Safe Use of Technologies & Online Environment Policy

Policy Relevant to:	All Team members, educators, families, volunteers and visitors
Last Reviewed:	August 2025
Next Review:	August 2027
ECS National Law:	S.162A, S165, S167
ECS National Regulations:	r12, r73, r76, r84, r115, r122, r123, r149, r155, r156, r168, r170, r171, r172, r175, 176, r181, r183, r184
NQS:	2.2, 2.2.1, 2.2.3, 7.1.2
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

Adventure Patch is committed to fostering a culture that creates and maintains a safe online environment with support and collaboration from staff, families and the community. As a child safe organisation. Our services embed the National Principles for Child Safe Organisations and continuously address the 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 technologies in a child-safe environment.

Purpose

Children's safety and well-being is paramount, and Adventure Patch 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 philosophy, privacy and legislative requirements to ensure the safety of enrolled children, educators and families.

TERMINOLOGY	
Artificial intelligence (AI)	An engineered system that generates predictive outputs such as content, forecasts, recommendations, or decisions for a given set 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 abused, 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
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

Adventure Patch services use 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 services

Adventure Patch follows the National Model Code and Guidelines for taking images or videos of children. This is attached to the policy for reference. Reference *Personal Electronic Device Policy*.

Adventure Patch will inform staff, educators, visitors, volunteers and family members that the use of personal electronic devices to take photos, record audio, or capture video of children who are being educated and cared for at our services 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 cards, USB drives, hard drives and cloud storage). These devices should not be in the possession of staff, educators or visitors (e.g. ISS professionals) while working directly with children.

Staff and educators are advised that electronic devices belonging to Adventure Patch 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.

Adventure Patch 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. Exemptions need to be provided for in writing (*Exemption for use of Personal Electronic Device Form*) 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)

Adventure Patch will develop and maintain a register of all electronic devices purchased for and used within our services. This register will include details such as the 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, smart toys, baby monitors and any other internet-connected or data-enabled devices used within Adventure Patch.

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

Images and Videos

Adventure Patch 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 Adventure Patch policies, and careful consideration must be 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.

Adventure Patch 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 regularly. Digital data stored at services will be destroyed in accordance with the *Record Keeping and Retention Policy* and procedure.

Adventure Patch will ensure staff, 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

Adventure Patch and our nominated supervisors, 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 that 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 the 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

Adventure Patch uses a range of secure software programs and apps on service-issued devices to support the educational program and administration of the service. 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 is protected to ensure the privacy of children, families and staff. Software programs and Apps are centrally controlled.

Adventure Patch will ensure programs that require additional background checks, such as CCS Software, are only accessed by authorised staff who have completed necessary screening processes in accordance with the 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, we may use accounting and payroll software such as MYOB, HR systems, and compliance tools. These platforms assist in managing Adventure Patch's financial, staffing, and operational requirements.

Artificial Intelligence (AI) Interactions and Guidelines

Educators and staff members adopting the use of generative chatbot AI need to be aware of limitations, privacy risks and the potential for errors in the responses and information generated. AI can assist and support staff as a documentation tool; however, it is their responsibility to ensure the accuracy of information generated and not rely upon it as an authoritative source.

Educators and staff should ensure they input original work into the AI program/tool 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 that 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 Adventure Patch services is collected, stored, used, and shared in accordance with privacy legislation and Adventure Patch procedures, to maintain confidentiality and protect the safety and well-being of children.

Report as soon as possible regarding any potential threat to security information and access to data-sensitive information. Our services will follow practices outlined within the *Safe Use of Digital Technologies and Online Environments Procedure* to protect personal and sensitive digital data.

Adventure Patch 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 database 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

Adventure Patch will implement measures to keep children safe whilst using digital technology and accessing online environments.
Adventure Patch 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 management.
- 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 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.

Adventure Patch 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 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 is embedded into the organisational structure and operations.
- Professional learning is provided to educators and staff relating to the safe use of digital technologies and online environments.
- Develop and monitor an *Electronic Device Register* for all electronic devices purchased and used at services.
- 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 Adventure Patch services 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 video 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 Adventure Patch 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.
- Children, educators and parents are aware of the Adventure Patch complaints handling process to raise any concerns they may have about the use of digital technologies or any other matter (see: *Complaints and Grievances Policy(Families)*)
- The Adventure Patch *Privacy and Confidentiality Policy* is adhered to at all times by staff, educators, families, visitors, volunteers and students.
- Parents/guardians are informed of how our services will take, use, store and destroy images and videos of children enrolled at our services 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.
- Written authorisation is obtained from parents/guardians for children to use electronic devices.
- Written authorisation is obtained from parents/guardians to collect and share personal information, images or videos of their children online (Website, Facebook, Instagram, Playground or Xplor).
- 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.
- 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.
- They remain informed of privacy legislation through monitoring of updates 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 staff and children at services, 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 well-being 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 websites, 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 from 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 with 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 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, ensuring adherence to the *Child Safe Environment* and *Child Protection Policies,* including mandatory reporting obligations.
- Participate in practical training related to digital safety, privacy protection and responsible use of technology.
- Understand the critical importance of implementing active supervision strategies when children are accessing online environments to keep children safe.
- Promote and contribute to a culture of child safety and wellbeing in all aspects of our Service's 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 Service, access social media (Facebook, Instagram or other) or 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.
- 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 Will:

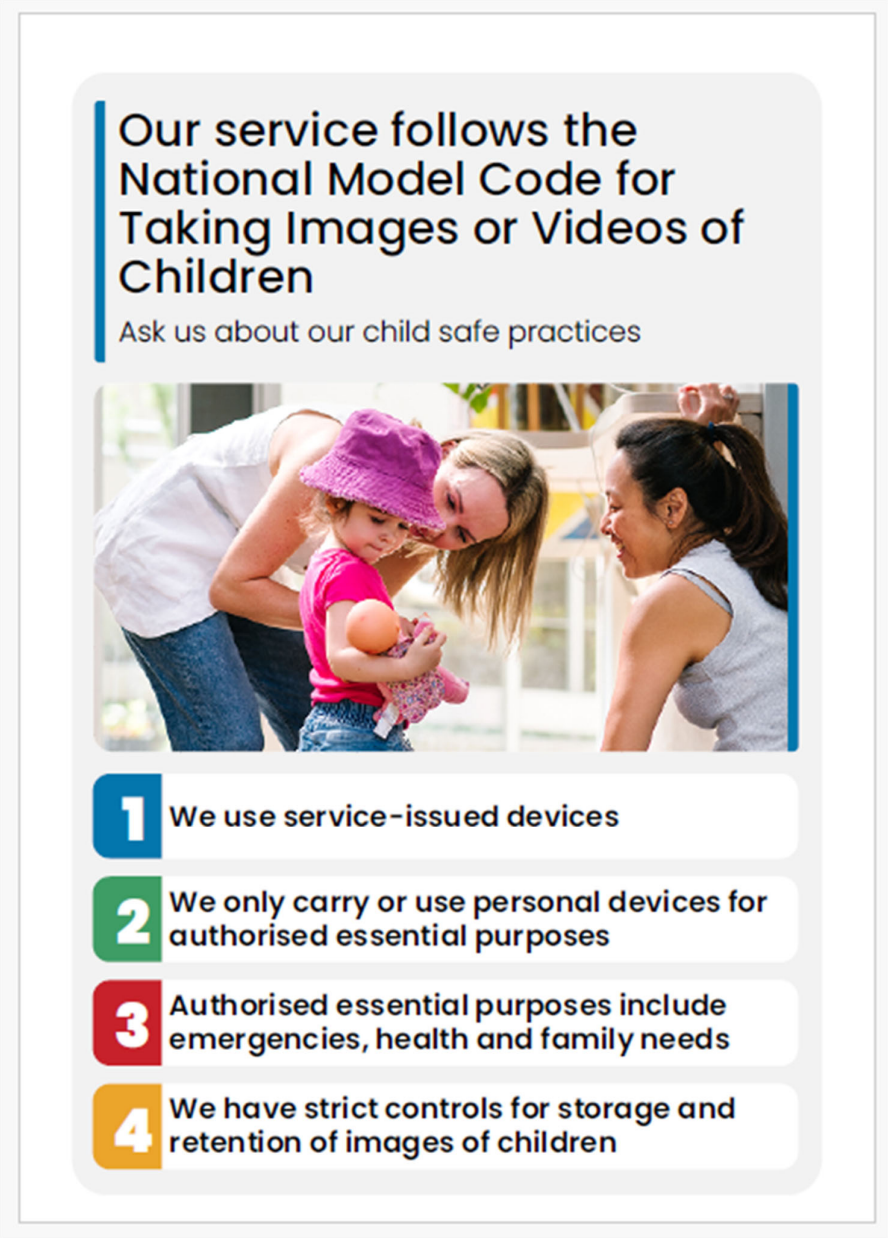
- Adhere to the *Safe Use of Digital Technologies and Online Environments Policy* and associated procedure.
- Not use personal electronic devices, such as mobile phones, smart watches or META sunglasses, to take photos, record audio, or capture video of children being educated and cared for at Adventure Patch services.
- 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, families are never to duplicate or upload them to the internet/social networking sites or share them with anyone other than family members.

Visitors and Volunteers Will:

- Adhere to the *Safe Use of Digital Technologies and Online Environments Policy* and associated procedure whilst visiting the Adventure Patch services.
- 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 Adventure Patch services.
- Report any concerns related to child safety, including inappropriate use of digital technology, to the approved provider or nominated supervisor.
- 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) .

National Model Code

ACECQA, in partnership with all governments, developed the National Model Code and Guidelines to promote a child safe culture when it comes to taking, sharing and storing images or videos of children in early childhood education and care.
The National Model Code and Guidelines are intended to support early childhood educators, as champions of child safety, and complement relevant child safety activities and strategies already in place across the early childhood education and care sector.



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)

Related Policies

Behaviour Guidance Policy CCS Data Security Policy CCS Personnel Policy CCS Governance Policy CCTV Policy Child Safe Environment Policy Child Safe and Wellbeing Policy Child Protection Policy Code of Conduct	Complaints and Grievances Policy Enrolment Policy Governance Policy Record Keeping and Retention Policy Privacy and Confidentiality Policy Personal Electronic Device Policy Social Media Policy Supervision Policy

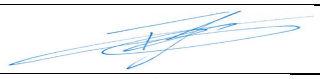
Sources

Australian Children's Education & Care Quality Authority. (2025). https://www.acecqa.gov.au/sites/default/files/2023-03/Guide-to-the-NQF-March-2023.pdf*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: 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.

Review History

Policy Reviewed By:	Tim Short	CEO	August 2025
POLICY REVIEWED	August 2025	NEXT REVIEW DATE	August 2027
Modifications	• New Policy, replacing Technology Policy (POLS00337)		
POLICY REVIEWED	PREVIOUS MODIFICATIONS		NEXT REVIEW DATE
	•		

Signed

CEO:	
Manager: