Technology and Device Use Policy

Quick reference: technology | device use | service-supplied devices | personal devices | screen time | digital learning | online safety | privacy | child safe environment | image use | social media | communication apps | online communication | administrative software | security | password protection | unapproved storage media | data security | unauthorised access | inappropriate content | software | cyber threats | cyber security | secure storage | National Model Code| AI | | child safety

PURPOSE AND BACKGROUND

(1) To outline our guidelines for managing technology and device use to ensure that we maintain a child safe environment, privacy is protected, and that technology is used safely and for educational and care purposes

(2) This policy helps us to comply with the *Education and Care Services National Law and Regulations*, which requires our service to have restrictions and controls for devices (*National Law* s 175), and policies and procedures in place for providing a child safe environment, including and matters relating to the safe use of digital technologies and online environments (*National Regulations* reg 168(2)(ha))

(3) It complies with the *Privacy Act 1988 (Cth),* and complies with the Victorian Statement of Regulatory Expectations – National Model Code (SRE-NMC), the ECEC Code of Ethics, and the Child Safe Standards

SCOPE

(4) This policy applies to:

- Staff': the approved provider, persons with management or control, nominated supervisor, paid workers, volunteers and work placement students, third parties who carry out work at our service that is relevant to this policy, including contractors, subcontractors, self-employed persons, employees of a labour hire company
- Children who are in our care, their parents, families and care providers
- Visitors to our service, including paid or unpaid third parties delivering programs or activities to children and allied health support workers
- Tertiary provider representatives assessing students on practicum at our service

(5) It covers the use of both service-supplied and personal devices on our premises and during any related off-site activities, such as excursions, regular outings and travel.

(6) The safe use of technology for taking, using, storing and destroying images or videos of children is also covered in our Photography and Video Policy

(7) Obtaining authorisation from parents to take, use and store images and videos of children is covered in our Photography and Video Policy, Social Media Policy and Authorisations Policy

(8) The safe use of CCTV covered by our CCTV Policy

(9) Staff must also adhere to our Child Safe Code of Conduct and Staff Code of Conduct when using technology

DEFINITIONS

(10) The following definitions apply to this policy and related procedures:

- 'Capture', in relation to an image of a child, includes to film, record or take and image of the child
- 'Devices' means any device capable of capturing, storing or transmitting images or videos. Examples include (but are not limited to): mobile phones, tablets, computers, cameras, smartwatches that can capture or store or transmit images, wearables (such as smart/camera glasses), smart toys, USB drives, memory cards, hard drives
- 'Excursion' means an outing organised by our service to and from a destination outside of our premises.
- 'Inappropriate conduct' is defined in the *National Law* as conduct in relation to a child that a reasonable person would consider inappropriate in an education and care service – including in relation to technology and device use
- 'Online' means connected to or available through the internet or a digital network, including websites, apps, social media platforms, email, cloud-based systems, and other digital technologies or platforms used for communication, learning or information sharing
- 'Personal devices' are devices owned or controlled by a person (not including a service-supplied device') and capable of capturing, storing or transmitting an image or video. For the purposes of this policy, personal devices also include any devices issued to students by their training provider
- 'Personal information' is defined in the *Privacy Act 1988* and includes any information about an identified individual such as their home address, email address, telephone number, date of birth, medical records, bank account details, and tax file number. Photos and videos are also treated as personal information
- 'Service-supplied devices' are devices supplied by the approved provider to be used by an authorised person exclusively for the purposes of providing education and care to children as part of our service. Service-supplied devices are configured to operate in accordance with this policy and procedure and any other policies and procedures related to child safety or the security of devices
- 'Technology' means any electronic device or digital platform used to access, store, or communicate information. This includes but is not limited to computers, laptops,

tablets, smartphones, smartwatches, cameras, televisions (including smart TVs), DVD players, and internet-enabled devices

- 'Unapproved storage media' refers to any storage devices not authorised by our service, such as USB drives, external hard drives, and non-approved cloud storage platforms
- 'Staff', unless otherwise indicated, refers to the approved provider, persons with management or control, nominated supervisor, paid workers, volunteers, students, and third parties who are covered in the scope of this policy. Note: 'staff', 'employees' and 'workers' etc may have their own, different definitions in legislation covered in this policy

POLICY STATEMENT

Safe use of digital technologies and online environments

(11) The approved provider must ensure that we have child safe systems in place for the use of digital technologies and online environments (*National Regulations* reg 168(2)(ha)), including in relation to:

a. The taking, use, storage and destruction of images and videos of children

b. The use of any optical surveillance device at the service

c. The use of any digital device issued by the service

d. The use of digital devices by children

(12) Our service complies with the *National Laws and Regulations* and the Victorian Statement of Regulatory Expectations - National Model Code to ensure that our use of digital technologies and online environments are respectful, child-centred and comply with our legal and ethical obligations for child safety

(13) The approved provider will ensure that regular child safety risk assessments are carried out for devices and digital and online environments, and that staff have appropriate training on digital and online safety [ACECQA has a guide online and digital technology risk assessments available to download]

