SAFE USE OF DIGITAL TECHNOLOGIES AND ONLINE ENVIRONMENTS POLICY

Highland Grove Preschool 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 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.

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 Protection Child Safety and Protection (effective Jan 2026)	Management, educators and staff are aware of their roles and responsibilities to identify and respond to every child at risk of abuse or neglect. 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 that is child safe.

EDUCATION AND CARE SERVICES NATIONAL LAW AND NATIONAL REGULATIONS	
S. 162A	Child protection training
S. 165	Offence to inadequately supervise children
S. 166A	Offence to subject child to inappropriate conduct [NSW]
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
149	Volunteers and students
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

PURPOSE

Children's safety and wellbeing is paramount, and our 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 Service philosophy, and privacy and legislative requirements to ensure the safety of enrolled children, educators and families. We believe that children's safety, rights, and best interests are the paramount consideration for all Service operations, decisions and functions.

SCOPE

This policy applies to children, families, staff, educators, management, approved provider, nominated supervisor, students, volunteers and visitors of the Service.

TERMINOLOGY For additional definitions and key terms used within this policy, refer to *Key Terms – Policies and Procedures.*	
Artificial intelligence (AI)	An engineered system that generates predictive outputs such as content, forecasts, recommendations, or decisions for a given sent of human defined objectives or parameters without explicit programming.
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 and equipment/devices, including mobile phones and 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	Includes: images and videos of child sexual abuse Content that advocates terrorist acts Content that promotes, incites or instructs in crim or violence Footage of real violence, cruelty and criminal activity
Optical Surveillance Device	Has the same meaning as in section 6(1) of the Surveillance Devices Act 2004 of the Commonwealth
Online hate	Any hateful posts about a person or group based on their race, religion, ethnicity, sexual orientation, disability or gender
Smart toys	Smart toys generally require an internet connection to operate as the computing task is on a central server
Sexting	Sending a sexual message or text, with or without a photo or video. It can be done using a phone service or any platform that allows people to connect via an online message or chat function
Unwanted contact	Any type of online communication that makes you feel uncomfortable, unsafe or harassed

Source: Glossary to NQF Child Safe Culture and Online Safety Guides- ACECQA 2025

IMPLEMENTATION

Highland Grove 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. 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

We follow the National Model Code for taking images or videos of children. The use of personal electronic devices, record audio or capture children who are being educated and cared for at this service is strictly prohibited. This includes items such as tablets, phones, digital cameras, smart watches, META sunglasses 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 staff while working directly with children. In the case of visiting professionals (such as allied health professionals) working with children at our centre, parents/guardians can sign for permission to allow a device to be used while working with the child, however this relates strictly to only the child being visited at that time.

Staff and educators are advised that electronic devices belonging to Highland Grove must not be removed from the premises as they may contain personal details of staff or children, including photos or videos. The exception is for operational activities, for example emergency evacuations or excursions.

The approved provider will inform staff, educators and visitors of exemptions that may warrant a person to use or be in possession of a personal electronic device that can be used to take images or videos. Staff, educators or visitors with an exemption must not use the personal device to take images or videos of children. Requests and approved exemptions are required to be in writing and recorded in the designated Register kept in the office, and may include:

- Emergency communication during incidents such as a lost child, injury, lockdown, or evacuation
- Personal health needs requiring device use (e.g. heart or blood sugar monitoring)
- Disability related communication needs
- Urgent family matters (e.g. critically ill or dying family member)
- Local emergency event to receive alerts (e.g. government bushfire or evacuation notifications).

This registering of the exemption will include details such as the device type, intended use and assigned user/space (if applicable).

Children enrolled at Highland Grove are not permitted to bring electronic devices to the service, unless an exception has been discussed with the approved provider or nominated 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 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 Service 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 our 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.

PHYSICAL ENVIRONMENT AND ACTIVE SUPERVISION

The centre director, leaders 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 physical environment, layout and design to ensure it supports child safe practices when children are engaged in using technology
    - perform annual reviews of the centre 'Digital Technologies and online Environments' Risk Assessment to identify risks to children's safety.
    - ensure location of digital technology/equipment allows educators to remain in line-of-sight of other staff members 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 visitors and volunteers 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

Highland Grove uses a range of secure software programs and apps on service-issued devices to support the educational program and administration. All apps used by staff, educators, visitors and children 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.

