SAFE USE OF DIGITAL TECHNOLOGIES AND ONLINE ENVIRONMENTS POLICY

PURPOSE

Village Early Education is committed to providing a safe and secure environment for children, educators, staff and families when using digital technologies and accessing online environments. We recognise the importance of digital technologies in supporting children's learning, documenting their development, communicating with families and managing Service operations. All digital technologies must be used responsibly, with children's safety, rights, privacy and wellbeing remaining our highest priority.

DIGITAL TECHNOLOGY AND ELECTRONIC DEVICES

All digital technologies and electronic devices used at Village Early Education must be appropriately authorised, managed and secured to minimise risks to children and protect confidential information.

- Only Service-issued devices may be used to capture, store or transmit images and videos of children.
- Service-issued devices must be used for authorised work-related purposes and must not be used for personal activities.
- All Service-issued devices must be appropriately configured, maintained, secured and recorded in the Electronic Device Register.
- Service-issued devices must not be removed from the premises unless required for authorised operational purposes, such as excursions, transportation or approved work arrangements.
- Access to devices, software and online systems must be restricted to authorised personnel.
- Personal electronic devices and storage media must not be used or possessed while working directly with children, except where a permitted exception applies.
- Digital technologies and online environments must be included in relevant risk assessments and reviewed regularly to identify and manage potential safety and security risks.

PERSONAL ELECTRONIC DEVICES AND EXEMPTIONS

The use or possession of personal electronic devices capable of capturing, storing or transmitting images or videos is prohibited while working directly with children, except in circumstances permitted by legislation and authorised in accordance with Service procedures.

This includes personal mobile phones, tablets, cameras, smart watches, smart glasses and personal storage devices.

Exceptions may be considered for essential purposes, including:

- Personal health or disability-related needs.
- Urgent family communication.
- Emergency situations or safety-related communication.
- Circumstances where a Service-issued device is unavailable or not functioning and a device is necessary for children's safety or care.
- Other circumstances permitted under applicable legislation.

Where authorisation is required, it must be documented using Village's Electronic Device Exemption Form.

Personal devices must not be used to capture, store or transmit images or videos of children, including where an exemption has been granted for another purpose.

Employees may use personal devices during designated breaks in areas where children are not present.

IMAGES, VIDEOS AND AUTHORISATION

Village Early Education recognises children's rights to privacy, dignity and protection when capturing, using, storing and sharing images or videos.

- Written parent/guardian authorisation must be obtained before images or videos of children are captured, used, stored or shared, as required by the Service's authorisation arrangements.
- Families must be informed about how images and videos will be captured, used, stored, shared and destroyed.
- Images and videos must only be captured for legitimate and authorised educational, communication or operational purposes.
- Children's views and preferences must be respected, with age-appropriate consent sought before capturing images or videos.
- Images and videos must be appropriate, respectful and preserve children's dignity.
- Images or videos must not be taken of children in a state of undress, in distress or in circumstances that may compromise their privacy or safety.
- Images and videos must only be captured using authorised Service-issued devices.
- Images and videos must not be transferred to personal devices, personal accounts or unauthorised storage platforms.

- Separate authorisation must be obtained where required for marketing, social media, external photography or other purposes outside routine educational documentation.
- External professionals must obtain the required authorisations before capturing images or videos of children.
- Families may withdraw their authorisation in writing. Changes to authorisation must be recorded and communicated to relevant employees, and further use of images and videos must comply with the updated authorisation.

STORAGE, SHARING AND DESTRUCTION OF DIGITAL INFORMATION

All digital information, including images, videos and personal information relating to children, families and employees, must be securely managed.

- Digital information must be stored within approved Service systems, including OWNA and SharePoint, as appropriate.
- Access must be restricted to authorised personnel based on their responsibilities.
- Confidential information must not be stored on personal devices or unauthorised storage platforms.
- Images and videos must only be shared with authorised recipients and for approved purposes.
- Images and videos must not be downloaded, copied or distributed without appropriate authorisation.
- Digital records must be retained, securely deleted or destroyed in accordance with applicable recordkeeping requirements and Village's Record Keeping and Retention Policy.
- Where an authorisation is withdrawn, existing images and videos must be reviewed to determine whether further use, removal or retention is appropriate and legally required.

CHILDREN'S USE OF DIGITAL TECHNOLOGIES

Digital technologies may be incorporated into children's learning experiences where they are age-appropriate, purposeful and consistent with the educational program.

- Children must be actively supervised whenever accessing digital devices or online environments.
- Digital devices must be used in areas where educators can maintain appropriate supervision.
- Content, applications and programs must be age-appropriate, culturally respectful and suitable for children.