(14) Technology and device procurement decisions will also be subject to child safety risk assessment to ensure that third-party providers, digital and online platforms and equipment meet child safe standards and do not introduce physical, digital or institutional risks to children (see Child Safe Procurement Policy)

(15) Staff must not use devices if doing so jeopardises their capacity to supervise, interact or engage with children

Using technology for education

(16) Technology is used to support the educational and operational goals of our service

(17) Experiences involving technology are limited and balanced with children's needs for physical, literacy, numeracy and social-emotional development

(18) Technology is used with intention and purpose, and as a tool to extend/enhance children's learning and development. It is not used as a substitute for direct educator-child interactions or to manage children's behaviour. For example, educators should not routinely use devices to tell stories, sing songs, placate children, answer questions that can be explored with the children without the use of the internet, or to teach children in place of in-person instruction

(19) Any digital content we use, such as music, videos, or educational software, is age-appropriate and aligns with our educational objectives

(20) Streaming content is allowed only from legal and reputable platforms (e.g., iTunes, YouTube Kids, ABC iView) and should be directly relevant to the children's learning or staff development

(21) We use child friendly search engines and apps that are enabled to block websites and inappropriate content. Chat functions are switched off on apps and games

(22) Photos and recordings of children are used (with parental consent) for planning and programming, such as documenting children's learning experiences, supporting reflective practices, and engaging families in their child's development

(23) Our service is guided by the Australian Government's recommendations for screentime for children aged 5-17 years – no more than two hours per day (not including schoolwork)

(24) Educators take into consideration the time children may also spend on the screen at home

(25) Educators teach children about safe and respectful use of technology, including not sharing personal information or inappropriate content online, avoiding online threats and being kind and polite in any digital interactions (cyber harassment/bullying), the risks of excessive use of devices and screentime, age-appropriate lessons about online grooming

(26) Educators constantly and actively supervise and engage with children who are using devices, and encourage children to speak up if they see or experience something online that makes them feel uncomfortable

Use of service-supplied devices

(27) Service-supplied devices may be used by staff used exclusively for the purposes of providing education and care to children in our care (*National Law* s 175B(1). For example, for:

- Documenting children's learning and activities
- Communicating with families about children's progress and daily activities
- Accessing educational resources and child development information
- Completing administrative tasks such as reporting and record-keeping
- Participating in professional development and training
- Authorised promotional and marketing purposes

- Internal communications
- Documenting incidents or child safety matters

(28) The approved provider must ensure that any service-supplied device is configured to operate in accordance with this policy and any other relevant policies and procedures for child safety or the security of devices (*National Law* s 175B(2))

(29) Personal devices will not be approved as service-supplied devices

(30) The approved provider and nominated supervisor must ensure that all inappropriate digital content (e.g., on websites, apps, videos) is blocked on service-supplied devices

(31) The use of the internet on service-supplied devices is permitted for accessing child-appropriate educational websites, professional development materials, and communication tools

(32) Access to social media platforms is restricted unless approved for service-related purposes (see our Social Media Policy)

(33) Only AI tools that have been formally approved by the approved provider or nominated supervisor may be used on service-supplied devices (see our AI Policy)

(34) Staff must not use any unapproved storage media to store or access content or data on service-supplied devices

(35) All service-supplied devices must be labelled with an identification code, distinctly branded and easily identifiable from a distance (*Victorian Statement Regulatory Expectation*)

(36) Shared devices will be allocated according to the educational needs, age group, and specific activities in each room, the frequency of use, the need for specific applications, and the ability to support learning objectives

(37) Where possible, our service provides dedicated devices in each room to ensure availability and accountability. Where sharing is necessary, room leaders will share according to a roster and service-supplied device use will be recorded and tracked

(38) Staff must not take any service-supplied devices home with them must not take any service-supplied devices home with them or off the premises unless they have the written authorisation of the approved provider. Before authorising a device to be taken off-site, the approved provider will undertake a documented risk assessment and put into place appropriate measures to protect children and families' personal information

(39) Students or their training providers and third-party professionals will need to seek the approved provider's written permission to use any service-supplied devices

Service-supplied devices record

(40) The approved provider will ensure a written record is kept for all service-supplied devices with information on how these devices are issued and returned

(41) The record will be kept in a safe and secure place at our premises for a minimum of three years from the date on which the record was made

Use of personal devices

(42) Personal devices must not be in the possession or control of any person while they are providing education and care and working directly with children unless the use of the personal device is:

- Is necessary to ensure children's safety, or to provide them with education and care, during children's excursions or transport by our service or arranged by our service; or
- Is in accordance with the advance written authorisation given by the approved provider where the approved provider is reasonably satisfied that the personal device is needed:
    - To provide support or assistance with the person's disability or health needs
    - To communicate with a family member of the person
    - For the safety or provision of education and care to children if a service-supplied device stops working
    - For use during an emergency, or
    - For work health and safety; or
- Would be considered necessary by a reasonable person for one of the authorised purposes listed above, in circumstances where it is not practicable for advanced authorisation to be given by the approved provider (e.g., in an emergency situation) (*National Law* ss 175H, 175I, 175J)

