

SAFE USE OF DIGITAL TECHNOLOGIES AND ONLINE ENVIRONMENTS POLICY

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

PURPOSE

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

The use of Close Circuit Television (CCTV) installed at the OSHC Service aims to address crime prevention strategies to reduce concerns, deal with complaints and support investigations.

IMPLEMENTATION

Our OSHC 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/out platforms and CCTV monitoring. Our educators are diligent in ensuring children are only able to access age-appropriate technology on a Service issued device.

DIGITAL TECHNOLOGY AND ELECTRONIC DEVICES USED AT THE SERVICE

Our Service adopts and aligns with the [National Model Code](#) for taking images or videos of children.

The approved provider will inform staff, educators, visitors and family members that the use of personal electronic devices used to take, store or transfer images or videos of children who are being educated and cared for at the OSHC Service is strictly prohibited. This includes items such as tablets, mobile phones, computers/laptops, digital cameras, smart watches, META sunglasses (wearables) and personal storage and file transfer media (such as SD/memory cards, USB drives, hard drives and cloud storage) and other new and emerging technologies. These devices should not be in the possession of educators or visitors while working directly with children, including during excursions or when children are being transported

Staff and educators are advised that electronic devices supplied or issued by and registered with to the OSHC Service must not be removed from the premises as they may contain personal details of staff or children, including photos or videos. Except where required for operational activities, for example excursions or transportation.

SERVICE-SUPPLIED OR ISSUED ELECTRONIC DEVICES

Service-supplied or issued devices must be configured to comply with Service policies and procedures as outlined within this policy. Our Service will maintain records of electronic Service-supplied devices. Including the date of supply, type of device, make, model, serial number, name and signature of approved provider supplying the device and a declaration that the device is configured to operate in line within this policy. If the device is no longer used within the Service, a record of revocation will be documented

Our OSHC Service in conjunction with the nominated supervisor will develop and maintain a register of all electronic devices purchased for and used within the Service. Each device purchased for and used at the centre will be clearly marked with an identification code and marked to state it is property of the Service. This register will include details such as the identification code, device type, date of purchase, intended use, assigned user (if applicable), security settings, and any features related to connectivity, data storage, or recording capabilities. Devices recorded in the register may include, but are not limited to, computers, tablets, mobile phones, cameras, CCTV systems, audio recorders, DVD player, Playstation and any other internet-connected or data-enabled devices used within the Service. Electronic devices issued by and registered with the OSHC Service will be stored in the OSHC office.

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

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 OSHC Service-supplied or issued digital devices. Images and videos will be stored securely with password protection, with access limited to authorised personnel only. Images and videos of children must only be taken and used in accordance with OSHC Service policies, and careful consideration given to the purpose of the image or video. Educators will engage in discussions that consider the intent, appropriateness, context and consent involved in capturing and using the images and videos, ensuring the process aligns with children's learning, wellbeing and right to privacy.

Our OSHC Service will regularly review how digital data, including images and videos of children, is stored. Digital data stored at the OSHC Service will be destroyed in accordance with the *Record Keeping and Retention Policy* and procedure. The approved provider will ensure staff, educators, visitors do not transfer images or videos from OSHC Service issued devices to personal devices, unauthorised transferring of digital data may result in disciplinary action.

PHYSICAL ENVIRONMENT AND ACTIVE SUPERVISION

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

- ensure children are always supervised and never left unattended whilst an electronic device is connected to the internet
- provide a child safe environment to children- reminding them if they encounter anything unexpected that makes them feel uncomfortable, scared or upset, they can seek support from staff
- reflect on our 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/equipment allows educators to remain in line-of-sight of other staff members when working with children



- ensure all visitors are supervised at all times
- ensure all devices are password protected with access for staff only
- where digital devices are used during transportation and excursions, they must be used in accordance with practices outlined within this policy and associated procedure.

SOFTWARE PROGRAMS AND APPS

Our OSHC 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 OSHC Service. All apps used by educators and visitors are carefully selected, regularly checked and kept up to date with the latest available system updates. Access to software programs and apps are password protected to ensure the privacy of children, families and staff. Each user is required to create their own user account and ensure log in, and password information is not shared.

The approved provider will ensure programs which require additional background checks, such as CCS Software, are only accessed by authorised staff who have completed necessary screening processes in accordance with Family Assistance Law. Our educational program software is used by educators to share observations, photos, videos, daily reports, and learning portfolios with families in a secure, closed platform. In addition, our OSHC Service may use accounting and payroll software such as Lightning, HR systems, and compliance tools. These platforms assist in managing the Service's financial, staffing, and operational requirements.

CONFIDENTIAL AND PRIVACY GUIDELINES

Our *Privacy and Confidentiality Policy* applies to all use of digital technology and online environments. All staff, educators, and visitors must ensure that any information, images, or digital content related to children, families, and the Service is collected, stored, used, and shared in accordance with privacy legislation and Service procedures, to maintain confidentiality and protect the safety and wellbeing of children. The nominated supervisor will advise the approved provider as soon as possible regarding any potential threat to security information and access to data sensitive information. Our OSHC Service will follow practices outlined within the *Safe Use of Digital Technologies and Online Environments Procedure* to protect personal and sensitive digital data.

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

- a device containing personal information about children and/or families is lost or stolen (parent names and phone numbers, dates of birth, allergies, parent phone numbers)
- a data base with personal information about children and/or families is hacked
- personal information about a child is mistakenly given to the wrong person (portfolios, child developmental report)
- this applies to any possible breach within the OSHC Service or if the device is left behind whilst on an excursion

USE OF CLOSED-CIRCUIT TELEVISION (CCTV) MONITORING

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

Access to the monitor is restricted through a password-protected system to ensure security and prevent unauthorised viewing. Families are informed the OSHC Service uses CCTV as a surveillance method during enrolment and orientation to the OSHC Service.



CAMERA USE

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

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

CAMERA LOCATIONS

- The entrance and exit points of the site and surrounding the buildings.

Cameras are not installed indoors or in private areas such as bathrooms or shower areas (for adults or children). All cameras are clearly visible.

The CCTV recording system operates in real mode, monitoring the site continuously 24 hours a day. Footage and information collected via the recording system will be governed by [Australian Privacy Principles](#) and all relevant staff will be kept up to date with requirements under Australia's privacy law. CCTV footage is kept in a secure location, located school meeting room at the OSHC Service for a period of up to 7 days. Any recorded footage will be destroyed or de-identified when it is no longer needed for the purpose it was collected.

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

Access to the recordings will only be disclosed to:

1. to a member or officer of a law enforcement agency e.g., Police for use in assisting with investigations.
2. the approved provider or nominated supervisor to investigate situations that may have occurred.

THE APPROVED PROVIDER/NOMINATED SUPERVISOR/MANAGEMENT WILL ENSURE:

- that obligations under the *Education and Care Services National Law and National Regulations* are met
- educators, staff, students, visitors and volunteers have knowledge of and adhere to this policy and associated procedure
- new employees and students are provided with a copy of the *Safe Use of Digital Technologies and Online Environments Policy* and procedure as part of their induction and are advised on how and where the policy can be accessed
- all educators are aware of current child protection law, National Principles for Child Safe Organisations and their duty of care to ensure that reasonable steps are taken to prevent harm to children
- families are aware of this *Safe Use of Digital Technologies and Online Environments Policy* and procedure and are advised on how and where the policy can be accessed
- 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
- they promote and support a child safe environment, ensuring adherence to the *Child Safe Environment and Child Protection Policies*
- professional learning is provided to educators and staff relating to the safe use of digital technologies and online environments
- children, educators and parents are aware of our OSHC Service's complaints handling process to raise any concerns they may have about the use of digital technologies or any other matter (see: *Dealing with Complaints Policy*)



Government of South Australia
Department for Education

- the OSHC Service *Privacy and Confidentiality Policy* is adhered to at all times by staff, educators, families, visitors, volunteers and students
- parents/guardians are informed of how the OSHC Service will take, use, store and destroy images and videos of children enrolled at the Service during enrolment and orientation
- written authorisation is requested from families to take, use, store and destroy digital documentation including images and videos of children
- images or videos of children are not taken, used or stored without prior parent/guardian authorisation
- a record of all children who are NOT to be photographed or captured on video is to be developed, maintained and shared with educators and staff. This record will remain private and confidential.
- written authorisation is obtained from parents/guardians to collect and share personal information, images or videos of their children for programming purposes and newsletter via Edsmart
- Early Childhood Professionals (ECIP) visiting the Service must obtain authorisation from the approved provider and parent/guardian prior to taking images or videos of children whilst at the Service. Images and videos must NOT be taken on personal devices.
- families are informed to withdraw authorisation, a written request is required
- images and videos for individual children are deleted or destroyed and removed from storage when authorisation has been revoked from the parent/guardian
- they review how images and videos are stored on a regular basis and ensure new educators and staff have access to relevant folders and files, if required, in accordance with their role
- digital data is stored securely, whether offline or online, using a cloud-based service, and that data is archived regularly (monthly is recommended)
- images and videos are deleted or destroyed and removed from storage devices in accordance with the *Record Keeping and Retention Policy*, images and videos used for documenting children's learning and development must be held for 3 years after the child's last day of attendance
- every child in our care is protected from any exploitation of photographic and video images of themselves whilst they attend the Service
- images or videos of children must be appropriate in nature and 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
- educators, families and children are informed of updates to policies, procedures or legislation relating to digital technologies and online environments
- a review of practices is conducted following an incident involving digital technologies or online environments, including an assessment of areas for improvement
- educators are informed of, and adhere to recommended timeframes for 'screen time' according to Australia's Physical Activity and Sedentary Behaviour Guidelines:
 - children 5-12 years of age should limit screen time for entertainment to no more than 2 hours a day.
- the use of watching DVD's is kept to a minimum, with programs are chosen that are engaging and age appropriate to children. When used, the following conditions apply:
 - only 'G' and 'PG' rated television programs and movies will be viewed at the Service
 - programs depicting violence and/or inappropriate content (including graphic news reports) will not be shown
 - TV programs or videos will only be shown that have positive messages about relationships, family and life

EDUCATORS WILL:

- adhere to the *Safe Use of Digital Technologies and Online Environments Policy* and associated procedure
- ensure they are aware of current child protection law, National Principles for Child Safe



- ensure they promote and support a child safe environment, including adherence to the *Child Safe Environment* and *Child Protection* policies and mandatory reporting obligations
- not breach children and families' privacy
- keep passwords confidential and log out of computers and software programs after each use
- ask permission before taking photos of children on any device and explain to children how photos of them will be used and where they may be published

FAMILIES WILL:

- adhere to the *Safe Use of Digital Technologies and Online Environments Policy* and associated procedure
- not use personal electronic devices, such as mobile phones, smart watches or META sunglasses, to take photos, record audio, or capture video of children being educated and cared for at the OSHC Service
- provide written authorisation indicating whether or not the Service may take, use, store or destroy images or videos of their child
- provide written notification if they wish to withdraw the authorisation for the Service to take, use, store or destroy images and videos of their child
- be able to withdraw authorisation for the Service to take, use, store or destroy images or videos of children at any time in writing
- be provided with clear information about how to make a complaint and our complaints handling processes
- be aware that sometimes other children in the OSHC Service may feature in the same photos, videos, and/or observations as their children. In these cases, families are never to duplicate or upload them to the internet/social networking sites or share them with anyone other than family members.

VISITORS WILL:

- adhere to the *Safe Use of Digital Technologies and Online Environments Policy* and associated procedure whilst visiting the OSHC Service
- not use personal electronic devices, such as mobile phones smart watches or SMART Glasses (wearables), to take photos, record audio, or capture video of children being educated and cared for at the OSHC Service
- obtain written authorisation from parents/guardians and the approved provider to capture images or video of a child for observation/documentation purposes only. This applies to visitors who are supporting children at the OSHC Service (NDIS funded support professionals, Inclusion Support professionals) (See *ECIP Confidentiality Agreement*).

BREACH OF POLICY

Staff members or educators who fail to adhere to this policy may be in breach of their terms of employment and may face disciplinary action which may lead to notification to the regulatory authority and child protection. 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.

RESOURCES

Australian Children's Education & Care Quality Authority. [National Model for Early Childhood Education and Care.](#)
[Australian Government Office of the eSafety commission](#)
[eSafety Early Years Program for educators](#)
[eSafety Early Years Program checklist](#)
[eSafety Young People](#)
[eSmart Alannah & Madeline foundation](#)



Government of South Australia
 Department for Education

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

Office of the Australian Information Commissioner (OAIC)

CONTINUOUS IMPROVEMENT/REFLECTION

Our *Safe Use of Digital Technologies and Online Environments Policy* will be reviewed on an annual basis 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.

SOURCES

Australian Children's Education & Care Quality Authority. (2025). [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 Government eSafety Commission (2020) www.esafety.gov.au

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

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

Australian Government, Office of the Australian Information Commissioner. (2019). Australian Privacy Principles:

<https://www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/>

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

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

Early Childhood Australia Code of Ethics. (2016).

[Education and Care Services National Law Act 2010](#). (Amended 2025)

[Education and Care Services National Regulations](#). (Amended 2025)

NATIONAL QUALITY STANDARD (NQS)

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



Government of South Australia
Department for Education

EDUCATION AND CARE SERVICES NATIONAL LAW AND NATIONAL REGULATIONS	
S. 162A	Child protection training
S. 165	Offence to inadequately supervise children
S. 167	Offence relating to protection of children from harm and hazards
12	Meaning of serious incident
73	Educational Program
76	Information about educational program to be given to parents
84	Awareness of child protection law
115	Premises designed to facilitate supervision
122	Educators must be working directly with children to be included in ratios
123	Educator to child ratios – centre-based services
155	Interactions with children
156	Relationships in groups
168	Education and care services must have policies and procedures
168(2)(ha)	The safe use of digital technologies and online environments at the service
170	Policies and procedures to be followed
171	Policies and procedures to be kept available
172	Notification of change to policies or procedures
175	Prescribed information to be notified to Regulatory Authority
176	Time to notify certain information to Regulatory Authority
181	Confidentiality of records kept by approved provider
183	Storage of records and other documents
184	Storage of records after service approval transferred



RELATED LEGISLATION

Child Care Subsidy Secretary's Rules 2017	Family Law Act 1975
A New Tax System (Family Assistance) Act 1999	<i>Privacy Act 1988</i> (the Act)
Family Assistance Law – Incorporating all related legislation as identified within the Child Care Provider Handbook	

REVIEW

POLICY REVIEWED BY	Jason Sheehy	Principal	01/12/2025
POLICY REVIEWED		NEXT REVIEW DATE	01/12/2026
VERSION NUMBER	V3.11.25		
MODIFICATIONS			
POLICY REVIEWED	PREVIOUS MODIFICATIONS		NEXT REVIEW DATE

