



POLICY STATEMENT

As a child safe organisation, Mawson Lakes School OSHC embeds the National Principles for Child Safe Organisations and continuously identifies and addresses risks to ensure children are safe in both physical and online environments. We recognise that in today's technology-driven world, cyber safety is an essential part of protecting the children and young people in our care. We understand that sharing images online can affect a child's privacy and contribute to a permanent digital footprint. To safeguard children, we obtain parent or guardian consent before capturing or sharing photographs, and we ensure that no personal or identifying information is included in any images. Our photographs are used only to celebrate children's positive experiences within the service and are stored securely in accordance with our privacy and confidentiality procedures. We also engage children in age-appropriate discussions about online safety and responsible technology use. Through clear policies on photography, technology, and digital communication, ongoing family consultation, and the promotion of safe and respectful online behaviours, Mawson Lakes School OSHC is committed to maintaining a safe, inclusive, and supportive environment for all children, both offline and online.

BACKGROUND

At Mawson Lakes School OSHC, our commitment to child safety extends beyond the physical environment to include the safe and responsible use of digital technologies and online environments. By implementing clear policies and procedures, working collaboratively with families, and educating children about age-appropriate online safety and responsible digital behaviour, we create a secure environment where children can confidently engage with technology while remaining protected. We ensure that the use of digital technologies, online platforms, and the sharing of images complies with the Education and Care Services National Law and Regulations, privacy legislation, and our Child Safe Environment policies, safeguarding the wellbeing, privacy, and rights of every child.

REGULATIONS

Regulation	Description	Implementation
Part 6A	Devices in education and care service	We have clear policies that regulate the use of electronic devices by educators and children, ensuring they are used only for approved educational or operational purposes. Educators model appropriate use, supervise children's access to devices, and ensure all equipment is securely stored and protected from misuse. We manage privacy by preventing unauthorised recording, sharing, or exposure to inappropriate content. In addition, we provide educators with devices to document programming and spontaneous experiences for children, supporting reflective practice, assessment, and planning. These practices are consistently applied with the paramount consideration being the safety, rights, and wellbeing of children.
73 (a-e)	Educational program	Our educational program aims to foster a strong sense of identity, connection to the world, wellbeing, confident learning, and effective communication in each child.
76	Information about educational program to be given to parents	We provide parents with information about their child's educational program, participation, and relevant information upon request.
S.2A	Paramount consideration - Safety, rights and best interests of children	This is achieved by embedding child-safe principles into policies aligned with the Australian Children's Education & Care Quality Authority and the National Quality Framework, ensuring staff are well-trained to recognise and respond to risks, and fostering a culture where children feel safe,

		respected, and heard. Active supervision, inclusive practices, and clear reporting processes help prevent harm, while valuing children's voices and partnering with families supports their overall wellbeing.
S.162A	Child protection training	Child Protection Training is implemented by ensuring all educators complete approved child protection training. This equips them to recognise signs of harm, respond appropriately to disclosures, and meet mandatory reporting obligations, supporting a child-safe environment.
S.162B	Child safety training	Foundation Child Safety training is required to be refreshed every 2 years by all educators and staff.
S.165	Offence to inadequately supervise children	We are committed to ensuring that every child is actively and adequately supervised at all times in accordance with Section 165. Educators maintain active supervision by positioning themselves to see and hear children, conducting regular headcounts, monitoring attendance during transitions, and communicating effectively with one another to ensure all areas are supervised. Educator-to-child ratios are always maintained, and risk assessments are used to identify and minimise potential hazards within the environment and during excursions. Our learning environments are organised to reduce blind spots and support effective supervision, while educators remain vigilant and responsive to children's individual needs and changing circumstances.
S.167	Offence relating to protection of children from harm and hazard	Mawson Lakes School OSHC recognises that it is an offence under education and care services legislation to fail to protect children from harm and hazards. The service is committed to providing a safe environment and taking all reasonable precautions to safeguard children from injury, illness, abuse, neglect, and foreseeable risks.
12	Meaning of serious incident	A "serious incident" includes child deaths, injuries, illnesses, emergencies, missing children, and unauthorised removal or locking incidents within an education and care service.
73	Educational program	Our educational program aims to foster a strong sense of identity, connection to the world, wellbeing, confident learning, and effective communication in each child.
76	Information about educational program to be given to parents	We provide parents with information about their child's educational program, participation, and relevant information upon request.
84	Awareness of child protection law	We ensure all staff, volunteers, and students are aware of child protection laws and their responsibilities.
115	Premises designed to facilitate supervision	The service has been designed and maintained in a way that always facilitates supervision of children while being cared for at the service.
122	Educators must be working directly with children to be included in ratios	Only educators who work directly with children are included in the daily ratios.
123	Educator to child ratios-Centre based services	The service over rosters where possible allowing the Director and Assistant Director to not be in the ratio to assist and support a high-quality service. We adhere to a 1:5 ratio for a water excursion, 1:8 excursion and 1:15 when facilitating care at the service.
149	Volunteers and students	All volunteers and students participate in an induction process and are appropriately always supervised by

