DIGITAL DEVICE POLICY

National Quality Standard: QA 2 – Children's Health and Safety

Policy Owner: Safety and Compliance

1.0 Introduction and Purpose:

The purpose of this policy is to establish clear guidelines and expectations for the appropriate use of digital devices and technology, ensuring the highest standards of safety, wellbeing, privacy, and developmental appropriateness for all children in our care. This policy is informed by and aligns with the *National Model Code for Managing Digital Devices in Early Childhood Education and Care Settings (2024)* ("the Code").

In an increasingly digital environment, we must adopt thoughtful, responsible, and transparent practices in relation to the use of iPads, laptops, mobile phones, online documentation platforms, CCTV, and other digital technologies.

This policy prioritises the safety and protection of children by preventing the misuse of digital devices, safeguarding against inappropriate access to or sharing of children's personal information or images, and minimising exposure to potential digital risks such as data breaches, unauthorised recordings, or cyberbullying.

In doing so, the policy reflects our legal and ethical obligations under the National Quality Framework (NQF), the Child Safe Standards, and the *Australian Privacy Act*, and embeds children's rights, safety, and wellbeing as the paramount consideration in all decisions relating to the use of digital devices and technology.

2.0 Who does this policy apply to:

This policy applies to all educators, team members, work experience/practicum students, volunteers, families, contractors, and visitors involved with our centres, support offices or other Guardian organised locations.

3.0 What is our policy:

3.1 Our Scope

3.1.1 Device Development

As digital technology continues to evolve, this policy applies to all current and future digital devices capable of capturing, storing, or transmitting images, videos, or audio. This includes, but is not limited to, mobile phones, tablets, smartwatches, wearable devices, and any emerging technologies with similar capabilities such as sunglasses and digital rings. Devices may not be individually named within this policy; however, any device with the functional capacity to record or store visual or audio content will be subject to the same requirements and restrictions as smartwatches to ensure the privacy, safety, and wellbeing of children and team members.

3.1.2 Digital Device Usage

The use of digital technology must always support, and not compromise, children's rights. Devices are used in ways that enhance children's learning, support high-quality documentation, and strengthen engagement with families, but never at the expense of a child's safety, dignity, or developmental needs. Educators and team members are expected to model safe, respectful, and ethical behaviour in all digital interactions, including the handling of devices and data.

This policy ensures that the use of digital technologies across Guardian is transparent, intentional, secure, and subject to ongoing monitoring and review. Team members will not take photographs/video of children who are sick, injured, asleep, toileting or distressed. Photos/video must not be taken routinely as part of incident reporting unless explicitly instructed by Compliance or a Regulator including the police.

Families provide media permission as part of the enrolment process, authorising the centre to capture and use photographs and videos for educational, media, and promotional purposes. For any specialised media activity, including events where external photographers or videographers are engaged the centre will notify families in advance and request a separate, event-specific media consent e.g. external photographer retained for end-of year photos, Guardian marketing arranged events.

Families may revoke their media consent at any time. To ensure accurate record-keeping, any withdrawal of permission must be submitted in writing (by email or written note) by the family and placed on the child's file.

3.2. Devices, images and exemptions

3.2.1 Guardian Owned Devices
The use of *personal devices* as defined in the definitions section such as iPad, tablet or laptops, phone etc are prohibited for work purposes unless a *Personal Digital Device Exemption Form* has been completed and approved. This includes personal devices owned by families and used by team members to monitor a child's medical condition.

Guardian owned iPads and tablets available for use in our centres, are important tools for programming, documentation, and educator communication. These devices are used to:

- record child observations, develop learning stories
- communicate with families and research educational content

Only Guardian team members are permitted to use these devices for documentation or programming purposes. Students may be able to use Guardian iPads whilst supervised where it relates to assessment related work or supporting programming.

All centre-owned devices must be stored securely when not in use and must be password-protected and must not be removed from centre premises unless for the purposes of approved excursions and emergency evacuations or technology outage and /or where an approved and valid exemption is in place. Access to information will be managed in accordance with *Guardian's Privacy Statements*.

3.2.2 Images and Videos
Images and recordings are used to document children's learning, support planning, and communicate with families.

