



bookings@tpsoosh.com.au
(02) 9144 4769

Safe Use of Digital Technologies and Online Environments

Policy Statement

In today's digitally connected world, the safe and responsible use of digital technologies in primary age education and care is paramount. This policy outlines the commitment of South Turramurra Out of School Hours Care (OOSH/Service) to ensure the safety and well-being of children.

Key considerations for educators, students, parents and volunteers utilising digital devices in the service context include:

- Supporting the implementation of child-safe practices when using electronic devices to capture images or videos of children enrolled in early education and care services.
- Increasing awareness of educators, students, volunteers, and families regarding safety risks associated with using electronic devices in the service and implementing strategies to support child safety.
- Aligning with the Education and Care Services (Supply, Authorisation and Use of Devices) Order 2025 (NSW) and supporting the National Quality Framework, National Child Safe Principles, and the National Model Code for Taking Images or Videos of Children. Ensuring every reasonable precaution is taken to protect children from harm and hazard, including when using digital technologies and online environments.
- The timely and effective identification of, and response to, children who may be at risk of or are experiencing abuse or maltreatment through digital technologies and online environments. This includes appropriate notification to the relevant regulatory authorities, where required.

Legislative Requirements

This policy aligns with the following legislation and frameworks:

- Children and Young Persons (Care and Protection) Act 1998
- Children's Guardian Act 2019
- Education and Care Services National Law Act 2010
- Education and Care Services National Regulations 2011
- Education and Care Services (Supply, Authorisation and Use of Devices) Order 2025 (NSW)
- National Quality Standard (QA2, QA4, QA5, QA7)
- National Principles for Child Safe Organisations
- Privacy Act 1988 and Australian Privacy Principles
- Online Safety Act 2021

Creating Goals/What are we going to do?

Children have the fundamental right to be safe and protected from digital exploitation. All educators have a responsibility to ensure that children's interactions with digital technologies are secure, and their personal information and any images or videos used in the service are safeguarded.

OOSH is committed to exercising its duty of care to do everything that is reasonably practicable to avoid potential digital threats and maintain children's right to digital safety and privacy. Our educators will exercise their duty of care by:

- Creating a safe, supportive and informed environment where digital technologies can enhance learning whilst prioritising the safety and security of every child in care.
- Establishing a nurturing and secure environment, prioritising every child's well-being, safety and development.
- Committing to fostering a culture of vigilance and care in which all children feel protected, supported and valued.
- Providing children with the opportunity to maintain their rights and dignity, express their autonomy and have the right to say no if they do not want their photo or video taken.
- Actively supervising children when they use digital devices, particularly when accessing an online environment, to create a safe, supportive culture, monitor the physical environment in which these digital technologies and online environments are used, and prevent incidents.
- Using devices with purpose to enhance learning and support development, self-regulation and leisure.
- Recognising that digital technology is a valuable tool when used intentionally with children to extend and support active, practical, creative and authentic engagement with their surroundings, the community and the world.
- Supporting children to use digital technology when applicable, with intentionality to inform and educate children on how to safely use digital devices and support children's positive relationships with different forms of technology.

Implementation Strategies – how will it be done?

OOSH adopts the National Model Code and the accompanying Guidelines developed by ACECQA (Australian Children's Education and Care Quality Authority). These resources will be used in the service to implement child-safe practices and enhance awareness of the associated risks and considerations when educators, students and volunteers use personal and service devices.

To create a digitally safe environment for the children in care, the service will:

- Provide and enforce the use of service-supplied devices for all digital activities involving children.
- Regularly update and maintain these devices with the latest security software and firmware.
- Not permit personal devices for childcare-related tasks to minimise the risk of data breaches unless written approval is provided by the Approved Provider, as defined by the National Model Code.
- Not permit personal devices in areas where children are educated and cared for, unless it is used for essential purposes, as defined by the National Model Code.
- Develop and enforce strict privacy policies that govern the collection, storage and sharing of children's digital information.
- Ensure that all digital content, such as photos and videos, is stored securely and access is limited to authorised personnel only.
- Obtain consent from parents and guardians before capturing or sharing any digital media involving their children.

- Obtain consent from children, whenever possible, before capturing or sharing any digital media involving themselves.
- Avoid sharing children's images and digital media on open online platforms, without parental consent.
- Conduct regular training sessions for staff on digital safety best practices, including recognising and mitigating online risks.
- Provide specific training on the service's privacy policies and the proper use of service-supplied devices.
- Keep staff updated on the latest trends and threats in digital safety to ensure they remain vigilant and informed.
- Implement continuous audits of digital device usage to ensure compliance with established policies and procedures.
- Conduct regular digital content and storage audits to identify and address potential security vulnerabilities.
- Request that families, associated onsite workers and members of the public do not use personal devices to record images or videos of children in our care.