(43) Personal device rules and restrictions apply to:

- The approved provider
- Persons with management or control
- Nominated supervisors
- Educators and other paid staff
- Contractors
- Students and volunteers
- Tertiary provider representatives assessing students
- Paid or unpaid third-parties working directly with children (e.g., allied health workers, children's entertainers, contractors running incursions or programs, mentors or coaches, primary school teachers etc)
- Anyone employed, appointed or engaged to work in or as part of our service in any capacity

(44) The restrictions on personal devices do not apply to:

- Parents or carers (unless they are volunteering and working directly with children as part of our service)
- Third-party contractors who are attending the service but who are not providing education or care to children and not working directly with children (e.g., maintenance contractors, IT technicians)
- Victorian regulatory authority authorised officers, police or officers from other government regulatory authorities (e.g., environmental health officers)

(45) If a third-party professional needs to use a device for the purposes of providing education or care for a child or children as part of our service (e.g., where consent has been provided by the parent for a professional photographer to take photos, allied health professional to record notes or undertake an assessment etc), they may only use a device that is:

- Supplied by their business or institution, and
- Used only for work purposes (and not personal use); or
- A service-supplied device with the approved provider's written authorisation

(46) Staff may use personal devices during break-times, planning time or during administrative activities in non-childcare areas. At all other times, personal devices must be stored securely, away from children

(47) Staff must not use personal devices for multi-factor authentication to access and use 'Arrival' while providing education and care and working directly with children

(48) Staff may wear smart watches that do not have the capability to capture, transmit or store images.

(49) Educators must actively supervise any use of devices by children at all times to prevent them from high-risk behaviour online, such as uploading private information or images, engaging with inappropriate content, making in-app purchases or interacting with unsafe individuals

Record of authorisations for personal devices

(50) The approved provider must keep a written record of any authorisation granted for personal devices (*National Law* s 175J), including those granted retrospectively where advance authorisation is not practicable

(51) The written record must contain the following information (*National Regulations* reg 179A):

- The authorised person's name and role at the service
- The approved provider's name
- The name of the person who is making the written record
- A description of the personal device
- The purpose for which the personal device is being authorised

- The period of the authorisation

(52) Records of authorisations must be kept in a safe and secure place at our premises for a minimum of three years from the date on which the record was made (*National Law* ss 175J(3-4))

Capturing, storing or transmitting images and videos

(53) Everyone at our service must follow our Photography and Video Policy to ensure the rights and dignity of children are protected

(54) With few exceptions, only service-supplied devices – not personal devices - may be used to capture, store or transmit an image or video of any child while they are in our care

(55) Capturing, storing or transmitting an image or video of a child in our care with a personal device, in circumstances that are not permitted, is an offence and a serious breach of this policy. Doing so may result in disciplinary action and may be deemed as subjecting a child to inappropriate conduct, which is also an offence under the *National Law*

(56) We inform children, staff, families and visitors about our safe use of devices, and give them information about our rules for photographing and recording children at our service

(57) This section of the policy does not apply to optical surveillance devices (see below)

(58) For details, refer to our Photography and Video Policy

Optical surveillance devices

(59) Any use of optical surveillance devices (e.g., security cameras, webcams, live streaming, CCTV, baby monitors) must be in line with our relevant policies and procedures (e.g., CCTV Policy, Child Safe Environment Policy, Photography and Video Policy), privacy laws and any applicable workplace surveillance laws

(60) We must inform families, staff and visitors about why and where we have surveillance devices, in advance of any recording. We also place signs at all entrances and exits alerting people to the surveillance

(61) Surveillance data is kept secure, destroyed or de-identified when no longer needed, and access is limited to authorised personnel only

(62) Cameras are never placed in areas where people would usually expect privacy or in non-work areas (e.g., bathrooms, change rooms, staff rooms, private offices, breastfeeding rooms)

(63) Where optical surveillance devices are used, they must not be used as a replacement to physical checks or active supervision by staff

(64) Refer to our detailed CCTV Policy

Unacceptable use of service technology

(65) The following actions are strictly prohibited at our service:

- Using devices or other technology in any way that breaches our Child Safe Code of Conduct, including subjecting a child to inappropriate conduct, which is an offence
- Accessing systems, data or networks without authorisation
- Installing or using software without authorisation
- Misusing the service's equipment or resources
- Circumventing security measures
- Sharing passwords or login details
- Introducing viruses, malware or other malicious code
- Hacking or trying to gain unauthorised access to systems
- Spamming or sending out unsolicited mass emails
- Using the IT systems to harass, threaten or bully other users
- Sharing or creating inappropriate, discriminatory or offensive content
- Violating intellectual property (e.g., using pirated content or software)
- Using the service's network for illegal activities
- Disrupting or damaging our systems, networks, equipment or resources
- Uploading personal or sensitive information onto an AI tool
- Disclosing confidential information without authorisation

Data and system protections

(66) Personal information and other sensitive information is protected in line with our Privacy and Confidentiality Policy, the *Privacy Act 1988*, the *National Regulations* and relevant child protection laws