Media consent is obtained at enrolment and again for any specialised marketing, promotional activity, or external media event to ensure families remain informed and in control of how their child's image is used.

Families may revoke their consent at any time in writing. When consent is withdrawn or a child's enrolment ends, the centre reviews all stored media and permanently deletes any images or recordings not required for regulatory purposes or linked to a specific approved event.

Additional NSW Policy Requirement: All centres must have a current *Digital Device Asset Register* accessible on Centre Desktop that details all current service devices. This must include when the device was provided and revoked as well as declaring that the devices comply with policy.

3.2.3 The Transfer and Deletion of Images or Videos
Any images or videos of children or other sensitive information (e.g. completed enrolment forms, medical information, care routine daily charts, confidential written communication between families and team members) that are taken on company issued iPads or laptops cannot be shared or transferred to a personal device.

Where images of the physical environment or a blank document is transferred from a Guardian device to a personal device for the purposes of meeting assessment requirements, verbal approval must be gained from the Lead Educator/Teacher or a Responsible Person. This includes sharing via cloud-based services, hard drive, USB or any other method.

All Guardian devices will have their photos/videos deleted on a monthly basis with centres undertaking a check of all images and also delete these after use, when not needed. Centres are also required to delete their virtual 'rubbish bin'. Team members should delete images from Guardian devices (e.g. laptops and iPads etc) after they have been used for planning purposes and /or where the child ceases enrolment. Centre Managers will check and verify that images are deleted from iPads and laptops monthly

Centres may keep a file on Centre Desktop in their secure Centre Manager File that can be used for lockers, medical conditions photos or where a photo is required to for a child to be identified. This file will be deleted when the child ends their enrolment or at the end of each year whichever is sooner.

Apps are unable to be downloaded onto Guardian devices without approval. All app requests must be sent to our IT team where approval will be considered and centrally uploaded onto our network devices. Our IT team hold a register of approved apps. Where apps remain inactive for over 12 months, these will be removed centrally by the IT department.

3.3 Personal Digital Device Use

3.3.1 Centre Managers and Responsible Persons

Centre Managers and Responsible Persons in charge are authorised to use their personal mobile phones during emergency situations including technology outages, drills and evacuations. This includes using a personal device to receive government emergency alerts through official warning systems (e.g. bushfire evacuations), allowing for timely evacuation or action. Phones must be returned to the office upon completion of the emergency activity. The taking of images on personal mobile phones at these times is not permitted.

When the Responsible Person-in-charge is working directly with children, their personal mobile device must be stored in a location that is inaccessible to children. This exemption applies only to days when the individual is acting as the Responsible Person in charge for that shift. As this use is pre-approved, Centre Managers and Responsible Persons are not required to complete a *Personal Digital Device Exemption Form* for these purposes.

3.3.2 Team Members

Team Members are not permitted to use personal digital devices during working hours whilst working with the children unless an approved exemption is in place. All team member i.e. chefs, administration must not have a personal digital device on their person during working hours unless an approved exemption is in place. Team members who require a personal digital device in a learning space or on their person must have completed and have approved a *Personal Digital Device Exemption Form* (**'exemption form'**) that is kept on their team member file. requirements of the code.

The exemption form details the only permitted reasons for a personal device. The reasons that that an exemption may be approved relates to health-related matters including a disability or family emergency. Other exceptional circumstances may be considered on a case-by-case basis but must meet the requirements of the National Law. If the reason for granting a personal device is not detailed on the exemption form, you must contact the Safety and Safety and Compliance Team for approval.

The exemption form must detail the reason for the personal digital device access, any supporting documentation and document control strategies.

Where an exemption is in place, team members must not take their personal digital device in children's bathrooms, adult bathrooms or used at times in spaces where children are getting dressed or undressed.

This exemption must be updated annually or at the conclusion of the exemption period. Further reviews will occur every three months to ensure that the exemption is valid. Where a Centre Manager becomes aware that the reason for the exemption no longer applies the centre manager will inform the team member within 48 hours and issue them with a Removal *of Digital Device Exemption Form*.

Personal digital devices (e.g. mobile phones, iPads etc) must be stored away securely during shifts in either a team room/office and not in a location children are currently or would be present.

