Safe Use of Digital Technologies and Online Environments Policy

Purpose

Children's safety and wellbeing is paramount and Ridgehaven OSHC has the responsibility to provide and maintain a safe and secure working and learning environment for educators, children, visitors and contractors, including online environments. As a child safe organisation, Ridgehaven OSHC embeds the National Principles for Child Safe Organisations and continuously addresses risks to ensure children are safe in physical and 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.

Scope

This policy applies to children, families, educators, management, approved provider, nominated supervisor, work experience/placement students, volunteers and visitors to Ridgehaven OSHC.

Terminology

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
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 crime or violence Footage of real violence, cruelty and criminal activity

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

Digital Technology and Electronic Devices used at the service

Ridgehaven OSHC follows the National Model Code and Guidelines for taking images or videos of children.

National Model Code for Early Childhood Education and Care	
Part 1	Only service-issued electronic devices should be used when taking images or videos of children while providing education and care. The appropriate use of service-issued 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 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 exceptions 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-issued electronic devices has occurred • local emergency event 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

All educators, visitors, volunteers, work experience/placement students and family members will be strictly prohibited from using personal electronic devices to take photos, record audio or capture video of children who are being educated and cared for at the service. This includes items such as tablets, phones, digital cameras, smart watches, META sunglasses, fitness trackers (with image taking and/or messaging capabilities) and personal storage and file transfer media (such as SD cards, USB drives, hard drives and cloud storage). These devices should not be in the possession of educators or visitors (e.g., ECEC professionals) while working directly with children.
The service's Family Handbook, new employee inductions, Employee and Student/Visitor Handbooks and other documents will include this policy and related procedures around the safe use of digital technologies and online environments.

Educators will not be permitted to remove electronic devices, belonging to the service, from the premises as they may contain personal details of other educators or children, including photos or videos.
Exceptions will be made when required for operational activities, such as excursions or transportation.
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, may be sort after by individuals through the Director (as an authorised representative of the Ridgehaven School Governing Council - approved provider).

Exemptions will be given in writing, by the Governing Council and/or Director, and may include:

- 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)

Educators or visitors with an exemption must not use their personal device to take images or videos of children.

A register of all electronic devices purchased for and used within the service will be developed and maintained. This register will include details such as the device type, date of purchase, intended use, assigned users (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, audio recorders and any other internet-connected or data-enabled devices used within the service.

Children are not permitted to bring personal electronic devices to the service, unless an exception has been discussed with the Governing Council or Director/Nominated Supervisor, when the device is required to support a diagnosed medical condition or disability. If a child brings an electronic device to OSHC, it will be switched off, stored in the office and given to caregivers upon collection.

Images and Videos

The Governing Council is responsible for determining who is authorised to take, use, store and destroy images and videos of children using service issued digital devices.
At Ridgehaven OSHC, paid educators, directly in contact with children, are authorised to take videos and images as part of the service's educational programs. The **Director/Nominated Supervisor** is authorised to take, use, store and destroy images and videos.
Digital images and videos will be stored securely on the service's password protected, administration computer, with access limited to authorised personnel only – Director/Nominated Supervisor, school leadership (Principal and Deputy Principal) and site I.T department. Images and videos of children will only be taken and used in accordance with 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.

Consent will be obtained from all caregivers, upon children's enrolment, for images and videos to be taken and used by the service, in accordance with service policies. Caregivers will be informed, through the service's enrolment form and Family Handbook, about the ways in which the service may use, store and dispose of their child's image.

Educators will regularly review how digital data, including images and videos of children, is stored. Back-ups of all digital data, whether offline or online (such as a cloud-based service), will be performed each month. Digital data stored at the service will be destroyed in accordance with the *Record Keeping Policy* and procedure. The Governing Council and Director/Nominated Supervisor will ensure educators, visitors and volunteers do not transfer images or videos from service issued devices to personal devices; unauthorised transferring of digital data may result in disciplinary action.