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. In addition, our Service may use accounting and payroll software HR systems, and compliance tools. These platforms assist in managing the Service's financial, staffing, and operational requirements.

ARTIFICIAL INTELLIGENCE (AI) INTERACTIONS AND GUIDELINES

Educators or staff using AI are to be aware of limitations, privacy risks, and the potential for errors in the information it provides. AI can support and assist staff as a documentation tool; however, it is their responsibility to ensure the information's accuracy and not rely upon it as an authoritative source. Staff and educators should ensure they enter original work into the AI program and are required to monitor, verify, and check information obtained from AI to ensure specific details are contextually relevant. Data and privacy concerns must be addressed, and staff should not enter details which may identify individual children, such as names and date of birth.

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 Responsible Supervisor will advise the

approved provider as soon as possible regarding any potential threat to security information and access to data sensitive information. Highland Grove 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 Service or if the device is left behind whilst on an excursion
- ensure educators are aware of their mandatory reporting requirements and report any concerns
  related to child safety including inappropriate use of digital technology to the approved provider or nominated supervisor.

IDENTIFICATION AND REPORTING OF ONLINE ABUSE AND SAFETY CONCERNS

Highland Grove will implement measures to keep children safe whilst using digital technology and accessing online environments.

The centre director will:

- 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, to the approved provider or nominated supervisor [See *Child Protection Policy*]
- support educators to:
  - 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, adhering to the *Child Protection Policy, Behaviour Guidance: Bullying Policy* and reporting procedures
  - respond to and report any breaches and incidents of inappropriate use of digital devices and online services to management

- ensure all concerns are documented and responded to promptly and appropriately, with support provided to the child and their family as required
- 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 NQAITS, if a child is involved in a serious incident,
  including any unsafe online interactions, exposure to inappropriate content or suspected online abuse.

USE OF CLOSED-CIRCUIT TELEVISION (CCTV)

Our Service uses Closed-Circuit Television (CCTV) to monitor some of the physical environment outside of the playgrounds and classrooms, meaning access areas, carparks and adjoining fences and gates. No cameras are used in the children's spaces. The cameras utilised are for security purposes only.

THE CENTRE DIRECTOR 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, 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
- all staff, educators, volunteers and students are aware of current child protection law, National Principles for Child Safe Organisations (Child Safe Standards in NSW) 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
- they promote and support a child safe environment, ensuring adherence to the *Child Safe Environment and Child Protection Policies,* including mandatory reporting obligations
- the National Principles for Child Safe Organisations (Child Safe Standards in NSW) is embedded into the organisational structure and operations
- appropriate ratios and adequate supervision are maintained for children at all times including when using digital technology and accessing online environments

- students, volunteers and/or visitors are never left alone with a child whilst at Highland Grove under any circumstances
- all staff, educators, volunteers and students are aware of the National Model Code and Guidelines and adhere to these recommendations for taking images or videos of children including:
    - personal electronic devices or personal storage devices, that can take images or videos, are not used by educators, staff, visitors or volunteers when working directly with children
    - staff and educators only use electronic devices issued by the centre for taking images or videos of children enrolled at Highland Grove
    - Service issued devices are securely configured, monitored and maintained to prevent unauthorised access
    - visitors who are supporting children at the Service (For example: NDIS funded support professionals, Inclusion Support Professionals) obtain written authorisation from parents/guardians to capture images or video of a child for observation/documentation purposes only.
- children, educators and parents are aware of our 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*)
- the 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 Service will take, use, store and destroy images and videos of children enrolled at the Service during enrolment process
- written authorisation is obtained from parents/guardians 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
- written authorisation is obtained from parents/guardians to collect and share personal information, images or videos of their children online (Eg. Instagram). This is quite rare, however in the case where sharing would benefit our communication of curriculum, written permission is sought.
- 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
- the review of 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

