Bacchus Marsh Grammar

ELC POLICY

Early Learning Centre

Technology and Device Use Policy

Approved by the Approved Provider: 26 August 2025

Bacchus Marsh Grammar PO Box 214 Bacchus Marsh VIC 3340 **E** school@bmg.vic.edu.au
Maddingley Campus South Maddingley Road, Bacchus Marsh VIC 3340 **P** 03 5366 4800
Woodlea Campus and ELC 111 Frontier Avenue, Aintree VIC 3336 **P** 03 5366 4900

An Independant Ecumenical School for Girls and Boys
Reg. No. 1919
ABN: 24 128 531 078
www.bmg.vic.edu.au

Technology and Device Use Policy

1 Quick reference:

technology | device use | service-issued 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

2 Purpose and Background

2.1.1 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 purposes

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

2.1.3 It complies with the Privacy Act 1988 (Cth), and aligns with the National Model Code for Taking Images or Videos of Children while Providing Early Childhood Education and Care (National Model Code), the ECEC Code of Ethics, and the Child Safe Standards/National principles for Child Safe Organsiations

3 Scope

3.1.1 This policy applies to:

- The approved provider, paid workers, volunteers and work placement students, **referred to as 'staff' throughout this policy**
- Third parties who carry out child-related work at our service, including contractors, subcontractors, self-employed persons, employees of a labour hire company, **referred to as 'staff' throughout this policy**
- Children who are in our care, their parents, families and care providers
- Visitors to our service who carry out child-related work, including allied health support workers

3.1.2 It covers both personal and professional use of social media, particularly when referencing our service or our service's activities, staff, children and families

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

3.1.4 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

3.1.5 The safe use of CCTV covered by our CCTV Policy

3.1.6 The safe use of AI is covered in our AI Policy

3.1.7 Staff must also adhere to our Child Safe Code of Conduct and Staff Code of Conduct when using technology

4 Definitions

4.1.1 The following definitions apply to this policy and related procedures:

• '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 privately owned devices (such as smartphones, tablets, laptops, voice recorders, cameras, smart toys and smartwatches) capable of accessing the internet or capturing images and videos. For the purposes of this policy, personal devices also includes 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-issued devices’ are devices provided by our service for professional use, including phones, tablets, cameras, and computers

• ‘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, 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

5 Policy Statement

5.1 Safe use of digital technologies and online environments

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

- The taking, use, storage and destruction of images and videos of children
- The use of any optical surveillance device at the service
- The use of any digital device issued by the service
- The use of digital devices by children

5.1.2 Our service follows the 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

5.1.3 The approved provider will ensure that regular risk assessments are carried out for our digital and online environments, and that staff have training on online safety

5.2 Using Technology for Education

5.2.1 Technology is used to support the educational and operational goals of our service

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

5.2.3 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 electronic 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

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

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

5.2.6 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

5.2.7 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

5.2.8 Our service is guided by the Australian Government’s recommendations for screentime for children:

- from birth to 2 years - zero time per day (very short viewings for educational purposes is okay)
- 2-5 years - no more than one hour per day

- 5-17 years – no more than two hours per day (not including schoolwork)

5.2.9 Educators take into consideration the time children may also spend watching screen content at home

5.2.10 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

5.2.11 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

5.2.12 Educators who use AI tools for educational purposes must follow our AI Policy

5.3 Digital learning and communication apps [e.g.,Xplor]

5.3.1 Our service uses digital learning and communication apps to:

- Communicate with parents and amongst staff
- Manage attendance, invoicing, and other administrative tasks

5.3.2 We only use apps that have strong privacy and security features

5.3.3 The apps are monitored by staff to make sure that all content is appropriate

5.3.4 Our digital learning and communication apps may have integrated AI to support educators to document, communicate and reflect on children's learning and development (see our AI Policy for how we ensure children's privacy and safety is protected)

5.3.5 We get written consent from parents before we share information about their child on these apps. Parents can opt out of using the app or specific features at any time by notifying the nominated supervisor in writing

5.3.6 We will only share photos/videos of children on these apps if we have written consent to do so from parents (see Photography and Video Policy)

5.3.7 The apps are monitored by staff to make sure that all content is appropriate

5.3.8 Staff using private social media groups (e.g., , Facebook) or video conferencing platforms (e.g. MS Teams, Google Meet, Zoom) must ensure that personal and confidential information is handled according to our usual practices, and in line with our policies, including our Privacy and Confidentiality Policy

5.3.9 The nominated supervisor manages the day-to-day use of the apps, ensuring that software and security is kept up-to-date and that the apps are being used appropriately

5.4 Use of Service-issued Devices

5.4.1 Service-issued devices are used solely for work-related tasks, such as:

- 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

5.4.2 Only service-issued devices can be used for taking images or videos of children in our care

5.4.3 Personal electronic devices will not be approved as service-issued devices

5.4.4 The nominated supervisor/BMG ICT must ensure that all inappropriate digital content (e.g., websites, apps, videos) are blocked on service-issued devices

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

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

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

5.4.8 Staff must not use any unapproved storage media to store or access content or data on service devices

5.4.9 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

5.4.10 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

5.4.11 Shared devices should be handled with care, wiped clean after use, properly maintained by the staff using them and stored in our secure storage cabinet/ admin office when they are not in use and at the end of every day

5.4.12 Staff must not take any service-issued devices home with them

5.4.13 Staff may only take, use, store images, videos and audio recordings of children on our service devices (not their personal devices), and only with the appropriate parental authorisation (refer to Photography and Video Policy)

5.4.14 Students or their training providers will need to seek the nominated supervisor's permission to use any service issued devices

Use of Personal Devices – staff and children

5.4.15 Our service has adopted the voluntary National Model Code to ensure the safe use of personal electronic devices

5.4.16 By law in Victoria, staff (including students and volunteers) must not have personal devices capable of taking images or videos (such as smartphones, tablets, and smartwatches) and personal storage and file transfer media (such as SD cards, USB drives, and cloud storage) on their person while they are with children [Legal restrictions on the use of personal electronic devices are expected to take effect in Victoria on 26 September 2025]

5.4.17 Exceptions may be granted for limited, essential purposes authorised in writing by the approved provider, provided they do not interfere with the active supervision of children

5.4.18 Personal devices may be authorised for use in specific essential situations, including:

- Communication during emergencies involving a lost child, injury, serious incident, or lockdown
- Personal health monitoring, such as for heart or blood sugar levels
- Essential communication for individuals with disabilities
- Family emergencies, such as communicating with an ill or dying family member
- Technology failures, when service-issued devices are temporarily unavailable
- Receiving emergency notifications, such as bushfire evacuation alerts

5.4.19 Staff may use personal devices during break-times in non-childcare areas. At all other times, personal devices must be stored securely, away from children

5.4.20 If a staff member has approval to use a personal device, they must not use it to take photographs, videos or record audio of children in our care

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

5.4.22 If a personal device is used to take photographs, audio or videos in an emergency, any images or videos must be transferred as soon as practicable to a service-issued device or platform, and the content must be deleted from the personal device

5.4.23 Staff must report any accidental or necessary use of a personal device for photography or recording to the nominated supervisor immediately

5.4.24 Taking an unauthorised photograph or video of a child in our care with a personal device is considered a serious breach of this policy and may result in disciplinary action

5.4.25 Unless otherwise approved by the approved provider for an essential purpose, children should not bring any personal devices to the service

5.4.26 Educators must supervise any use of devices by children at all times

6 Optical surveillance devices

6.1.1 Any use of optical surveillance devices (e.g., security cameras, webcams, live streaming, CCTV,)must be in line with privacy laws and any applicable workplace surveillance laws

6.1.2 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

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

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

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

6.1.6 Refer also to our detailed CCTV Policy

6.2 Unacceptable Use of Service Technology

6.2.1 The following actions are strictly prohibited at our service:

•Using technology in any way that breaches our Child Safe Code of Conduct

- 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

6.3 Data and system protections

6.3.1 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

6.3.2 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

6.3.3 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-issued 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-issued 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

6.3.4 The approved provider/nominated supervisor maintains a log detailing the issuance of each electronic device, including the device's unique identification (serial number), the room it is assigned to, the date of issuance, and the purpose for which it is issued [Digital devices log template at Appendix A or services can use tracking software]

6.3.5 All service-issued devices are securely stored and accessed only by authorised staff

6.3.6 Staff must not install unauthorised software or applications on service-issued devices

6.3.7 Any breaches of digital security protocols or data must be reported immediately to the nominated supervisor/approved provider