Physical Environment and Active Supervision

The Governing Council, Director/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 for children - reminding them if they encounter anything unexpected that makes them feel uncomfortable, scared or upset, they seek support from educators
- 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/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 visitors, volunteers and work experience/placement students are supervised at all times
- ensure all devices are password protected with access for educators 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

Ridgehaven OSHC uses a range of secure and approved (by the Department for Education) software programs and apps on approved and registered (through site-based I.T systems) service-issued devices to support the educational program and administration of the service.
All devices used at the service are connected to Ridgehaven School's secured wifi network, with Department for Education's EdProtect Internet Filtering and Security and monitored by SWiFT. All apps used by educators 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 educators. Each user is required to create their own user account and ensure log in, and password information is not shared.
The Governing Council and Director/Nominated Supervisor will ensure programs which require additional background checks, such as CCS software, are only accessed by authorised educators who have completed necessary screening processes in accordance with Family Assistance Law.

Xplor, 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 service uses Lightning Payroll software and compliance tools. These platforms assist in managing the service's financial, staffing, and operational requirements.

Artificial Intelligence (AI) Interactions and Guidelines

Educators using AI will be aware of limitations, privacy risks, and the potential for errors in the information it provides. AI can support and assist educators as a documentation tool; however, it is their responsibility to ensure the information's accuracy and not rely upon it as an authoritative source.
Educators will 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 educators should not enter details which may identify individual children, such as images, names and date of birth.

Confidentiality and Privacy Guidelines

Our *Privacy and Confidentiality Policy* applies to all use of digital technology and online environments. All 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 Director/nominated supervisor will advise the Governing Council, as soon as possible, regarding any potential threat to security information and access to data sensitive information. Ridgehaven OSHC will follow practices outlined within the *Safe Use of Digital Technologies and Online Environments Procedures* to protect personal and sensitive digital data.

The Governing Council 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

Educators will be aware of their mandatory reporting requirements and report any concerns related to child safety including inappropriate use of digital technology to the Director/Nominated Supervisor and Governing Council.

Identification and Reporting of Online Abuse and Safety Concerns

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

The Governing Council, Director/Nominated Supervisor and management will:

- ensure all educators, work experience/placement students, visitors 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 Governing Council, Line Manager or Director/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, Discrimination and Harassment 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 eSafety 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.

Responsibilities

Governing Council, Advisory Committee, Director/Nominated Supervisor will ensure

- obligations under the *Education and Care Services National Law and National Regulations* are met
- educators, work experience/placement students, visitors and volunteers have knowledge of and adhere to this policy and associated procedures
- new employees, work experience/placement students and volunteers are provided with a copy of the *Safe Use of Digital Technologies and Online Environments Policy* and procedures as part of their induction and are advised on how and where the policy can be accessed
- families are aware of this *Safe Use of Digital Technologies and Online Environments Policy* and procedures 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 Environments* and *Child Protection Policies*
- the National Principles for Child Safe Organisations is embedded into the organisational structure and operations
- all educators, volunteers, visitors and work experience/placement students 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
- professional learning is provided to educators relating to the safe use of digital technologies and online environments
- an *Electronic Device Register* for all electronic devices purchased and used at the service is developed, maintained and monitored
- an *Electronic Device Authorisation Register* for all people who have access to service electronic devices is developed, maintained and monitored
- appropriate ratios and adequate supervision are maintained for children at all times including when using digital technology and accessing online environments
- work experience/placement students, volunteers and visitors are never left alone with a child whilst at the service under any circumstances
- all educators, volunteers, visitors and work experience/placement students are aware of the National Model Code and Guidelines and adhere to these for taking images or video of children including:
  - personal electronic devices or personal storage devices, that can take images or videos, are not used when working directly with children
  - only using electronic devices issued by the service for taking images or videos of children enrolled at the service
  - service issued devices are securely configured, monitored and maintained to prevent unauthorised access

- visitors who are supporting children at the service (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 and provide it to the Director/Nominated Supervisor.