(67) Images and recordings of children are captured, shared, used, protected, stored and destroyed according to our Photography and Video Policy and with the written consent of parents

(68) All digital content and data are stored securely, and we take appropriate measures to prevent unauthorised access, loss, or misuse, including, for example:

- Password protection
- Limiting access to authorised staff
- Regular backups
- Storing service-supplied devices in locked cabinets or secure areas when not in use, and ensuring that personal devices are not left unattended in accessible areas

- Installing and regularly updating firewall and antivirus software on all service-supplied devices to protect against malware and cyber threats
- Regularly monitoring access logs and conducting audits to detect and address any unauthorised access or suspicious activity
- Educating staff on data security best practices, including identifying phishing attempts and other cybersecurity threats
- Encrypting devices where possible
- Software and written records to track who uses the devices and when

(69) All service-supplied devices are securely stored and accessed only by authorised staff

(70) Staff must not install unauthorised software or applications on service-supplied devices

(71) Any breaches of digital security protocols or data must be reported immediately to the nominated supervisor and approved provider

(72) In the event of a data breach involving service-supplied electronic devices or systems, immediate action will be taken to mitigate potential harm and protect the affected individuals' personal information. The approved provider/nominated supervisor follows our data breach response plan, contained in our Privacy and Confidentiality Policy

Oversight, control, and access to data

(73) The approved provider and nominated supervisor must take every reasonable precaution (*National Law* ss 175D, 175H) to ensure that:

- Only service-supplied devices are used to capture, store or transmit images or videos of children in our care, unless the use of another device is permitted in accordance with this policy and the law
- Persons who are working directly with children as part of our service do not have a personal device in their possession or under their control, unless they are authorised by the approved provider in accordance with this policy and the law

(74) The approved provider and nominated supervisor will ensure that there are processes and systems in place, and those processes and systems are followed to ensure that service-supplied devices are regularly reviewed to assess whether the devices are being used appropriately – that is, only for the purposes of, or in connection with, the provision of education and care to children, and in line with our policies and procedures

(75) The approved provider is responsible for:

- Making sure that staff access to digital and hardcopy files is being monitored, and for preventing the unauthorised movement of files onto non-approved devices or platforms

- Making sure that any images, videos, and content shared online is limited to its intended purpose (e.g., educational, promotional), and that inappropriate or unauthorised sharing does not occur
- Having processes in place to monitor the use of service-supplied devices and authorised personal devices, including registers and logs
- Ensuring that device and technology usage is covered in our service's risk assessments, including for emergencies, and the potential for loss, misuse, or technical failures
- Implementing device controls such as limiting app installations and disabling certain functionalities to prevent misuse
- Fostering a culture of vigilance and accountability, and encouraging staff to report any inappropriate device usage

(76) The nominated supervisor is responsible for overseeing the day-to-day use of devices, digital technology and online environments, monitoring staff compliance, ensuring that data and devices are securely managed, tracked and stored, and that we have appropriate and up-to-date authorisations

Breaches and complaints

(77) Anyone can raise concerns or complaints regarding the handling of technology or devices according to our Complaint Handling Policy

(78) Staff must follow our Child Protection Policy and Procedures if they have concerns for a child's safety or well-being, including for effectively identifying and responding where a child may be at risk of or are experiencing abuse or maltreatment through digital technologies and online environments

(79) Any breaches of this policy, including the improper use of devices, inappropriate conduct, or unauthorised use of technology, are treated seriously

(80) Depending on the nature of the breach, staff members may be subject to disciplinary action by our service and/or the regulatory authority, referred to the police/child protection authority, and/or have their employment terminated

PRINCIPLES

(81) The safety, rights, best-interests and well-being of children is our one number one priority

(82) We use technology and devices purposefully to enrich children's learning and development

(83) We maintain the privacy of children, families and staff members, and protect and store data and content securely, confidentiality and in line with our child safe obligations

(84) Our staff maintain high standards of professionalism in all interactions involving technology and devices

(85) Our use of technology and devices complies with all relevant laws, regulations and best practice guidelines, including the National Model Code

POLICY COMMUNICATION, TRAINING, AND MONITORING

(1) This policy and related documents can be found on our website and in our front office

(2) The approved provider and nominated supervisor provide information, training and other resources and support regarding our Technology and Device Use Policy and related documents

(3) All staff (including volunteers and students) are formally inducted. They are given access to, review, understand and acknowledge our Technology and Device Use Policy and related documents

(4) Each staff member engages in a professional development program, which covers this policy

(5) Roles and responsibilities are described in our Technology and Device Use Policy and in individual position descriptions. They are communicated during staff inductions and in ongoing training

(6) The approved provider and nominated supervisor monitor and audit staff practices and address non-compliance. Breaches to this policy are taken seriously and may result in disciplinary action against a staff member

(7) At enrolment, families are given access toour Technology and Device Use Policy and related documents

(8) Families are notified in line with our obligations under the *National Regulations* when changes are made to our policies and procedures

LEGISLATION (OVERVIEW)

Education and Care Services National Law and Regulations

Law	Description
s 165	Offence to inadequately supervise children
s 166A	Offence to subject a child to inappropriate conduct
s 167	Offence relating to protection of children from harm and hazards
s 175	Devices in education and care services
Regulations	
reg 73	Educational program
reg 74	Documenting of child assessments or evaluations for delivery of educational program
reg 168(h)	Education and care services must have policies and procedures in relation to providing a child safe environment, including matters relating to the promotion of a culture of child safety and wellbeing within the service
reg 168(ha)	Education and care services must have policies and procedures in relation to the safe use of digital technologies and online environments at the service
reg 170	Policies and procedures to be followed
reg 171	Policies and procedures to be kept available
reg 177(1)(a)	Prescribed enrolment and other documents to be kept by approved provider

reg 179A	Prescribed information to be kept in written record of authorisation to possess or control personal device
regs 181,183 - 184	Confidentiality and storage of records

Other applicable laws and regulations

Act/ Regulation	Description
Australian Human Rights Commission Act 1986 (Cth)	Provides guidance on how to uphold the principles in the Convention on the Rights of the Child
Privacy Act 1988	Principal act protecting the handling of personal information
State/territory-based child protection and child safety laws	Covers child safety for organisations and reporting obligations
Victorian Statement of Regulatory Expectations – National Model Code (SRE-NMC)	Guidelines for implementing the National Model Code in Victoria

National Quality Standard

Standard / Element	Concept	Description
1.1.1	Approved learning framework	Curriculum decision-making contributes to each child's learning and development outcomes in relation to their identity, connection with community, wellbeing, confidence as learners and effectiveness as communicators
1.2	Practice	Educators facilitate and extend each child's learning and development
1.3	Assessment and planning	Educators and co-ordinators take a planned and reflective approach to implementing the program for each child
1.3.1	Assessment and planning cycle	Each child's learning and development is assessed or evaluated as part of an ongoing cycle of observation, analysing learning, documentation, planning, implementation and reflection
1.3.2	Critical reflection	Critical reflection on children's learning and development, both as individuals and in groups, drives program planning and implementation
1.3.3	Information for families	Families are informed about the program and their child's progress
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 hazards
2.2.3	Child Protection	Management, educators and staff are aware of their roles and responsibilities regarding child safety, incluidng the need to identify and respond to every child at risk of abuse or neglect
4.2.2	Professional standards	Professional standards guide practice, interactions and relationships
7.1.2	Management systems	Systems are in place to manage risk and enable the effective management and operation of a quality service that is child safe

My Place, Our Time (MTOP) V2.0 / Victorian Early Years Learning and Development Framework

Outcome	Key component

1: CHILDREN AND YOUNG PEOPLE HAVE A STRONG SENSE OF IDENTITY	• Children and young people learn to interact in relation to others with care, empathy and respect
3: CHILDREN AND YOUNG PEOPLE HAVE A STRONG SENSE OF WELLBEING	• Children and young people become strong in their social, emotional and mental wellbeing • Children and young people are aware of and develop strategies to support their own mental and physical health, and personal safety
4. CHILDREN AND YOUNG PEOPLE ARE CONFIDENT AND INVOLVED LEARNERS	• Children and young people develop a range of learning and thinking skills and processes such as problem solving, inquiry, experimentation, hypothesising, researching and investigating • Children and young people resource their own learning through connecting with people, place, technologies and natural processed materials
5: CHILDREN AND YOUNG PEOPLE ARE EFFECTIVE COMMUNICATORS	• Children and young people collaborate with others, express ideas and make meaning using a range of digital technologies and media and communication technologies

National Principles for Child Safe Organisations

Most relevant principles
Children and young people are informed about their rights, participate in decisions affecting them and are taken seriously
Equity is upheld and diverse needs respected in policy and practice
Staff and volunteers are equipped with the knowledge, skills and awareness to keep children and young people safe through ongoing education and training
Physical and online environments promote safety and wellbeing while minimising the opportunity for children and young people to be harmed

SOURCES

Education and Care Services National Law and Regulations | National Quality Standard | National Principles for Child Safe Organisations | Child Safe Standards | Victorian Statement of Regulatory Expectations – National Model Code (SRE-NMC) |National Model Code for Taking Images or Videos of Children while Providing Early Childhood Education and Care | Australian Privacy Principles (Privacy Act 1988) | eSafety Commissioner Resources | ACECQA's NQF Online Safety Guide | ACECQA's NQF Child Safe Culture Guide | Early Childhood Australia Code of Ethics | Australian Government Information Security Manual (ISM) | Australian Signals Directorate guidance on device and data security | ACECQA's Safe Use of Digital Technologies and Online Environments Policy and Procedure Guidelines | Victorian Government guidelines for child safe practices for digital technologies and personal electronic devices