		qualified educators. They are never left alone with children, counted in educator-to-child ratios where prohibited, or given sole responsibility for the supervision or care of children. Educators provide ongoing guidance, monitor their interactions with children, and ensure that all volunteers and students understand and adhere to the service's child safe practices, policies, and procedures. This approach ensures that children remain safe while volunteers and students gain valuable experience in a supportive and well-supervised environment.
155	Interactions with children	We create an inclusive environment that respects children's voices, independence, dignity, and individuality. Taking into considerations their age, cultural backgrounds, and abilities.
156	Relationships in groups	We foster positive interactions and respectful relationships between children and staff through thoughtfully designed group experiences
165	Record of visitors	The record of visitors must include the signature and the time of the visitor's arrival and departure.
168	Education and care service must have policies and procedures	The service has policies and procedures that reflect the needs of the service. These are reviewed every two years or when deemed necessary.
168(2)(ha)	The safe use of digital technologies and online environments at the service	We are committed to ensuring the safe and responsible use of digital technologies and online environments. Educators actively supervise children's use of technology and ensure that all digital devices, applications, and online resources are age-appropriate, educational, and support children's learning and wellbeing. Children are taught about cyber safety, respectful online behaviour, privacy, and the importance of protecting personal information through age-appropriate discussions and experiences. Parent or guardian consent is obtained before any photographs or videos of children are taken or shared, and all digital images and information are stored securely in accordance with the service's privacy and confidentiality policies. Staff, volunteers, and students are expected to model responsible technology use and comply with the service's digital technology, photography, and child safe policies, ensuring that online environments are safe, respectful, and supportive for all children.
170	Policies and procedures are to be followed	Policies and procedures are always followed by our educators.
171	Policies and procedures are to be kept available	Policies and procedures are kept available to all educators and families, via the sign-out bench that is in TR9 or are available on the Mawson Lakes School website.
172	Notification of changes to policies or procedures	The approved provider must ensure that parents of children enrolled at the service are notified at least 14 days before making any change that will affect the fees charged or the way in which the fees are collected.
175	Prescribed information to be notified to the Regulatory Authority	The service is committed to notifying any relevant information to the Regulatory Authority within the required time frame.
176	Time to notify certain information to Regulatory Authority	In the case of a death of a child as soon as practicable but within 24 hours that person becomes aware of the death. In