- children, educators and parents 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 (see: *Complaints & Grievances Policy*)
- the service's *Confidentiality and Privacy Policy* is adhered to at all times by educators, families, visitors, volunteers and work experience/placement 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 and orientation
- written authorisation is requested from families for authorised service educators 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 during enrolment, for children to use service electronic devices
- written authorisation is obtained from parents/guardians during enrolment, to collect and share personal information, images or videos of their children online (Facebook, Instagram and Xplor Playground)
- families are informed how 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 by the parent/guardian
- how images and videos are stored is reviewed on a regular basis and ensure new educators have access to relevant folders and files, if required, in accordance with their role
- digital data is stored securely, whether offline or online, 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 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
- all data contained on service electronic devices no longer in use (due to becoming obsolete, broken/damaged or decommissioned) is wiped and the device factory reset
- 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
- collaboration with relevant professionals, as required, to support equitable access to digital technologies for all children
- remain informed of privacy legislation through monitoring of updated from relevant government authorities such as the Office of the Australian Information Commissioner (OAIC)
- a risk assessment is conducted regarding the use of digital technologies by educators and children at the service, including accessing online environments
- 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
- 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 internet monitoring/filtering, anti-virus and 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 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.*

Educators will

- adhere to the *Safe Use of Digital Technologies and Online Environments Policy* and associated procedures
- 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 them safe
- promote and contribute to a culture of child safety and wellbeing in all aspects of service's operations, including when accessing digital technologies and online learning environments
- not use, or have access to, any personal electronic device capable of taking images or video of children at the service, access social media (Facebook, Instagram or other) or breach children, families' and other educator's privacy
- obtain written consent from the Governing Council and/or Director/Nominated Supervisor to access a personal electronic device for medical or emergency situations
- 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
- 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.

Families and authorised adults 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 AI glasses, to take photos, record audio, or capture videos of children being educated and cared for at the service
- be aware that sometimes other children in the service may feature in the same photos, videos, and/or observations as their children. In these cases, they are never to duplicate or upload them to the internet/social networking sites or share them with anyone without altering/blurring other children's images, so they cannot be identified.

Visitors and Volunteers will

- adhere to the *Safe Use of Digital Technologies and Online Environments Policy* and associated procedures whilst visiting the service
- 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 service
- report any concerns related to child safety, including inappropriate use of digital technology, to the Director or Responsible educator
- obtain written authorisation from parents/guardians to capture images or video of a child for observation/documentation purposes only. This applies to visitors who are supporting children at the service (NDIS funded support professionals, Inclusion Support professionals).

Breach of Policy

Educators who fail to adhere to this policy will be in breach of their terms of employment and will face disciplinary action. Visitors or volunteers who fail to comply to this policy will face termination of their engagement. Family members and other authorised adults who do not comply with this policy may place their child's enrolment at risk and limit the family members/authorised adult's access to the service.
Breaches will be dealt with by the Governing Council (as approved provider) on a case-by-case basis.

Continuous Improvement/Reflection

Our *Safe Use of Digital Technologies and Online Environments Policy* will be reviewed on an annual basis in consultation with children, families, educators and management. Families will be notified of changes to policies within 14 days to ensure they remain informed and can provide feedback or ask questions as needed.

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 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 2023).
• Education and Care Services National Regulations. (Amended 2023).
• *Office of the Australian Information Commissioner (OAIC)*
• *Privacy Act 1988.*
• *Western Australian Legislation Education and Care Services National Law (WA) Act 2012*
• *Western Australian Legislation Education and Care Services National Regulations (WA) Act 2012*

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 that is child safe.

Education and Care Services National Regulations

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
149	Volunteers and students
155	Interactions with children
156	Relationships in groups
168	Education and care services must have policies and procedures
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	*Privacy Act 1988* (the Act)
Family Assistance Law – Incorporating all related legislation as identified within the Child Care Provider Handbook	

Review

POLICY DEVELOPED & RATIFIED	Ridgehaven OSHC Management Committee & Ridgehaven School Governing Council (operator) in conjunction with Childcare Centre Desktop		SEPTEMBER 2025
POLICY REVIEWED		NEXT REVIEW DATE	AUGUST 2026
AUGUST 2025	• New policy developed following changes to child safety regulations effective from 1 September 2025 • Merger of the following policies: Information Technologies – Acceptable Use Policy and Mobile Device Policy		
POLICY REVIEWED	PREVIOUS MODIFICATIONS		NEXT REVIEW DATE