6.3.8 In the event of a data breach involving service-issued 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

6.3.9 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-issued devices
- 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

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

6.4 Breaches and Complaints

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

6.4.2 Staff must follow our Child Protection Policy and Procedures if they have concerns for a child's safety or well-being

6.4.3 Any breaches of this policy, including the improper use of devices, or unauthorised use of technology, are treated seriously

6.4.4 Depending on the nature of the breach, staff members may be subject to disciplinary action, referred to the police/child protection authority, and/or have their employment terminated

7 Principles

7.1.1 The safety and well-being of children is our one number one priority

7.1.2 We use technology and devices purposefully to enrich children's learning and development

7.1.3 We maintain the privacy of children, families and staff members, and protect and store data and content securely and confidentiality

7.1.4 Our staff maintain high standards of professionalism in all interactions involving technology and devices

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

8 Policy, Communication, Training and Monitoring

8.1.1 This policy and related documents can be found in our Policy Folder and OneDrive Policy folder

8.1.2 The approved provider and nominated supervisor provide information, training and other resources and support regarding the Social Media Policy and related documents

8.1.3 All staff (including volunteers and students) are formally inducted. They are given copies of/access to, review, understand and formally acknowledge this Technology and Device Use Policy and related documents

8.1.4 Each staff member engages in a professional development program, which covers this policy

8.1.5 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

8.1.6 The approved provider and nominated supervisor monitor and audit staff practices e.g. through spot checks, performance reviews, supervision sessions, compliance visits from operations managers, spot checks from area managers, regular performance appraisal) and address non-compliance. Breaches to this policy are taken seriously and may result in disciplinary action against a staff member

9 Legislation Overview

9.1 Education and Care Services National Law and Regulations

Law	Description
s 165	Offence to inadequately supervise children
s 167	Offence relating to protection of children from harm and hazards
Regulations	
s 73	Educational program
s 74	Documenting of child assessments or evaluations for delivery of educational program
s 168(2)(h)	Education and care services must have policies and procedures in relation to providing a child-safe environment
s 170	Policies and procedures to be followed
s 171	Policies and procedures to be kept available
s 177(1)(a)	Prescribed enrolment and other documents to be kept by approved provider
ss 181,183 - 184	Confidentiality and storage of records

9.2 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, including photos and videos

9.3 National Quality Standard

Standard	Concept	Description
1.1	Program	The educational program enhances each child's learning and development
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
1.1.3	Program Learning Opportunities	All aspects of the program, including routines, are organised in ways that maximise opportunities for each child's learning
1.2	Practice	Educators facilitate and extend each child's learning and development
1.2.1	Intentional teaching	Educators are deliberate, purposeful and thoughtful in their decisions and actions
2.1	Health	Each child's health and physical activity is supported and promoted
2.1.3	Healthy lifestyle	Healthy eating and physical activity are promoted and appropriate for each child
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
3.1	Physical environment	The design of the facilities is appropriate for the operation of a service
3.1.2	Upkeep	Premises, furniture, and equipment are safe, clean, and well maintained
3.2	Use	The service environment is inclusive, promotes competence and supports exploration and play-based learning
3.2.2	Resources support play-based learning	Resources, materials and equipment allow for multiple uses, are sufficient in number, and enable every child to engage in play-based learning.
4.2	Professionalism	Management, educators and staff are collaborative, respectful and ethical
4.2.2	Professional standards	Professional standards guide practice, interactions and relationships
5.1	Relationships between educators and children	Respectful and equitable relationships are maintained with each child
5.1.1	Positive educator to child interactions	Responsible and meaningful interactions build trusting relationships which engage and support each child to feel secure, confident and included
5.1.2	Dignity and rights of the child	The dignity and rights of every child is maintained
5.2	Relationships between children	Each child is supported to build and maintain sensitive and responsive relationships

6.1	Supportive relationships with families	Respectful relationships with families are developed and maintained and families are supported in their parenting role
7.1	Governance	Governance supports the operation of a quality service
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
7.1.3	Roles and responsibilities	Roles and responsibilities are clearly defined, and understood, and support effective decision-making and operation of the service
7.2	Leadership	Effective leadership builds and promotes a positive organisational culture and professional learning community
7.2.3	Development of professionals	Educators, co-ordinators and staff members' performance is regularly evaluated, and individual plans are in place to support learning and development

9.4 Early Years Learning Framework (EYLF) v2.0 / Victorian Early Years Learning and Development

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

9.5 National Principles for Child Safe Organisations

Most relevant principles
Child safety and wellbeing is embedded in organisational leadership, governance and culture
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.