- 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
- external agencies or specialists are consulted if concerns are identified relating to online abuse, cyberbullying or digital safety risks
- policies and procedures reflect a commitment to equity and diversity, protect children's privacy, and empower children to be independent
- they remain informed of privacy legislation through monitoring of updated from relevant government authorities such as the Office of the Australian Information Commissioner
- a risk assessment is conducted regarding the use of digital technologies and online environments by staff and children at the Service
- risk assessments for digital technology and online environments are reviewed annually or as soon as possible after becoming aware of any circumstances that may affect the safety, health or wellbeing of children
- policies and procedures are reviewed following an identification of risks following the review of risk assessments relating to the use of digital technologies and online environments
- staff, 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
- to install and maintain anti-virus and internet security systems including firewalls to block access to unsuitable web sites, newsgroups and chat rooms
- educators are informed of, and adhere to recommended timeframes for 'screen time' according to Australia's Physical Activity and Sedentary Behaviour Guidelines:
    - children birth to one year should not spend any time in front of a screen
    - children 2 to 5 years of age should be limited to less than one hour per day
    - children 5-12 years of age should limit screen time for entertainment to no more than 2 hours a day.
- they share information to families about recommended screen time limits based on *Australia's Physical Activity and Sedentary Behaviour Guidelines*
- that families will be made aware of professional photographers utilising a system of using a mobile phone to access a QR code to link the child's photos to an individual gallery. When photographs are ready to be purchased, this occurs online through the photographer's website and families can only view their own child's individual gallery via an individual code. Parents' permission will be sought for the centre to provide parent details to the

Photographers. Families who choose for their child's Group Photo not to be in each child's portal must notify the centre/photographer.

- TAFE – electronic devices will be used in the staff areas and not with the children in playrooms.

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 Organisations and their duty of care to ensure that reasonable steps are taken to prevent harm to children
- ensure they promote and support a child safe environment, including adherence to the *Child Safe Environment* and *Child Protection* policies and mandatory reporting obligations
- 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 operations, including when accessing digital technologies and online learning environments
- not use, or have access to, any personal electronic devices, including mobile phones or smart watches used to take images or video of children at the centre, unless there is an emergency
- keep passwords confidential and log out of computers and software programs after each use
- ensure children's personal information where children can be identified such as name, address, age, date of birth etc. is not shared online
- ensure that screen time is NOT used as a reward or to manage challenging behaviours under any circumstances
- introduce concepts to children about online safety at age-appropriate levels
- support children's understanding of online safety by providing age-appropriate guidance, discussions and activities that help them to recognise safe and unsafe online behaviours
- consult with children about matters that impact them, including the use of digital technologies and online environments, to ensure their voices are heard and respected in a meaningful way.
- Visitors to the centre will not be left alone with children. Professionals visiting in a support role and Professional Photographers will always be in hearing and/or sight of a member of staff.

FAMILIES WILL:

- adhere to the *Safe Use of Digital Technologies and Online Environments Policy* and associated procedure
- not upload photos or videos of any child other than their own, that are taken on the premises of Highland Grove Preschool, to social media.
- this includes being aware that sometimes other children who attend our centre may feature in the same photos, videos or observations as their child. 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.
- Families are also responsible for notifying their family and friends of this policy regarding other children, videos and images and social media.

VISITORS AND VOLUNTEERS WILL:

- adhere to the *Safe Use of Digital Technologies and Online Environments Policy* and associated procedure whilst visiting the centre
- 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 Highland Grove.
- NOTE: Visitors who are Allied Health or other professionals visiting children in a supporting capacity may obtain written authorisation from parents/guardians to capture images or videos of a child for observation/documentation purposes only. This applies to visitors who are supporting children at the centre (NDIS funded support professionals, Inclusion support professionals)
- report any concerns related to child safety, including inappropriate use of digital technology, to the approved provider or nominated supervisor

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. 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.

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

eSmart Alannah & Madeline foundation

Family Tech Agreement. eSafety Early Years Online safety for under 5s

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)

SOURCES

Australian Children's Education & Care Quality Authority. (2025). *Guide to the National Quality Framework*

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

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. (2025). *NQF Online Safety Guide*

Australian Government eSafety Commission (2020) www.esafety.gov.au

Australian Government Department of Education. (2025). *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://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)

NSW Government. (2025). Ministerial Direction. *Education and Care Services (Supply, Authorisation and Use of Devices) Order 2025.*

Office of the Australian Information Commissioner (OAIC)

Privacy Act 1988.

Western Australian Legislation Education and Care Services National Law (WA) Act 2012 (for WA Services only)

Western Australian Legislation Education and Care Services National Regulations (WA) Act 2012 (for WA Services only)

REVIEWED: 15/3/26