RELATED DOCUMENTS

Key Policies	Child Safe Environment Policy | Complaint Handling Policy | Child Safe Risk Management Plan | ECEC Code of Ethics | Staffing Arrangements Policy | Governance Policy | Educator and Management Policy | Privacy and Confidentiality Policy | Child Safe Code of Conduct | Recruitment, Induction, Training and WWCC | Photography and Video Policy | Social Media Policy | CCTV Policy | AI Policy | Child Safe Procurement Policy
Procedures	Roles and responsibilities – technology and device use (attached) | Child safety related procedures

Resources	Shared service-supplied device log template (attached)| Supply of service-supplied device record template (attached) | Personal device authorisation record template (attached))| Summary version of Technology and Device Use Policy for staff (attached)

POLICY INFORMATION

Approval	Dina Kahn
Review	Reviewed annually and when there are changes that may affect this policy or related procedures. The review will include checks to ensure the document reflects current legislation, continues to be effective, or whether any changes and additional training are required **Last reviewed: 25th March 2026 Date for next review: 25th March 2027**

APPENDIX A

ROLES AND RESPONSIBILITIES – Technology and device use

Approved provider responsibilities (not limited to)
Ensure our service meets its obligations under the *Education and Care Services National Law* and *Regulations*, including as they relate to devices, and other digital technologies and online environments. Take every reasonable precaution to protect children from harm and hazards likely to cause injury and ensure that children in our care are adequately supervised at all times
Ensure that our service's governance, management, operations, policies, plans, (including risk management/action plans), systems, practices and procedures for technology and device use are appropriate in practice, best practice, align with the Child Safe Standards / National Principles for Child Safe Organisations, the National Model Code and comply with all other relevant legislation, including privacy laws
Ensure this Technology and Device Use Policy and related procedures are in place and available for inspection
Take reasonable steps to ensure this Technology and Device Use Policy is followed (e.g. through clear and accessible communication, and systemised inductions, resourcing, training and monitoring of all staff – including volunteers, students)
Provide staff with the necessary resources, such as service-supplied devices and secure data storage solutions
Organise and facilitate regular training sessions for all staff members on the appropriate use of technology, data security, and privacy policies. Ensure that staff are updated on any changes to relevant laws or service policies
Establish and maintain systems for monitoring and reviewing compliance with this policy. This includes periodic audits, spot checks, written records and reviews of digital content and device usage
Handle incidents of non-compliance, including conducting investigations and taking appropriate disciplinary action. This includes reporting any illegal activities to the relevant authorities, such as the police or child protection services
Ensure this policy and related documents are reviewed regularly in consultation with staff and families. Notify families of reviews and changes according to legislation and our policies and procedures
Use service-supplied devices solely for work-related tasks, and do not have personal devices in your possession or control while you are working directly with children (unless otherwise authorised for an approved reason). Ensure the same for the nominated supervisor, relevant staff, visitors, students and volunteers
Ensure images and videos of children are only captured, stored, or transmitted with a service-supplied device (not a personal device), and only for an approved purpose and in line with our Photography and Video Policy. Ensure the same for the nominated supervisor, relevant staff, visitors, students and volunteers
Ensure that service-supplied devices are configured to operate in accordance with our Technology and Device Use Policy, Photography and Video Policy, child safety policies and procedures and any other relevant policy or procedure
Ensure the written records of the supply of service-supplied devices and any authorisation for personal devices are kept in accordance with this policy

Nominated supervisor / persons in day-to-day charge responsibilities (not limited to)
Ensure our service meets its obligations under the *Education and Care Services National Law* and *Regulations,* including as they relate to devices, and other digital technologies and online environments. Take every reasonable precaution to protect children from harm and hazards likely to cause injury, and ensure that children in our care are adequately supervised at all times
Support the approved provider to ensure that our service's management, operations, policies, plans, (including risk management/action plans), systems, practices and procedures for technology and device use are appropriate in practice, best practice, align with the Child Safe Standards / National Principles for Child Safe Organisations, the National Model Code and comply with all other relevant legislation, including privacy laws
Take reasonable steps to ensure this Technology and Device Use Policy is followed (e.g. through clear and accessible communication, and systemised inductions, resourcing, training and monitoring of all staff – including volunteers, students)
Ensure that daily operations adhere to the Technology and Device Use Policy. This includes monitoring the use of service-supplied and personal devices by staff
Provide guidance to staff on acceptable and unacceptable technology use. Address any questions or concerns related to the policy and offer support in implementing it
Document and report any breaches of the policy to the approved provider
Act promptly to address any instances of non-compliance. This includes confiscating devices used inappropriately, issuing warnings, and escalating issues to the approved provider, police or child protection services if necessary
Inform families about our service's technology and device use policies and how they can access related documents. Communicate any significant updates to the policy that may affect their child's experience at the service
Use service-supplied devices solely for work-related tasks and do not have personal devices in your possession or control while you are working directly with children (unless otherwise authorised for an approved reason). Ensure the same for relevant staff, visitors, students and volunteers
Ensure images and videos of children are only captured, stored, and transmitted with a service-supplied device (not a personal device), and only for an approved purpose and in line with our Photography and Video Policy. Ensure the same for other relevant staff, visitors, students and volunteers
Support the approved provider to ensure the written records of the supply of service-supplied devices and any authorisation for personal devices are kept in accordance with this policy
Establish and maintain systems for monitoring and reviewing compliance with this policy. This includes periodic audits, spot checks, written logs and registers, and reviews of digital content and device usage

Educators / other staff responsibilities (not limited to)
Follow this Technology and Device Use Policy and other related child safety policies and documents, including:

- Using service-supplied devices solely for work-related tasks
- Not having personal devices in your possession or control while you are working with children (unless otherwise authorised by the approved provider for an approved reason)
- Only capturing, storing or transmitting images or videos of children with a service-supplied device, and only for an approved purpose and in line with our Photography and Video Policy
- Maintaining accurate logs and records in relation to device use

Maintain a high standard of professionalism in all digital interactions. Ensure that any digital content created or shared is appropriate, educational, and aligns with our service's curriculum, policies and codes, including our Child Safe Code of Conduct, Never subject a child to inappropriate conduct

Prioritise the safety and privacy of children at all times. This includes obtaining written consent before capturing or sharing images and videos of children and ensuring that all digital content is securely stored

Immediately report any breaches of the policy to the nominated supervisor or approved provider (or police or child protection services if necessary). Cooperate fully with any investigations into incidents of non-compliance or misuse of technology

Participate in ongoing training and professional development related to technology use, data security, and child protection. Stay informed about updates to the policy and relevant legislation

Families and visitors' responsibilities (not limited to):
Follow our rules about personal devices and photography and videos
Report any concerns you have about staff, families or visitors use of devices or any possible breaches to our Photography and Video Policy

APPENDIX B

TEMPLATE – Shared devices log (sign-in/sign-out log)

[This template is optional - some services track shared devices electronically. It can be customised to fit the specific needs of your service and should be maintained regularly to ensure accurate tracking of shared devices and accountability]. . It is separate to the approved provider's record of service-supplied devices at Appendix C]

Device ID	Device Description	Staff Name and Role	Purpose of Use	Time & Date taken	Return Time & Date returned	Condition on Return	Remarks
001	*iPad Pro 11"*	*Zaim Sainsbury (Educator)*	*Capturing Learning*	*9:00am 01/08/25*	*1:10pm - 01/08/20242025*	*Good*	
002	*Samsung Galaxy Tab*	*Jo Rodriguez (Nominated supervisor)*	*Administrative Use*	*9:40am 02/08/25*			*Not yet returned*
003	*Nikon D3500 Camera*	*Amina Al-Hassan (Educator)*	*Documenting Activities*	*1:30pm 03/08/2025*	*2:30pm 03/08/20254*	*Minor scratches*	

Additional Notes

- Ensure all staff members authorised to use service-supplied devices understand our rules and their responsibilities for device use
- Devices must be configured according to the Technology and Device Use Policy, including secured with passwords and other necessary security measures to protect sensitive information

- Any incidents, such as misuse, loss or damage, should be reported to the nominated supervisor/approved provider

APPENDIX C

RESOURCE – Service-supplied device record template

Date of supply:	_____/_____/_____
Type of device supplied:	☐ Mobile phone ☐ Tablet ☐ Laptop ☐ Camera ☐ Other (specify):_____
Device details:	Make: _____ Model: _____ Serial number (if available): _____ Device ID: _____
Declaration of configuration	I confirm that this device has been configured in accordance with the service's policies and procedures relating to: ☐ Child safety ☐ Digital security and data protection ☐ Photography and video use ☐ Technology and device use ☐ Privacy and confidentiality Approved provider / authorised delegate name: _____ Signature: _____ Date: _____/_____/_____
Staff member receiving device	Name: _____ Position: _____ Signature: _____ Date: _____/_____/_____ Shared device? ☐ No ☐ Yes – details (e.g., room, tracking, security): _____ _____
Record of revocation (if	Date of revocation: _____/_____/_____

applicable)	Reason for revocation: _____ Approved provider / authorised delegate name: _____ Signature: _____

This record must be stored securely at the service premises for a minimum of three years from the date of supply or revocation, in accordance with the *Education and Care Services National Regulations* and service policies

APPENDIX D

RESOURCE – Personal device authorisation record template

Name and address of service	<Insert name and address>
Person to whom the authorisation is granted	
Full name:	
Residential address	
Date of birth	Date: _____/_____/_____
Role/relationship to service *(e.g., educator, volunteer, allied health practitioner)*	
Details of the authorisation	
Reason for authorisation	☐ To provide support or assistance with the person's disability or health needs ☐ To communicate with the person's family member ☐ For the safety or provision of education or care because a service-supplied device has stopped working ☐ For an emergency ☐ For work health and safety Provide details_____
Scope of authorisation *(e.g., permitted times, locations, restrictions)*	