		the case of any other serious incident, within 24 hours that person becomes aware of the incident.
181	Confidentiality of records kept by approved provider	Maintaining the confidentiality and privacy of all records in accordance is paramount. Children, families', and educators' personal information is collected, stored, accessed, and disposed of securely to protect privacy and confidentiality. Records are only accessed by authorised persons who require the information to perform their role or where disclosure is permitted or required by law. All educators, staff, volunteers, and students are informed of their confidentiality obligations during induction and are expected to maintain the privacy of all information obtained through their role. Digital records are password protected, hard copy records are securely stored, and confidential information is not discussed with unauthorised individuals.
183	Storage of records and other documents	All records and other required documents are stored securely to protect the privacy, confidentiality, and integrity of the information they contain. Hard copy records are kept in locked filing cabinets or secure storage areas with access restricted to authorised personnel only. Electronic records are stored on password-protected systems with appropriate security measures, including secure backups where applicable. Records are retained for the periods required under the Education and Care Services National Regulations and relevant privacy legislation before being securely destroyed when no longer required. Our service adheres to all legislative and regulatory requirements relating to the storage and management of records, ensuring the confidentiality, security, and privacy of the personal information of children, families, educators, and staff.
184	Storage of records after service approval transferred	If the service approval is transferred to another approved provider, all required records and documents are securely transferred in accordance with Regulation 184 and the Education and Care Services National Law and Regulations. Records are managed to maintain their confidentiality, security, and integrity throughout the transfer process, ensuring that the privacy of children, families, educators, and staff is protected. The receiving approved provider is provided with all records required to continue the operation of the service and to meet legislative record retention obligations.
195	Application of Commonwealth Privacy Act 1988	To comply and protect children's data photos and information, we have clear policies and procedures for obtaining parental consent, secure storage, and limited sharing.

PURPOSE

Children's safety and wellbeing is paramount within our service. We have a responsibility to provide and maintain a safe and secure working and learning environment for educators, children and visitors including online environments. We aim to create and maintain a positive digital safety culture that aligns with our service Philosophy, privacy requirements, and relevant legislation to ensure the safety and wellbeing of enrolled children, educators, and families. We believe that children's safety, rights, and best interests are the paramount consideration in all service operations, decisions, and functions.

This policy provides the framework for:

- The safe use of digital technologies and electronic devices at OSHC
- The capture, use, storage and destruction of images and videos of children whilst being educated and cared for by OSHC
- Obtaining written authorisation from parents to take, use and store images and videos of children
- The use of digital devices by children whilst being educated and cared for at OSHC
- The responsible use of online environments, including artificial intelligence AI tools and software platforms

SCOPE

This policy applies to children, families, staff, educators, management, approved provider, nominated supervisor, students, volunteers and visitors of Mawson Lakes School OSHC.

IMPLEMENTATION

Our service uses digital technology and electronic devices as a tool for learning with children, documenting their learning and development, communicating with families and the wider community, supporting program planning and administration tasks and enhancing safety and security through systems such as sign in and out platforms. The use of digital technologies is guided by the paramount consideration of child safety and wellbeing. Our service ensures that all digital environment devices and online platforms are used in ways that protect children from harm, uphold privacy and confidentiality and prevent inappropriate conduct.

Upon signing the enrolment form parents give permission for their child/ren to be photographed and any information to be displayed at the service. They also consent for their child/ren to watch PG movies that are deemed appropriate by OSHC educators and have access to OSHC iPads and Nintendo switch. If parents do not agree to this, they must notify OSHC Nominated Supervisor's upon the submission of their enrolment form.

Digital technology, when used appropriately, can be a tool for learning, especially when educators play an active role. The internet is a resource for research, communication and extending programming ideas and interests. Technology use within our service aims to encourage children to solve problems and use logical reasoning, leading children to make decisions, choices and assisting them to use computer software competently and safely. Our educators are diligent in ensuring children are only able to access age-appropriate technology on any device provided by the service. To achieve this, children who attend OSHC can engage with a range of technologies, under educator supervision.

Displaying of photos provides children and families with a sense of belonging. Photographs allow children to see themselves at play, are a topic of conversation for children and parents, allow families to see their child at play, and convey the message to children that what they are doing is important. However, it is fundamental to respect the rights of all children and families to privacy and ensure child safety is embedded in our policies and procedures.

