



SAFE USE OF DIGITAL TECHNOLOGIES AND ONLINE ENVIRONMENTS

(required-regulation)

Policy Statement

New Lambton District OOSH (NLDOOSH) is dedicated to creating and sustaining a safe online environment through the active involvement of staff, families, and the wider community. As a child safe organisation, we are committed to embedding the National Principles for Child Safe Organisations into our practices and continuously identifying and managing risks to ensure children's safety in both physical and digital spaces.

With digital technologies now playing a significant role in many children's lives, it is essential that our educators not only understand these technologies but also support children in developing safe, respectful, and informed digital habits within a child safe environment.

The safety and wellbeing of children is our highest priority. Our Service is committed to providing and maintaining a secure and supportive environment for all staff, children, families, visitors, and contractors-both in physical and online settings.

We strive to foster a positive digital safety culture that aligns with our Service philosophy and complies with all relevant privacy and legislative requirements to protect the wellbeing of enrolled children, educators, and families

Procedures

Use of Digital Technologies at the Service

- a. Our Service integrates digital technology and electronic devices to enhance children's learning experiences, document development, communicate with families and the broader community, support curriculum planning and administrative functions, and strengthen safety measures such as sign-in/out systems.
- b. Educators ensure that children access only age-appropriate content using devices provided by the Service.

Digital Devices and the National Model Code

- a. We align our practices with the National Model Code and Guidelines for the responsible use of images and videos of children.
- b. The approved provider will clearly inform all staff, educators, visitors, volunteers, and family members that the use of personal electronic devices-including mobile phones, tablets, smartwatches, META smart glasses, cameras, and data storage devices (USBs, SD cards, hard drives, and cloud services)- to capture images or recordings

of children is strictly prohibited. These devices are not to be carried or used while working directly with children.

- c. Devices belonging to the Service must remain onsite unless taken offsite for approved purposes such as shutdown time, excursions or transport. These devices may contain sensitive data related to children, families, or staff.

Exemptions for Personal Devices

- a. In specific, approved circumstances, individuals may be permitted to carry a personal device, with authorisation from the nominated supervisor. However, these devices must not be used to photograph, record children or share information with the children. Approved exemptions may include:
 - Emergency situations (e.g. child missing, lockdown, injury)
 - Health requirements (e.g. glucose or heart rate monitoring)
 - Communication support for a disability
 - Urgent family communications (e.g. serious illness or death)
 - Receipt of emergency alerts (e.g. bushfire notifications)

Children's Use of Devices

- a. Children who bring mobile phones to the service must ensure they are handed in at the administration desk upon arrival to OOSH. They are then available for collection once they are signed out of the service.
- b. Children who wear smart watches are not to use the watch to communicate with people outside of OOSH or to take photographs. If they are seen doing this they will be asked to hand the smart watch in at the administration desk until they are signed out of the service.
- c. "Toy" devices such as toy cameras, Leap Pads, kindles etc that can take photos are to be handed in at the administration desk on arrival to OOSH (this includes devices brought in by younger siblings). They are then available for collection once they are signed out of the service.

Images and Videos

- a. Only authorised personnel may capture, use, store, or dispose of images and videos using Service-issued devices.
- b. Authorisation from parents to take, use and store images and videos of children being educated and cared for by the service is given when submitting the Application of Care Form.
- c. These media files are password-protected and stored securely. Educators must consider the purpose, appropriateness, and consent when capturing digital content.
- d. Transferring images or videos to personal devices is prohibited and may result in disciplinary action.
- e. Destruction of records will follow the "Maintenance of Records" procedure.

Supervision and the Physical Environment

- a. The approved provider and educators must:
 - Maintain supervision whenever children use internet-connected devices
 - Provide a safe and supportive digital environment
 - Regularly audit the physical space to identify risks and ensure safe tech use
 - Ensure digital equipment is visible and used only in monitored, open areas
 - Prevent access to high-risk online behaviors such as sharing personal information, accessing inappropriate content, or unsafe communication
 - Password-protect all devices with access restricted to staff
 - Follow policy procedures during excursions and transport

Software and Applications

- a. The Service uses secure, regularly updated software and apps on Service-owned devices for educational, administrative, and communication purposes. Access is protected with individual logins and passwords.

Artificial Intelligence (AI) Use

- a. Staff using AI must acknowledge its limitations and privacy concerns. AI can be a supportive tool for documentation but must not replace professional judgement.
- b. Personal data (e.g. children's names or DOB) must not be entered into AI systems.
- c. All AI-generated information must be verified and tailored to the specific context.

Privacy and Confidentiality

- a. Staff and visitors must handle all digital content involving children or families responsibly. Any suspected breach must be reported immediately to a nominated supervisor.

Identifying and Reporting Online Risks

- a. The Service implements safeguards to protect children online. Staff are trained in mandatory reporting and respond promptly to child safety concerns, including digital-related incidents.
- b. Reports are made to the relevant services and regulatory bodies as required, and concerns are documented and addressed with family support.

CCTV Monitoring

New Lambton District OOSH does not currently utilise any CCTV surveillance systems.

Considerations

Name	Reference
------	-----------

Education and Care Services National Regulations	5AA, S162,165,166A167 R73,76,84,115,122,123,149,155,156,168,170,171,172,175,176 181,183,184,
National Quality Standard	2.1.2, 2.2.2
Other NLDOOSH policies/ Documentation	• Bus Procedure • Child Protection Policy • Child Supervision Staff Procedure • Electronic Device Use and Social Media Agreement • Electronic Sign in Procedure • Excursion Policy • Excursions Procedure • Interactions with Children Policy • Providing a Child Safe Environment • Risk Assessment Policy • Staffing Policy and related procedures • Social Media Policy • Maintenance of Records Procedure • Terms and Conditions • Application of Care • Electronic Device Use and Social Media Agreement • Code of Conduct
Other	• <i>My Time, Our Place – Framework for School Age Care in Australia</i>, Council of Australian Governments 2011 • Education and Care Services National Law Act 2010 • Australian Children's Education & Care Quality Authority • Children and Young Person's (Care and Protection) Act 1998 • Department of Education Guidelines • Network of Community Activities • Australian Government eSafety Commission (2020)

Policy status

Policy developed	July 2025
Last reviewed	July 2025
Due for review	January 2027
Policy owned by	New Lambton District OOSH