Team Members must not use personal digital devices to take photos/videos, send messages, or store any information about children. This includes planning and programming information, photos or videos of children's documentation in permanent learning areas or any other location in the centre.

3.3.3 Smartwatches

Team members are permitted to wear watches whilst working with children. Fitness watches may be worn where they only track physical activity and basic health metrics such as heart rate, steps, distance, or sleep. Where a team member has a fitness watch they will complete a *Fitness Watch Declaration and Acknowledgement Form* to verify that this is only a fitness watch and not a smartwatch as defined in the definition section.

Smartwatches are **banned** when working with children unless an approved and valid *Personal Digital Device Exemption Form* is in place.

In addition, where team member requires an exemption for both a mobile phone and a smartwatch, the Centre Manager must forward the completed exemption form to Safety and Compliance tor approval.

3.3.4 Support Office Use
Support Office Team Members are not permitted to take any personal digital device nor wear a smartwatch into a learning space.

Where support office team members are required to take photos or video of children for the purposes of supporting teams or undertake their work they must use a Guardian digital device.

3.3.5 Families
The use of family/guardian's personal mobile phones is not permitted in learning spaces where children are present. Families must move to areas not used by children if a mobile call must be taken or made.

Families are not permitted to take photos or videos using a personal device in a learning space. In the case of events (e.g. Christmas party) refer to 3.6 of this policy.

3.3.6 Visitors, Students, Volunteers and Contractors
Visitors, Students, Volunteers and Contractors are similarly prohibited from using personal digital devices in learning areas, or taking photos or videos of children or printed photos of children (e.g. photos on display of children playing etc)

Volunteers who attend excursions and are parents/guardians of a child may use their personal device to take a photo/video of their own child. They cannot take a photo/video of another child with their personal device without written/verbal consent from the child and their child's parent/guardian.

Where a visitor (e.g. allied health, incursion etc) requires the use of an app on a digital device they must forward this requirement in advance in writing to the Centre Manager. The Centre Manager will make a request to the IT helpdesk for this app to be installed onto a Guardian Device.

Contractors are approved to take photos or video using their personal digital device of the environment (e.g. to quote a job, demonstrate works underway or complete). Children must not be in proximity whilst any photos/video are taken.

Practicum/Work Experience Students are not permitted to take images of children for the purposes of assessment. All assessment must be completed via onsite observation. Where onsite observation is not feasible due to a centre located in a rural area, the observation can occur via live streaming, provided the training provider and Nominated Supervisor/Responsible Person mutually agree.

3.3.7 Medical Exemption
Where a child or team member required a digital device to monitor or support the management of their medical condition i.e. mobile phone, there must be an approved *Personal Digital Device Exemption Request Form* in place. For specific information about the use of digital devices to support medical conditions refer to the *Medical Conditions Policy*.

3.4 Online Learning and Documentation Environments

3.4.1 Approved Online Platforms
Our network of centres uses secure, approved online platforms (e.g. Story Park), to document and communicate children's learning and development with families. Educators use these platforms to upload observations, learning stories, assessments, and individualised planning, aligning with the EYLF and NQS.

Centres also share best practice examples and stories of practice via Viva Engage (Intranet Social Media Site), Instagram and Facebook. For information about the appropriate use of Instagram and Facebook refer to the *Employee Social Media Policy*.

Team Members must ensure that media consent from families before using any photos or videos in public forums such as newsletters, marketing material, or social media.

3.4.2 Family Access
Families are given secure access to their child's digital portfolio through Story Park. They can view and respond to their child's learning updates but must not share documentation involving other children. Any media or data stored on these platforms is strictly protected, and team members must not use their personal or other people's email or cloud storage to save or send any child-related documentation.

3.4.3 Children's Use of Online Environments
When used with children, iPads and tablets must support educational objectives. Examples of appropriate use include digital storytelling, music experiences, language learning (e.g. ELLA), and creative apps that support Early Years Learning Framework (EYLF) outcomes. Screen time for children is limited and always supervised, ensuring that it is developmentally appropriate, interactive, and complements the play-based learning environment. Children are not allowed to access devices unsupervised or browse the internet independently.

The use of Guardian iPads and laptops and the use of online learning environments must be documented on centre risk assessments. This must include their use, storage and access.

3.5 CCTV and Surveillance
The centre may use Closed-Circuit Television (CCTV) to enhance security and monitor the safety of children and team members. The installation of CCTV is undertaken on a case-by-case basis and is used when supervision of spaces is complex. CCTV cameras are only installed in shared or external spaces, such as entrances and playgrounds/learning spaces. Cameras will never be placed in private or sensitive areas, such as bathrooms, nappy change areas, or sleep rooms.

Families and team members are notified of CCTV use through enrolment and employment documentation, and signage is clearly displayed where cameras are in operation. For more information review the *CCTV Policy.*

3.6 Events
Photography at family events, excursions, incursions, and routine activities is managed on a case-by-case basis and must be clearly outlined in the relevant routine outing or excursion/incursion form.

For large-scale events, a team member will be appointed as the photographer with images shared with families afterwards.

Annual photography days occur at most centres. Parents / Guardian must provide permission for their child to participate; in absence of permission the child must not appear in any photographs. As part of the permission process families will be informed of the storage and access arrangements to photos.

3.7 Cyber Safety and Professional Conduct
All team members must uphold the highest standards of cyber safety and digital conduct. Team members receive training in digital privacy, responsible device use, and ethical online practices. All devices and online accounts must be protected with strong passwords, and sensitive information must never be shared through unsecured channels. Personal use of social media must remain separate from professional responsibilities, and team members must not post any content that references children, families, or the centre.

For further specific information related to social media or digital security refer to the *Confidentiality, Privacy, Digital Information Security Policy*.

3.8 Breaches of Policy
Where a parent or Guardian refuses to adhere to this policy after a reminder this matter will be referred to the Centre

Manager. If a subsequent breach occurs this may result in preventing attendance at the centre or cancellation of the Guardian enrolment at a Guardian centre.

Where a student, volunteer (other than a parent), contractor visitor breaches this policy they will be exited from the centre after one reminder of their responsibilities.

Where a team member is found in breach of this policy they will be managed in accordance with the *Child Harm Classification and Management Table*.

5.0 Definitions

Fitness watch A fitness watch is a wrist-worn device designed solely to monitor physical activity and basic health metrics. A device is considered a fitness watch if it only tracks data such as heart rate, steps, distance, or sleep, and cannot send or receive calls, messages, notifications, access apps, record audio, or take photos.

Personal Device is any privately owned phone, tablet, smartwatch, computer, camera, or digital storage device capable of capturing, storing or sharing images, videos or audio, and not issued or managed by the service including USBs, SD Cards and Hard drives

Smartwatch A smartwatch is a wrist-worn device that functions as a watch and can connect to a mobile phone or the internet to send or receive notifications, calls, messages, or data. A device is considered a smartwatch if it can display, capture, store or transmit communications, record audio or images, or access apps beyond basic timekeeping.

Social Media websites and applications that enable users to create and share content or to participate in social networking such as Instagram and Facebook

6.0 Tools and Resources

The most important documents I need are:	**Other supporting documents will include:**
• *Personal Digital Device Exemption* • *Removal of Digital Device Exemption* • *Smartwatch and other device declaration* • *Fitness Watch Declaration and Acknowledgement Form*	• Social Media Policy • Confidentiality, Privacy, Digital Information Security Policy • Medical Conditions Policy • Guardian's Privacy Declaration

References

National Model Code for Managing Digital Devices in Early Childhood Education and Care Settings (2024)

Education and Care Services Act (2010)

Education and Care Services Regulations (2011)

6.0 Responsibilities

The **Approved Provider** will:

1. Ensure the development, implementation, and ongoing review of the Digital Device Policy
2. Provide access to secure, centre-owned digital devices that support documentation and communication requirements
3. Approve the use of CCTV and ensure that its installation and use meet legal and ethical standards
4. Monitor compliance with privacy laws and regulatory obligations regarding digital safety, data handling, and consent
5. Approve any exemptions to mobile phone use and ensure appropriate risk controls are in place
6. Ensure the secure management of cloud systems, data storage, and online platforms in accordance with privacy legislation

The **Centre Manager / Nominated Supervisor** will:

1. Implement the policy consistently across the service and ensure all educators, students, volunteers, and families are informed of digital device requirements
2. Monitor and supervise team member compliance with digital device usage, including the use of iPads, smartwatches, mobile phones, and online learning platforms
3. Ensure that all team members who need to use or access a Personal Digital Device completes a *Personal Digital Device Exemption Form* that is completed in full, where risks are managed and discussed with the team member. A copy of the completed form will be kept on the team members file and uploaded on Centre Desktop
4. Maintain accurate records including *Personal Device Exemption Forms*, risk assessments, and family consent documents
5. Where it is identified that a team member no longer has a valid reason for an exemption, they will inform the team member that the exemption no longer applies and provide them with a *Removal of Digital Device Form* and keep a copy on the team member's file.
6. Ensure digital records and documentation platforms (e.g., Story Park) are securely accessed, managed, and regularly backed up
7. Communicate photography guidelines clearly with families before centre events and ensure designated photographers are used as required
8. Report and respond to any breaches of this policy promptly, following appropriate disciplinary and regulatory procedures
9. Ensure that there is a process implemented so that iPads are checked monthly and photos that are not needed are deleted. This will include the deleting the deleted files that will appear in the 'rubbish bin'
10. That current *Personal Digital Device Exemption Forms* will be reviewed every three months to assess if they are valid
11. Ensure that where a team member has a fitness watch that they will complete a *Fitness Watch Declaration and Acknowledgement Form* that is kept on the team members file

In addition, Additional NSW Policy Statements:

1. Ensure that the centre maintains a current *Asset Register* that includes all service provided devices that is stored on their centre desktop and available on request

We recommend the **Centre Manager/Nominated Supervisor**:

1. Lead reflective practice and team training on digital safety, cyber conduct, ethical device use, and privacy protections

Team Members will:

1. Use only centre-approved and secure devices for educational documentation, family communication, and learning activities
2. Store all centre-owned devices securely and ensure devices are password-protected and logged out when not in use
3. Not use personal mobile phones during working hours unless on a planned break and not in the presence of children or an exemption has been approved and risk management strategies documented
4. Ensure children do not access digital devices unsupervised and use technology only in ways that support EYLF outcomes
5. Follow all consent and privacy protocols when using or storing digital images or videos of children

6. Participate in training and maintain professional conduct in all digital communications and online interactions
7. Ensure that images and videos are taken for programming and education purposes and photos are never taken of children who are distressed, hurt, asleep, injured or undressed
8. Ensure that smartwatches are not worn whilst working with children
9. Not wear smartwatches when working with children unless a valid and approved *Personal Digital Device Exemption Form* is in place
10. Ensure that if they have a fitness watch they sign *a Fitness Watch Declaration and Acknowledgement Form* to verify that this is only a fitness watch and not a smartwatch as defined in the definition section

Students and Volunteers will:

1. Use only Guardian devices when participating in documentation activities and obtain required permissions before taking photographs
2. Follow team members directions when using digital technology and maintain professional conduct at all times
3. Do not bring or use personal digital devices while engaging with children or in learning environments
4. Comply with all privacy, consent, and safety protocols in relation to digital records and images

Families will:

1. Read and sign media approval section on the enrolment form. Alternatively, where permission is not provided document this information and provide this to the Centre Manager
2. Support the centre's digital device policy by refraining from using their personal mobile phones or tablets in learning spaces and only photographing or recording their own children
3. Provide all required documentation when a personal mobile device is required for use by team members in a learning environment to support their child's medical condition
4. Seek permission before taking or sharing images of other children, following the 'no permission, no photo' rule
5. Follow all event photography arrangements and respect the role of the designated photographer at large-scale events
6. Use online platforms such as Story Park appropriately and securely to engage with their child's learning
7. Raise any concerns about digital safety, media consent, or device usage with the Centre Leadership Team
8. Communicate with the centre in writing if you do not approve or wish to revoke media permission approval

Policy owner	Chief of Quality and Curriculum Officer		**Content author**	National Safety and Compliance Manager	
Date published	27/02/ 2026	**Document version**	V2.0	**Revision due date**	01/10/2028
Ensure you are using the latest version of this procedure.					
Warning – uncontrolled when printed. This document is current at the time of printing and may be subject to change without notice.					