TECHNOLOGY AT MAWSON LAKES SCHOOL OSHC

Children have access to the following technology during their time at OSHC:

- Children's iPads
- Nintendo Switch
- Television & DVD'S

These devices are closely monitored and filtered by educators to ensure children and young people's safety. All movies, games and apps that are purchased or downloaded are age appropriate for the children.

In accordance with the Mawson Lakes School 'Primary Student Use of Mobile Phones and Personal Devices' policy, the use of mobile devices is strictly prohibited within the OSHC service. All personal devices and other items not permitted at OSHC must remain in children's school bags.

Smart watches are encouraged yet children need to understand the responsibilities around the use of the watch whilst in the OSHC environment. The child isn't to contact their parent via the watch; the Nominated Supervisor will make the call on behalf of the child. If the smart watch isn't used in the correct manner the Nominated Supervisor will involve the parents in a discussion, if deemed necessary the child may be refrained from wearing the watch.

PERSONAL DEVICE RESTRICTIONS

OSHC is committed to creating and maintaining a safe online environment through collaboration with children, young people, educators, staff and families. Service-supplied devices and software are regularly updated, configured, monitored, and maintained to protect confidential information, prevent unauthorised access or misuse, and support the safety and wellbeing of all members of the service community.

Between the hours of operation Before School Care 6:45am to 8:45am, After School Care 3pm to 6pm, Pupil Free Day and Vacation Care 7am to 6pm. All staff, educators and volunteers have knowledge of and adhere to legislative requirements and do not use, or have access to personal electronic devices, including mobile phones, digital cameras, tablets, smart watches and other new and emerging technology, where those technologies can take, store or share images or videos. It includes personal storage and file transfer media such as SD cards, USB drives, hard drives and cloud storage.

Before educators commence their shift, they place their personal electronic devices in the locked locker within the OSHC office between the hours of operation. We have educators that are SSO'S at the school and come straight from children's classrooms to pick children up on-site east. Those educators will have their personal electronic devices on them until they reach site west where they will then place their personal electronic devices in the locked locker in the OSHC office.

An educator is only allowed to have a personal electronic device in their possession if the site leader which is the Director of Mawson Lakes School OSHC authorises one of the below forms:

"Approval register for possession of a personal device" which includes:

- Essential planned purpose
- Essential once-off purpose
- Exemption request

Written authorisations must be retained for a period of 3 years

Educators may be in the possession of their personal device during a break, provided no enrolled children are present or have access to the designated area appointed by the Nominated Supervisor on the day.

Mawson Lakes School OSHC has three work mobile phones. One phone is equipped with a SIM card and can make and receive calls. The remaining two devices do not have SIM cards and are used solely for capturing images of children participating in the services program. The Essential Planned Purpose form will be actioned so that the Nominated Supervisors can carry their personal device when children and educators are transported on one or more buses for excursions, each bus must be provided with a fully charged and contactable mobile phone to ensure communication can be maintained in the event of an emergency. During excursions, the Nominated Supervisor may carry their personal mobile device in their bag. The device is to be used only in the event of an emergency and must not be used for personal purposes while supervising children. Once we return from the excursion all personal devices will return to the locked locker in the OSHC office.

Only Mawson Lakes School OSHC supplied or issued registered electronic devices are used by children and educators. Strict controls are in place to ensure the appropriate storage, retention and destruction of images and videos of children. Refer to the service device record located in the OSHC office to outline what device the service occupies. The electronic device register includes type of device, serial number, who the device is allocated to, dates of allocation and return. Electronic devices supplied or issued by and registered with the service is stored in a locked cabinet at the end of the day.

