 7.1.2 Child Safe Standards 1–10	– Child Protection Policy – Providing a Child Safe Environment – Behaviour Guidance Policy – Privacy and Confidentiality – Governance and Management – Management of Incidents, Injury, Illness & Trauma – Complaints & Grievance Handling – Excursion/Incursion/Extra-Curricular Activities – Staffing – The Participation of Volunteers and Students – Supervision of Children – Code of Conduct – Record Keeping and Retention	– National Principles for Child Safe Organisations (NSW Child Safe Standards) – Australian Privacy Principles – Privacy Act 1988 (Cth) – Workplace Surveillance Act 2005 (NSW) – Surveillance Devices Act 2007 (NSW) – eSafety Commissioner guidance – National Model Code and Guidelines for Taking Images and Videos of Children – Australia's Physical Activity and Sedentary Behaviour Guidelines – Electronic Device Register – Exemption Register

ENDORSEMENT BY THE SERVICE

Approval date: September 2026
Date for review: September 2027
Approved by: Irene R