- Screen time must be minimised and managed in accordance with relevant health recommendations and Village's Physical Activity Policy.
- Screen time must not be used as a reward or to manage challenging behaviours.
- Children must be supported to develop age-appropriate awareness of online safety, privacy and responsible technology use.
- Children must not independently access the internet or online platforms without appropriate educator supervision.
- Digital technologies must support inclusion and accessibility, including approved communication or assistive devices for children with additional needs.

Children must not bring personal electronic devices to the Service unless an appropriate arrangement has been approved to support their individual health, disability or communication needs.

SOFTWARE, ONLINE PLATFORMS AND ARTIFICIAL INTELLIGENCE

Village Early Education uses approved software and online platforms to support educational, administrative and operational activities.

- Only authorised software, applications and online platforms may be used for Service-related activities.
- Systems must be appropriately secured and maintained to minimise risks of unauthorised access or data breaches.
- Employees must use individual login credentials and must not share passwords or account access.
- Access to confidential information must be limited to personnel who require it for their authorised responsibilities.
- Service email accounts and approved organisational systems must only be accessed through authorised devices and arrangements.
- Artificial intelligence (AI) tools must be used responsibly, with outputs checked for accuracy, appropriateness and reliability.
- Personal or confidential information about children, families and employees must not be entered into unauthorised AI tools or platforms.
- AI-generated content must not replace professional judgement or compromise children's privacy, safety or wellbeing.

CLOSED-CIRCUIT TELEVISION (CCTV)

Village Early Education uses Closed-Circuit Television (CCTV) systems to support the safety and security of children, employees, families and Service premises. CCTV is only used for legitimate safety, security and authorised operational purposes.

Cameras are be positioned appropriately and are installed in areas where individuals have a reasonable expectation of privacy, including bathrooms and change facilities.

Village's CCTV system uses a Network Video Recorder (NVR) with automatic overwriting of older footage once storage capacity is reached.

Access to the CCTV system is restricted to authorised personnel only. Each authorised user is assigned unique login credentials, which are not to be shared under any circumstances.

Access is limited to:

- The Operations Manager
- The Area Manager
- The Nominated Supervisor

The system uses an internal audit trail to log records of user activity including:

- The identity of the user who logged in
- Which cameras were accessed or footage downloaded
- Whether access occurred locally or remotely

Families, employees and visitors are informed of CCTV use through appropriate signage and communication.

Access to the recordings will only be disclosed to authorised bodies to assist with investigations.

ONLINE SAFETY, INCIDENTS AND DATA BREACHES

All concerns relating to unsafe technology use, inappropriate digital content, unauthorised photography, online abuse or breaches of privacy must be taken seriously and responded to promptly.Employees must immediately report suspected misuse of digital technologies, inappropriate conduct or child safety concerns.

- Children must be supported to report anything encountered online that makes them feel unsafe, uncomfortable or distressed.
- Suspected online abuse, inappropriate content or other child protection concerns must be managed in accordance with Village's Child Protection Policy and relevant reporting requirements.

- Suspected loss, unauthorised access or disclosure of confidential information must be promptly reported to appropriate management.
- Data breaches must be assessed, contained, documented and notified to relevant authorities where required.
- Incidents involving digital technologies or online environments must be reviewed, with appropriate corrective actions implemented.

Failure to comply with this policy may result in disciplinary action, restrictions on system access or other appropriate action.

CONTINUOUS IMPROVEMENT/REFLECTION

Our *Safe Use of Digital Technologies and Online Environments Policy* will be reviewed on an annual basis or earlier if there are changes to legislation, ACECQA guidance or any incident related to our policy. Feedback will be requested from children, families, staff, educators and management and notification of any change to policies will be made to families within 14 days.

SOURCES

Australian Children's Education & Care Quality Authority. (2026). *Guide to the National Quality Framework*
Australian Children's Education & Care Quality Authority. (2025). *NQF Online Safety Guide*
Australian Children's Education & Care Quality Authority. (2026). *Using digital devices in centre-based education and care services*
Australian Government. eSafety Commissioner. (n.d.) *Report online harm*
Australian Government. Office of the Australian Information Commissioner. (2026). *Australian Privacy Principles guidelines*
Australian Human Rights Commission. *(n.d.) Child Safe Organisations.*
Education and Care Services National Law Act 2010
Education and Care Services National Regulations 2011
Privacy Act 1988.

REVIEW

POLICY REVIEWED BY	Kelsey Pearce		
POLICY REVIEWED	OCTOBER 2026	NEXT REVIEW DATE	OCTOBER 2027
VERSION NUMBER	V4.10.26		
MODIFICATIONS	• redrafted for clarity • sources checked for currency and updated as required		