Images and videos are stored on the program iPad for children and families to view. Our program displays that are around the service come down after a year and go into display folders for children and families to view. Individual photos come off the walls and doors and go into the basket in TR 11 for children to view. Any images or displays that have been taken or no longer required are deleted off our work iPad and phones or taken to the blue confidentially bin which is situated in the IT office on site east for destruction.

Parents interacting primarily with their child may retain their personal electronic devices, during arrival and departure. Parents must not use personal electronic devices for taking images, except of their own children. Parents are encouraged to refrain from using personal electronic devices whilst on site at Mawson Lakes School OSHC.

Visitors to the service, as a condition of entry, must agree in writing that they will not take any photographs or videos of children during their visit. All visitors will be directly supervised and will not be left alone with children.

PHYSICAL ENVIRONMENT AND SUPERVISION

- We will adhere to Australia's Physical Activity and Sedentary Behaviour Guidelines, limiting screen time for entertainment purposes to a maximum of 2 hours per day for children aged 5-12 years
- Reflect on the service'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 or equipment allows educators to remain in line-of-sight of other educators 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 devices are password protected with access for educators only
- Where service-supplied devices are used during transportation and excursions, they must be used in accordance with practices outlined within this policy and associated procedure
- All content used within the OSHC program will be socially and culturally considerate, ensuring inclusivity and respect for diverse backgrounds
- Ensure a risk assessment is conducted to assess the risks of children and young people bringing personal devices to OSHC. Risks such as access to inappropriate content, online interactions, photography or recording of other children, cyberbullying and distraction impacting supervision must be considered

SOFTWARE PROGRAMS AND APPLICATIONS

- Our service uses a range of secure software programs and apps on service-supplied or issued devices to support the educational program and administration of the service.
- All applications used by staff, educators, visitors and children must be carefully selected, regularly checked and kept up to date
- Access to software programs and applications must be password protected
- Each user must create their own user account and not share information
- Programs requiring additional background checks such as CCS Software must only be accessed by authorised staff who have completed necessary screening processes in accordance with Family Assistance Law

ARTIFICIAL INTELLIGENCE (AI) USE

Educators or staff using AI must be aware of limitations, privacy risks, and the potential for errors in the information it provides.

- AI may be used to support documentation tool; however, educators and staff must verify accuracy and not rely upon AI as an authoritative source
- Educators and staff must enter original work and verify that information obtained from AI is contextually relevant
- Educators and staff must not enter personal or identifying details of individual children such as names and dates of birth into AI tools
- Data and privacy concerns must be addressed in accordance with this policy and the Privacy and Confidentiality Policy

BREACH OF POLICY

Educators who fail to adhere to this policy may be in breach of their terms of Employment and may face disciplinary action which may lead to notification to the regulatory authority and child protection authorities. 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 OSHC service.

RESPONSES TO NON-COMPLIANCE

Where children use a personal device at school without an approved exemption, or use it inappropriately, a response will be provided in line with the Behaviour Guidance policy. An initial reminder will be provided to children about the importance of storing personal devices according to this policy, along with contact to the children's family.

Further breaches will be responded to according to the Behaviour Guidance policy, with possible consequences including:

- Rethink - office reflection and discussion with the Nominated Supervisor
- Documentation of repeated behaviours
- Confiscation of the device, stored securely until collection by the child's family
- Inappropriate Behaviour Form

Where a children's misuse of personal devices is serious, it may be necessary for the Nominated Supervisor to meet with the school's Principal, Wellbeing Leader, and or child's teacher to consider responses in line with the department's suspension, exclusion, and expulsion of students' procedure, or to contact South Australia Police if the behaviour is suspected to be illegal.

CYBER BULLYING

Mawson Lakes School OSHC has a duty of care to children under various legislative frameworks to ensure the environment is safe, inclusive, respectful, and free from risk of harm. We do not tolerate any forms of bullying behaviour. We will respond appropriately to cyberbullying by reporting this behaviour immediately to school leadership and seek further advice from the police if deemed necessary. Mawson Lakes School OSHC implements strategies suggested through the Mawson Lakes School 'Anti-Bullying and Harassment' policy in regard to Cyber-Safety.

KEY TERMS

Key Term	Meaning
Artificial intelligence (AI)	An engineered system that generates predictive outputs, such as content, forecasts, recommendations, or decisions, based on a given set of human-defined objectives or parameters, without being explicitly programmed for each specific task.
App	An abbreviation of the term 'Application'- refers to small programs that can be downloaded or installed on mobile phones.
Capturing	An image includes filming, recording or taking a photo/image of a child.
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, equipment and devices, including mobile phones and devices.
Digital devices	All electronic equipment capable of capturing, storing, transmitting or receiving data, images or video- including iPad, mobile phones, cameras, smart watches, wearable devices and any other internet-connected data-enabled devices.
Disclosure	Process by which a child conveys or attempts to convey that they are being or have been sexually abuses, 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.
Harmful content	Harmful content includes sexually explicit material; false or misleading information; violence; extremism or terrorism; hateful or offensive material.
ICT	Information and Communication Technologies.
Illegal content	Content that includes images and videos of child sexual abuse, content that includes terrorist acts, content that promotes, incites or instructs in crime or violence or footage of real violence, cruelty and criminal activity.
Images and videos of children	Any photographic, video or audio recording of children being education and cared for by the service, whether captured on service-supplied or personal devices.
National Model Code	The National Model Code for Early Childhood Education and Care, released by ACECQA which provides guidelines about the use of personal electronic devices in education and care services, including taking images or videos of children.
Online hate	Any hateful posts about a person or group based on their race, religion, ethnicity, sexual orientation, disability or gender.

TECHNOLOGY RISK ASSESSMENT

The approved provider, in conjunction with OSHC educators, conduct comprehensive risk assessments to identify any potential risks or hazards and ensure the safety of all children accessing technology devices at OSHC.

The risk assessments are reviewed every two years or after being aware of an incident or circumstance where the health, safety or wellbeing of children may be compromised during technology use at our service.

All risk assessments are regularly assessed and evaluated to facilitate continuous improvement. If a risk concerning a child's safety during technology use is identified during the risk assessment, the approved provider must update the Photograph, Technology & Cyber Safety Policy and Procedure as soon as possible. The risk assessment is understood and adhered to by all educators.

ROLES AND RESPONSIBILITIES

Roles	Responsibilities
Nominated Supervisor & Approved Provider	• Determine who is authorised to capture, use, store and destroy images and videos of children using service-supplied devices • Inform parents or guardians during enrolment and orientation how the service will capture, use, store and destroy images and videos • Request written authorisation from families to capture, use, store and destroy digital documentation including images and videos of children at time of enrolment • Ensure images or videos of children are not taken, used or stored without prior parent or guardian authorisation • Develop, maintain and share a confidential record of all children who are NOT to be photographed or videoed • Obtain written authorisation from parents or guardians for children to use electronic devices • Ensure staff, educators, visitors and volunteers do not transfer images or videos from service-supplied devices to personal devices. Unauthorised transferring of digital data may result in disciplinary action • Ensure that obligations under the Education and Care Services National Law including Part 6A Education and Care Services National Regulations and regulator directions where relevant are met • Ensure the Privacy and Confidentiality Policy is always adhered to • Ensure images and videos will be stored securely with password protection, with access limited to authorised persons only • Ensure every child is protected from exploitation of photographic and video images • Ensure images or videos do not show children in distress, in positions that may be perceived as sexualised or in a state of undress • 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 • Notify the Office of the Australian Information Commissioner 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 portfolios, child developmental report ○ Any possible breach within the service or if the device is left behind whilst on an excursion • Ensure educators, staff, students, visitors and volunteers have knowledge of and adhere to this policy and associated procedure • Take every reasonable precaution to prevent breaches of this policy and related legislation • Ensure families are aware of this policy and advised how and where it can be accessed • Ensure processes are in place to ensure families who speak languages other than English understand the requirements of this policy, including providing authorisation for images and videos • Ensure mandatory national child safety training is completed by the approved provider, management, staff, educators, students and volunteers • Ensure child safe practices are embedded into organisational practice as per National Principles for Child Safe Organisations • Remain informed of updates to privacy legislation and guidance from the Office of the Australian Information Commissioner