Where children are supported to use digital technology, the service will:

- Ensure age-appropriate, active, and engaging use of technology, accompanied by an educator.
- Support the interests of the children and their provocations, identified through play.
- Encourage exploratory play and enhance children's learning using technology.
- Allow children to engage in multimodal use of technology such as images, text, video, and audio.
- Offer insight into the role, use and presence of technology in today's world.
- Educate children on how to use digital platforms safely. For example, tell children to always communicate with team members and educators if they feel unsafe using digital devices.
- Support a positive relationship with digital technologies and devices, avoiding glorifying or condemning its use in the program.

The Approved Provider will:

- Apply the National Model Code and Guidelines for taking images or videos of children while enrolled and providing education and care in OOSH.
- Ensure only service-supplied devices are used to capture and transmit images. Ensuring the taking and transmitting of photos with personal devices is prohibited.
- When considering authorisation of a personal device, the Approved Provider or authorised delegate will apply a reasonable person test, asking whether an ordinary, sensible adult, prioritising child safety and active supervision, would consider the device genuinely necessary in the circumstances.
- Develop a 'Safe and Responsible Use of Service Technology' statement. Ensure all educators, students and volunteers sign and adhere to this statement.
- Establish and maintain processes including a service-supplied and approved use of personal devices log, for the ongoing monitoring and review of any authorised use of service and personal electronic devices.
- Ensure that all related policies including, but not limited to privacy and confidentiality, child-safe environments, child protection, relationships with families and record keeping, are in line with this policy.
- Continuously review and update digital safety policies and procedures to keep up with technological advancements and emerging risks.
- Establish procedures for the ongoing monitoring and review of the use of personal and service-supplied electronic devices to ensure it aligns with authorised guidelines and remains appropriate.
- Ensure the appropriate risk assessments and action plans are completed, and all identified actions are taken to minimise the risks to children's health and safety.
- Prohibit the use of personal digital devices in spaces where children are being educated and cared for. Digital devices include personal smartphones, personal tablets, personal computers, and any type of wearable

technology with access to image or video recording, such as some smartwatches and AI glasses, unless for essential purposes.

- Provide educators, students, and volunteers, with regular training and professional development on digital safety practices, including recognising and mitigating risks associated with digital technologies.
- Communicate with families about digital safety practices, involving them in discussions about how digital devices are used within the service and any associated risks.
- Establish secure access controls used to manage who can use digital devices and access digital content, ensuring that only authorised individuals can access sensitive information and technology.
- Establish protocols for safe online interactions, including supervision of children's online activities and the use of appropriate filters and monitoring software.
- Update software and security measures on all digital devices regularly to protect against viruses, malware, and other cybersecurity threats.
- Encourage responsible and respectful use of technology to promote a culture of digital responsibility among educators, students, and volunteers.
- Maintain clear documentation of any digital safety incidents and establish a protocol for reporting and addressing these incidents promptly, as part of the governance duty of care.
- Establish processes for safe digital record keeping, in line with the recommendations of the Royal Commission into Institutional Responses to Child Sexual Abuse; Section 175 of the National Law: Offence relating to requirement to keep enrolment and other documents; and Regulation 177 of the National Regulations: Prescribed enrolment and other documents to be kept by Approved Provider.
- Service-supplied device logs and approved use of personal device logs are to be retained for a minimum of 3 years, with Approvals for use of personal devices being reviewed every 3 months for the duration of the approval period.
- Through signage or other means, inform families, school staff, cleaners, tutors, and members of the public that the taking of photos or videos of children using their personal devices is prohibited whilst at the service.

The Nominated Supervisor will:

- Support the Approved Provider in applying the National Model Code and Guidelines for taking images or videos of children while enrolled and providing education and care in our service.
- Support the *Safe and Responsible Use of Service Technology statement* by ensuring that all educators, students, and volunteers sign and adhere to this statement.
- Support the Approved Provider to develop and maintain service policies and procedures.
- Monitor the prohibition of the use of personal digital devices in spaces where children are being educated and cared for. Digital devices include personal smartphones, personal tablets, personal computers, and any type of wearable technology with access to image or video recording, such as smartwatches and AI glasses, unless for essential purposes.
- Ensure that all digital safety policies and procedures are effectively implemented and adhered to within the service.
- Coordinate and provide ongoing training and education for educators, students, and volunteers on digital safety practices, including responsible use of electronic devices and recognising potential risks.
- Develop effective onboarding programs to ensure educators, students and volunteers are informed about the safety and responsibility of using digital devices safely in the service.
- Keep families informed about digital safety measures, policies and any updates or changes.
- Facilitate regular reviews and audits of digital device usage, ensuring that authorisations are current and devices are used appropriately and safely.
- As part of the service's child-safe practices, encourage a culture of digital responsibility and safety among educators, students, volunteers, children, and families, fostering an environment where all stakeholders understand the importance of digital safety.

- Stay current with the latest developments in digital safety and cybersecurity and ensure this knowledge is shared with educators, students and volunteers and incorporated into practice.
- Ensure that appropriate access controls, such as passwords and user permissions, are in place to protect sensitive information and limit access to authorised personnel only.
- Supervise staff to monitor for any data transfer between service-supplied devices and any other devices.
- Promptly address digital safety incidents, documenting them accurately and taking necessary actions to mitigate risks and prevent future occurrences.
- Provide feedback to educators, students and volunteers who are found using personal devices during work hours and implement appropriate action for non-compliance of policies and procedures.
- Work closely with the Approved Provider to regularly review and update digital safety policies and procedures, ensuring they remain practical and relevant.
- Implement and monitor the processes for safe digital record keeping, in line with the recommendations of the Royal Commission into Institutional Responses to Child Sexual Abuse, Section 175 of the National Law: Offence relating to requirement to keep enrolment and other documents and Regulation 177 of the National Regulations: Prescribed enrolment and other documents to be kept by Approved Provider.
- Maintain device-use procedures to minimise the need for staff to have personal devices onsite.

Educators and staff will:

- Adopt the implementation of the National Model Code and Guidelines for taking images or videos of children while enrolled and providing education and care in the service.
- Adhere to a child-safe code of conduct that emphasises the importance of child safety in the service, including using digital technologies safely.
- Read and acknowledge the 'Safe and Responsible Use of Service Technology' statement.
- Ensure digital safety when taking photos and video materials and documenting children's development while avoiding accessing service information using personal devices during and outside work hours.
- Implement locking systems and passcodes on their personal devices with service applications installed.
- Use service-provided cameras or devices to take photos and document children's development, not personal devices.
- Keep their personal digital devices away from areas where children are educated and cared for unless they are used for essential purposes. Digital devices include personal smartphones, personal tablets, personal computers, and any type of wearable technology with access to image or video recordings, such as some smartwatches and AI glasses, unless for essential purposes.
- Ensure that written consent is obtained from parents or guardians and children, when applicable, before taking any photos or videos of children using service-supplied devices.
- Adhere to the service's privacy policies when documenting children's development, ensuring that images and videos are stored securely and shared only with authorised individuals.
- When taking photos, ensure that only the intended child is in the frame or blur other children's faces to protect their privacy.
- Store all photos, videos, and documentation on secure, password-protected devices or cloud services provided by the service. Regularly back up data and ensure it is accessible only to authorised personnel.
- Be required to log out of the service's online platform and applications once their shift is complete.
- Be prohibited from using personal applications (Apps) and programs in their personal devices to obtain, store or access service information.
- Utilise only secure, service-approved platforms and applications for accessing and sharing information.
- Comply with regular reminders from your Nominated Supervisor about the importance of not using personal devices for work-related tasks and the potential risks involved.
- Follow clear rules and guidelines that personal devices should not be present in areas where children are being cared for.

- Have designated areas where educators, students and volunteers can use their devices during breaks. Educators may use personal devices in the staff room or office space, so long as no children are present.
- Not capturing images on personal devices, even in the office or staff room during child-contact hours.
- Be provided with secure storage for personal devices during work hours to minimise distractions and prevent unauthorised use.
- Lead by example by not using personal devices in the presence of children and encourage a culture of full engagement and attention while interacting with children.
- Provide feedback to staff who are found using personal devices during child contact hours. Repeat offenders will face disciplinary action due to non-compliance according to the Code of Conduct.
- Inform the Nominated Supervisor of non-compliance with this policy.
- Not be permitted to document or record conversations and information that is private and confidential using personal devices.
- Not be permitted to obtain, access and store images and videos relating to educators, students, volunteers, children, and families from personal devices.
- Educate children in acceptable and unacceptable behaviours (of adults and children) when children use digital devices and engage in digital platforms.
- Support children when using digital devices, to enhance their skills and development while cultivating a positive relationship with digital devices and platforms.
- Implement the NSW Government's screen time recommendations for children aged 5 – 12 years to have no more than two hours of sedentary recreational screen time each day (this does not include required schoolwork).
- Support families and the general public in adhering to this policy by not allowing authorised collectors, school staff, cleaners, tutors, or members of the public to use personal devices to take images or videos of children whilst at the service.

Procedures

Technology

Use of Technology

- Children will use technology as part of the program, to aid in emotional regulation and support transitions or due to extreme weather.
- Educators will use technology provided by OOSH for documentation, media streaming, activity research, record keeping, attendance records and emergency and evacuation procedures.
- Parents/guardians will use technology to record their child's attendance, sign medical administration and incident reports, provide permissions and for communication whilst at OOSH.
- Photography on personal devices is strictly prohibited. This applies to all educators, children, parents, and visitors/volunteers. Photographs will only be taken and stored on the service-supplied devices with prior approval from parents on enrolment.
- OOSH recognises and enforces the *Turramurra Public School Policy for the Use of Mobile Phones (and similar devices) in School by Students*.
- Medical devices are permitted for use by students where a medical management plan has been provided.

National Model Code

We follow the National Model Code for taking images of children while providing childcare. The code on this topic states the following:

Part 1

Only service-supplied electronic devices should be used when taking images or videos of children while providing education and care. The appropriate use of service-supplied electronic devices for taking, sending, and storing images or videos of children should be clearly outlined in policies and procedures.

Part 2

Personal electronic devices that can take images or videos (such as tablets, phones, digital cameras and some smart watches) and personal storage and file transfer media (such as SD cards, USB drives, hard drives and cloud storage) should not be in the possession of any person while providing education and care and working directly with children. Any exception to this should be for limited, essential purposes that are authorised in writing (or through another means if written authorisation is not reasonably practicable) by the Approved Provider of the service, and where that access does not impede the active supervision of children.

Part 3

Essential purposes for which use and/or possession of a personal electronic device may be authorised for purposes other than taking images or recording videos of children include:

- communication in an emergency situation involving a lost child, injury to child or staff member, or other serious incident, or in the case of a lockdown or evacuation of the service premises.
- personal health requirements, e.g., heart or blood sugar level monitoring.
- disability, e.g., where a personal electronic device is an essential means of communication for an educator or other staff member.
- family necessity, e.g., a worker with an ill or dying family member.
- technology failure, e.g., when a temporary outage of service-supplied electronic devices has occurred.
- local emergency events occurring, to receive emergency notifications through government warning systems, for example, bushfire evacuation text notification.

Part 4

Approved Providers and their services should have strict controls in place for the appropriate storage and retention of images and videos of children.

Considerations for Supervision

Child abuse, cyberbullying, and access to unsafe online environments can occur when the physical environment creates opportunities for a perpetrator to isolate a child without supervision or scrutiny. Supervising children when they use digital devices, particularly when accessing an online environment, is very important to keep them safe. Even if an educator is in the same room, they need to actively supervise a child using digital media and online environments.

High-risk behaviours for children online include:

- uploading private information or images
- engaging with inappropriate content (both inadvertently and purposefully)
- making in-app purchases
- interacting with unsafe individuals.

Active supervision helps prevent incidents and enables educators to step in if something goes wrong. It also creates a supportive environment where children feel comfortable making a disclosure or asking for help to learn how to use online programs, apps, etc, safely and appropriately, without fear of reprisal.

Active supervision is facilitated by the physical design and maintenance of the premises (Regulation 115), the supervision practices of educators (Section 165), and educator ratios (Section 169, Regulations 122-123).

Storage and Retention of Images

- Images will be stored locally, on devices which remain in the service when not in use.
- Images are uploaded to a secure Google Photos account to be displayed on devices at the service only.
- Images are curated before being uploaded to albums for display, to remove any images which may be inappropriate, e.g., visible underwear during gymnastics pose or a child with no photo permission visible in the background.
- Physical (printed) images of children and staff are displayed around the service's main OOSH Building.
- Images of children and staff are displayed on the service website with child, staff, and parental consent.
- Images may be sent to parents via text or email if the photo contains only the children of the recipient.
- Images may be sent to parents via Xplor as part of learning stories, updates, or incident reports.
- Faces of children are blurred on images used in newsletters sent to families unless written consent to share photos has been obtained from the child and parents of children in the image.
- Images will not be stored or distributed by any means other than those stated above.