10 Sources

Education and Care Services National Law and Regulations | National Quality Standard | National Principles for Child Safe Organisations | 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

11 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
Procedures	Roles and responsibilities – technology and device use (attached) | Child safety related procedures
Resources	Digital device log template (attached)| Summary version of Technology and Device Use Policy for staff (attached) | Consent form for digital learning and communication apps | [Centre Support resources available on Karla Resources at centresupport.com.au

12 Authorisation

ELC Document Name	**Technology and Device Use Policy**	
Name of Reviewer: Approved Provider	**CEO Andrew Neal**	**Signature:**
Name of Reviewer: Nominated Supervisor	**Kerry Osborn**	**Signature**:
Date Revised	**August 2025** Reviewed annually and when there are changes that may affect child safety, including after any responses to incidents, disclosures or suspicions of harm or risk of harm. 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	

13 History

Date	Amendment
September 2024	New policy to replace the Technology Usage Policy
April 2025	Reviewed - No changes
August 2025	Updates in response to the amended National Regulations commencing 1 Set 2025 and 1 Jan 2026

14 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 to 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 National Principles for Child Safe Organisations, the National Model Code and comply with all other relevant legislation, including privacy laws
Ensure the Technology and Device Use Policy is effectively implemented across all aspects of our service. This includes providing necessary resources, such as service-issued 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 compliance with this policy. This includes periodic audits, spot checks, 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

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 to 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 National Principles for Child Safe Organisations, the National Model Code and comply with all other relevant legislation, including privacy laws
Ensure that daily operations adhere to the Technology and Device Use Policy. This includes monitoring the use of service-issued 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

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-issued devices solely for work-related tasks and not having personal electronic devices in your possession while you are with children
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
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

15 Appendix B: Resource – Summary version of our Technology and Device Use Policy for Staff

Using technology safely and responsibly

- Use technology only for educational and work-related purposes
- Keep children's 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-issued devices to take, use and store photos, videos or audio of children — never use personal devices
- Follow our Photography and Video Policy, Social Media Policy, and AI Policy (if applicable)

Service-issued devices

- Must only be used for educational or work-related purposes
- Do not take service-issued devices home
- Store all devices securely when not in use
- Do not install unauthorised apps or software
- Treat devices carefully

Personal devices

- Keep personal devices (e.g., phones, tablets, smartwatches, digital cameras and USBs) off your person while working with children. Store them securely
- You may use personal devices on break, in non-child areas
- Any approved use (e.g. emergencies) must be logged and the relevant content deleted immediately after transfer to a service device
- Never use personal devices to capture, share or store photos, videos, or information about children

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

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 this policy at all times
- Participate in training and policy updates
- Keep informed about acceptable use, privacy, and digital safety
- Report any misuse or safety concerns to the nominated supervisor or approved provider

Our full Technology and Device Use Policy is available in our Policy Folder and One Drive Policy Folder

16 Appendix C: Digital Device Log Template

Date	Device ID	Device Description	Issued To (Name & Role)	Purpose of Use	Issued By (Name)	Return Date	Condition on Return	Remarks
01/10/2024	*001*	*iPad Pro 11"*	*Zaim Sainsbury (Educator)*	*Capturing Learning*	*Amy Li*	*01/08/2024*	*Good*	
02/10/2024	*002*	*Samsung Galaxy Tab*	*Jo Rodriguez (Nominated supervisor)*	*Administrative Use*	*Amy Li*			*Not yet returned*
03/10/2024	*003*	*Nikon D3500 Camera*	*Amina Al-Hassan (Educator)*	*Documenting Activities*	*Amy Li*	*03/08/2024*	*Minor scratches*	

Additional Notes

- Ensure all staff members authorised to use digital devices have read and acknowledged the Technology and Device Use Policy
- Devices should be secured with passwords and other necessary security measures to protect sensitive information
- Any incidents, such as loss or damage, should be reported to the nominated supervisor/approved provider