	• Ensure children, educators and families are aware of the service's complaints handling process to raise any concerns they may have about the use of digital technologies or any other matter • Ensure staff, educators, families and children are informed of updates to policies, procedures or legislation relating to digital technologies • Ensure 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 • Provide professional learning to educators and staff regarding the safe use of digital technologies and online environments • 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 or inappropriate conduct to the approved provider or Nominated Supervisor • Promote and support a child safe environment, ensuring adherence to the Child Safe Environment and Child Protection Policies, including mandatory reporting obligations • Maintain appropriate educator to child ratios and active supervision at all times, including when using technology • Ensure all students, visitors and volunteers are supervised at all times and never left alone with a child • Ensure a review of practices is conducted following an incident involving digital technologies and online environments, including an assessment of areas for improvement • Ensure reasonable precautions are taken to prevent personal device use in breach National Law and regulator directions • 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 • Respond to and report any breaches and incidents of inappropriate use of digital devices and online services to leadership • Ensure all concerns are documented and responded to promptly and appropriately, with support provided to the child and their family as required • Ensure all educators, staff, students and families are advised of the protected disclosure within the Privacy and Confidentiality Policy, whistleblower protections and processes • Report any suspected cases of online abuse to the relevant authorities, including the e-Safety Commissioner and Police, in accordance with legal requirements and child protection procedures • Notify the regulatory authority within 24 hours, via NQA ITS, if a child is involved in a serious incident, • Including any unsafe online interactions, exposure to inappropriate content or suspected online abuse • Oversee implementation of the technology policy and ensure educators, families and visitors are aware • Promote a child-safe environment and embed relevant child safe principles into the service's structure • Identify educators training needs on technology safety, responsible use, and relevant regulations including eSafety Commissioner resources, ECA Statement on young children • Develop guidelines for technology use within the service, considering educational value and responsible practices • Ensure secure access to technology with password protection and staff-only logins • Conduct regular security audits to identify and address any vulnerabilities
--	--

	• Review the physical environment to minimise supervision blind spots while children use technology • Ensure secure storage and handling of confidential information both online and offline backups • Establish procedures for handling complaints and reporting data breaches to relevant authorities
Educators	• Adhere to the Photograph, Technology & Cyber Safety Policy • Be aware of current child protection law, National Principles for Child Safe Organisations Child Safe Standards applicable and their duty of care to ensure that reasonable steps are taken to prevent harm to children • 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 OSHC service's operations, including when accessing digital technologies and online learning environments • Not use, or have access to, any personal electronic devices while working directly with children, unless an exemption has been authorised • Not access personal social media on any device while working directly with children • Keep passwords confidential and log out of devices • 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 images and videos must not show children in distress, in a position that may be perceived as sexualised or in a state of undress, including where genitalia may be exposed • Ensure children's personal identifiable information is not shared online • Ensure screen time is NOT used as a reward or to manage challenging behaviour • Ensure any digital media, television programs or online content accessed at the OSHC service will be age-appropriate, culturally respectful and consistent with the service's educational program • Introduce concepts about online safety to children at age-appropriate levels • Consult with children about matters that impact them, including the use of online environments • Report any concerns related to child safety, including inappropriate use of digital technology to the approved provider or nominated supervisor • Identify potential risks to children online inappropriate content, cyberbullying and in the physical environment lack of supervision. Report any concerns to Nominated Supervisors • Supervise children closely whenever they are using technology, being physically present and attentive • Ensure children are using technology in open areas where you can easily monitor their activity • Encourage collaboration and turn-taking when children are using technology together • Educate children on recognising safe physical and online environments • Discuss online behaviour as part of activities promoting respectful relationships • Teach children how to critically evaluate information they find online • Select and introduce only educational programs and apps that you have reviewed beforehand • Ensure children are never left unattended while using technology connected to the internet • Use appropriate privacy settings and parental controls on devices used by children

	Report any breaches, incidents of inappropriate technology use, or suspicious activity to the nominated supervisor immediately
Families	Parents interacting primarily with their child may retain their personal electronic devices, during arrival and departure. Parents must not use personal electronic devices for taking images, except of their own children. Parents are encouraged to refrain from using personal electronic devices whilst on site at Mawson Lakes School OSHC. - Adhere to this policy and associated procedure - Provide written authorisation indicating whether the service may take, use, store or destroy images or videos of their child - Provide written notification if they wish to withdraw the authorisation at any time - Be aware that other children may feature in the same photos, videos and observations as their child, and not duplicate or upload these to the internet or social networking sites - By signing the enrolment form, families or guardians are providing consent for their child/ren to watch PG movies - They also provide consent for their child/ren to access a variety of age-appropriate technology like iPads, and Nintendo Switch consoles - They also provide consent for their child/ren to have photos and videos taken for approved OSHC use only - Have access information about online safety resources eSafety and how to choose age-appropriate apps and games for their children - Understand the service's complaint handling process and how to raise concerns
Visitors, Volunteers and Students	- Adhere to this policy and associated procedure whilst visiting the OSHC service - Not use personal electronic devices to take photos, record audio or capture video of children being educated and cared for at the OSHC - Report any concerns related to child safety, including inappropriate use of digital technology to the approved provider or Nominated Supervisor

CONTINUOUS IMPROVEMENT/REFLECTION

Our Photograph, Technology & Cyber Safety Policy will be reviewed on an annual basis in consultation with children, families, educators, and leadership.

SOURCE

Australian Children's Education & Care Quality Authority. (2014).

Australian Government Department of Education. My Time, Our Place- Framework for School Age Care in Australia.V2.0, 2022

Australian Government Department of Education, Skills and Employment. (n.d.). Bullying No Way.
<http://www.bullyingnoway.gov.au>

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

Australian Children's Education & Care Quality Authority. (2026). Guide to the National Quality Framework

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.(2026). Using digital devices in centre-based education and care services 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. (2026). 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

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://childdsafe.humanrights.gov.au/Children> (Education and Care Services) National Law (NSW)

Early Childhood Australia (2016). Code of Ethics.

Education and Care Services National Law Act 2010

Education and Care Services National Regulations 2011

Education and Care Services National Regulations (NSW) (2025) (For NSW services only)

NSW Government. (2026). Ministerial Direction. Education and Care Services (Supply, Authorisation and Use of Devices) Order 2026

Office of the Australian Information Commissioner (OAIC)

Privacy Act 1988.

CONTINUOUS IMPROVEMENT & REFLECTION

Our Safe Use of Digital Technologies and Online Environments Policy will be reviewed every two years or earlier if there are changes to legislation or ACECQA guidance or any incident related to our policy.

Feedback will be requested from children, families, staff, educators and management and notification of any change to policies will be made to families within 14 days.

REVIEW

POLICY CREATED BY	Lorin & Sue - All educators	Nominated Supervisor	August 2025
MODIFICATIONS Policy reviewed out of scope following the release of the Education and Care Services Supply, Authorisation and Use of Devices			
POLICY REVIEWED BY	Lorin & Sue - All educators	Nominated Supervisor	April 2026
MODIFICATIONS Policy reviewed due to legislative changes relating to child safety - Child Safety Reforms			
POLICY REVIEWED BY			
MODIFICATIONS			