Device type *(e.g, iphone, Samsung phone, smartwatch)*	
Period of authorisation	Start: ____ / ____ / _____ End: ____ / ____ / _____
Review	Three-month review date (If still in effect after 3 months the approved provider must review to check reason for authorisation is still valid) ____ / ____ / _____ Review outcome ☐ Authorisation still required ☐ Authorisation no longer required Notes:_____
Revocation details (if applicable)	Date authorisation was revoked ____ / ____ / _____ *(Must be revoked in writing within 48 hours if no longer required)* Reason for revocation_____
Conditions	The person being authorised acknowledges and agrees to the following conditions: 1. The personal device will only be used for the authorised purpose described above 2. The device must not be used to capture, store, or transmit photographs or videos of any child at our service, except in an emergency or urgent situation where it is necessary to ensure the safety, health or wellbeing of a child 3. If an emergency requires the device to be used to capture, store or transmit an image or video, the person must: • Use it only to the extent necessary • Transfer the images or videos to a service-supplied device as soon as practicable • Immediately delete the images or videos from their personal device once the transfer is complete 4. The device must remain securely stored when not in use for the authorised purpose 5. The person must comply with all policies and procedures, including the Technology and Device Use Policy, Child Safe Environment Policy, Photography and Video Policy, and any lawful direction from the approved provider or nominated supervisor 6. The authorised person must immediately report any loss, theft, access, misuse or breach relating to the device 7. The authorised person must notify the approved provider as soon as practicable if the device is no longer required for the authorised purpose 8. The approved provider must revoke this authorisation if the original reason is no longer valid or if the device is being used contra to these conditions or in any way that risks the safety, privacy or wellbeing of children

Declaration by person being authorised	I declare that the information I have provided is true and correct. I understand the conditions of use and agree to comply with all requirements listed above **Signature: _____** **Name: _____ Date: ____ / ____ / _____**
Declaration by approved provider	I declare that: • I am satisfied that the personal device is necessary for the stated purpose • The stated purpose is one that is provided for under the *National Law* • Appropriate conditions are in place to manage risks to children's safety, privacy and wellbeing. I authorise the person named above to use their personal device strictly in accordance with this declaration. **Signature: _____** **Name: _____ Date: ____ / ____ / _____**

This record must be stored securely at the service premises for a minimum of three years from the date of authorisation or revocation, in accordance with the *Education and Care Services National Regulations* and service policies

APPENDIX E

RESOURCE – Quick guide version of our Technology and Device Use Policy for staff

[This an optional summary of our Technology and Device Use for staff. You can use it as a handout or to display]

Using technology safely and responsibly

- Use technology only for educational and work-related purposes
- Keep children's best interests, safety, privacy, and wellbeing at the centre of all technology use
- Comply with our Child Safe Code of Conduct, Staff Code of Conduct and Privacy and Confidentiality Policy
- Use only service-supplied devices to capture, transmit, use or store images or videos of children — never use personal devices
- Follow our Photography and Video Policy, Social Media Policy, and AI Policy (if applicable)

Service-supplied devices

- Must only be used for educational or work-related purposes
- Do not take service-supplied devices home (unless otherwise authorised)
- Store all devices securely when not in use

- Do not install unauthorised apps or software
- Treat devices carefully
- Use our device tracking logs/registers to record your use of service-supplied devices
- Third-party professionals (e.g., allied health professionals, professional photographers, entertainers etc) must only use devices issued by their business or institution or a service-supplied device with the approved provider's written authorisation

Personal devices

- Keep personal devices (e.g., phones, tablets, smart glasses, smartwatches, smart toys, digital cameras and USBs) off your person and not in your control while working directly with children. Store them securely
- You may use personal devices on breaks, in non-child areas
- If you have to use your personal device while you are working with children for an approved reason (e.g., disability or health need, work health and safety, to communicate with a family member), you need to get the approved provider's written authorisation first
- You can wear a smartwatch, but only if but only if it can't capture, store or transmit images
- Never use personal devices to capture, share or store photos, videos, or information about children
- If you use your personal device in an emergency situation, notify the nominated supervisor and approved provider as soon as possible
- Contractors, volunteers, students and third-party professionals must also follow our rules about personal devices

Technology use with children

- Technology must support children's learning — not replace educator interaction
- Actively supervise all device use
- Follow age-based screen time limits
- Teach and model safe, respectful technology habits
- Only use approved digital learning apps with parental consent

Unacceptable use

- No use of technology to bully, harass or breach privacy
- No access to inappropriate content or use of unauthorised storage (e.g. USBs, unapproved cloud)
- No unauthorised sharing of images, videos, or sensitive data
- No uploading of personal information of anyone at our service to AI tools
- No use that breaches our Child Safe Code of Conduct, including subjecting a child to inappropriate conduct

Protecting data and privacy

- Store all digital content securely (passwords, encrypted storage, access limits)
- Do not access or use personal information about children, families or other staff members unless you are authorised
- Report any data breaches, inappropriate content or policy breaches immediately
- Do not share login/passwords or allow unauthorised access to systems

Staff responsibilities

- Follow our Technology and Device Use Policy at all times
- Participate in training and policy updates
- Keep informed about acceptable use, privacy, and digital and online safety
- Report any breaches to this Policy or our Child Safe Code of Conduct, misuse or safety concerns to the nominated supervisor or approved provider

Our full Technology and Device Use Policy is available <insert location>