Destruction of Images

The service will take reasonable steps to ensure that personal information is securely stored and not misused. To further protect privacy, the service is committed to the timely destruction or de-identification of personal information when it is no longer needed for the purpose it was collected. Images and recordings of children will also be deleted when no longer relevant for the purpose they were collected. Turramurra OOSH will retain digital material only as long as required for the approved purpose and retention timeframes under Regulation 183 before destruction including:

- images and video of children
- authorisation required for taking, storing, using and destroying images and videos of children
- unused printed photographs will be shredded or securely destroyed to prevent any unauthorised retrieval or misuse.

The Approved Provider will 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.

When a child exits the service their individual educational documentation and personal information is exported to our secure external hard drive which is password encrypted.

Safe use of Online Environments

- Educators and volunteers will access and use online environments in line with the OOSH Code of Conduct and relevant communication protocols.
- Children and educators will engage with the online environment for research and program enrichment.
- When children are engaged with the online environment, they will be always supervised closely by educators to ensure safe online practices are used.
- Child safety restrictions will be utilised on all child-use devices. Any online activity will be closely monitored by staff.
- Children are not permitted to use service-supplied or personal devices to communicate online in line with standard eight of the Child Safe Standards.
- Where possible, children will not be subjected to in-game or media advertising whilst using service-supplied devices.

Consequences of Misuse

- If a child is found to be misusing technology within OOSH, whether it is their own device or a service-supplied device, the device will be removed from the child, and the parents/guardians will be informed. If the device is a personal device, it will be returned to parents/guardians upon pick up. If the misuse is continued or deemed serious enough, OOSH's *Behaviour Management policy* will be referred to.
- If educators are found to be using personal devices for anything other than what has been previously outlined within this policy or without previous agreement with the Responsible Person, they will be asked to return their device to their locker in accordance with the *Code of Conduct*.
- If misuse of technology by children and young people, educators, management or parents is deemed to be in breach of Child Safe Standards, the OOSH Code of Conduct, or the Online Safety Act 2021 and poses a risk to the wellbeing and safety of children and young people, it will be reported through either the eSafety website or the ReportCyber government website. The breach will be notified to management and the committee, along with the school and a police report will be made if applicable.

Safety and content guidelines and expectations

- OOSH will only engage with movies, apps and games with age-appropriate G or PG classifications unless written parental permission is provided for older children to watch a specific 'M rated' movie.
- PG rated content will be vetted by staff to be deemed appropriate before use with children. Some PG content may be deemed appropriate for older children. This content may be shown in a separate space, with limited access to children of appropriate age.
- Parental Lock filters and appropriate safety settings are placed on all devices accessed by children to ensure content being accessed and viewed is age appropriate.
- Children will be taught about the importance of not sharing personal information online.
- Personal data is protected and not shared without consent. Personal data is password protected with only management access to personal information.
- Information collected on Xplor is protected as per their 'Privacy Notice.'
- Microsoft Defender Antivirus Software is installed on service-supplied devices to detect, protect and respond to online threats.
- Training is provided for staff in line with standard seven of the Child Safe Standards, on safe technology practices including how to monitor and guide children's technology use effectively.
- Educators will use their training to educate children about digital literacy, including safe online behaviour, recognising inappropriate content, and understanding the importance of privacy and security.

CCTV

CCTV is not in use at Turramurra Public School or South Turramurra OOSH and there are no current plans for its installation.

References and Related Policies and Procedures

References

- National Quality Standard, Quality Area 2: Children's health and safety: Standard 2.2, Element 2.2.3
- National Quality Standard, Quality Standard 4: Staffing arrangements
- National Quality Standard, Quality Area 5: Relationships with children: Standard 5.1, Element 5.1.2
- National Quality Standard, Quality Area 7: Governance and leadership: Standard 7.1, Elements 7.1.2, 7.1.3
- National Principles for Child Safe Organisations: <https://childsafe.humanrights.gov.au/national-principles>

Related Policies and Procedures

- Child Protection
- Supervision
- Providing a Child Safe Environment
- Staffing Policy
- Professional Standards and Ethical Conduct
- Code of conduct
- Play
- Interactions with children
- Health and safety

Approval and Revision History

Review Date	Reviewed By	Approved By	Next Review
18/08/2025	Courtney Sparkes	Scott Everard	August 2025
29/08/2025	Scott Everard	Melanie Shea	August 2026
20/01/2026	CELA	Scott Everard	January 2027