

Safe use of Technology, Devices and the Internet Policy – NSW

1. Overview

1.1. Scope

This policy applies to any person involved in the provision of an approved JAG service. This includes but is not limited to:

- The Approved Provider and Persons with Management or Control.
- service leaders, including Nominated Supervisors, Service/Regional Managers, Regional Directors and any support office staff when visiting a service,
- educators (including casual and agency staff)
- other employees
- volunteers and students
- paid or unpaid third parties delivering programs or activities to children in a service

This policy **does not** apply to people who do not work directly with children and are not providing education and care, for example:

- parents and carers dropping off or picking up their child from a service or taking photos and videos of their own children at service events
- Police or other responding services including Ambulance, Fire Services
- officers from regulatory services (including NSW Early Learning Commission, NSW Office of the Children’s Guardian compliance officers and NSW Food Authority authorised officers)
- third parties attending the service but not working with children or providing education and care (e.g. maintenance contractors, security personnel, cleaners).
- children attending the service

Although this policy does not apply to these people, services must remain vigilant and implement policies and procedures on the provision of child safe environments.

2. Policy Statement

Junior Adventures Group recognises the use of technology, and the internet, is a necessary part of everyday life, shaping the way we work, and the way children learn, communicate and play. To ensure children’s safety, the service will implement the following guidelines around the safe use of technology, devices and the internet.

3. Principles

3.1. Duty of Care

JAG people have a duty of care to all children attending the program and will ensure that all children are protected from inappropriate use of multimedia and electronic devices. **Any person working directly with children will have their access to personal devices restricted** per the provision of this policy. 'Working directly with children' means any person involved in the provision of an approved Early Childhood Education and Care (ECEC) service who is, at a given time, physically present with a child or children and employed, engaged or appointed to provide education and care to the child or children at that time. A person is not working directly with children at a given time if the person is taking a break from providing education or care to children in accordance with the person's employment, engagement or appointment.

3.2. Educational Program

JAG recognises that creating a stimulating and engaging environment enhances children's learning and development. The development of life skills and relationships can be strengthened in the service environment by guiding the safe use information technology.

Children will be encouraged to:

- engage in meaningful face-to-face connections and interactions with others
- develop relationships that are positive and respectful
- focus on group activities in addition to independent activities
- participate in a wide variety of activities, including outdoor and active play, creative, dramatic, imaginative play and social experiences
- connect with the natural environment and develop a sensibility based on holistic and sustainable principles
- develop an awareness of their physical and emotional wellbeing in an environment that is not dominated by/is largely free of technology
- enjoy respite from the external stimuli associated with digital technology.

3.3. Partnership with Families

Families are encouraged to respect JAG's intention by ensuring expectations around the use of technology, devices and the internet are clear for the children. JAG families are also encouraged to role model and promote behaviour within the JAG environment consistent with this policy.

The service reserves the right to regulate device use by parents and carers to help protect the privacy and wellbeing of all children. If a family member is seen to be taking photos at the service which includes other children, for example, they will be instructed that this is not permitted. Generally, family members will be discouraged from taking photos at the service.

3.4. JAG Devices and Access

If services or team members are issued with, or have access to, a device owned by JAG, it always remains the property of the organisation. A service supplied device is one that:

- has been supplied by the approved provider, by way of a formal process of obtaining service issued devices through IT
- is used for the purposes of filming, recording, taking or otherwise capturing an image of a child being educated and cared for by the service

- is configured to comply with the service's child safety and device security policies and procedures.

JAG People must ensure the safety and security of equipment by storing devices in a safe place to prevent unauthorised access, damage or theft.

Where team members are issued with or informed of a password or other information that allows access to our equipment, software, hardware, information, or data, they must ensure it is kept safe and not shared.

At any time, management can access internet usage, data or email should it be necessary to ensure the adherence and security of our systems, equipment and information.

JAG devices will be kept in a register with the following information:

- a declaration the device is configured to operate in line with service policies and procedures that relate to child safety or device security
- the date of the supply of the device
- the type of device that is supplied
- the make, model and serial number of the device
- the name and signature of the approved provider or their authorised delegate supplying the device
- if applicable, the date of any revocation of the supply of the device and the name and signature of the approved provider or their authorised delegate authorising the revocation

These records will be stored in a safe and secure place for at least 3 years from the date on which the authorisation record was made. The register will be available at the service on request.

A service-supplied device must be used exclusively for the purposes of the direct provision of education and care to children. If a staff member is found to use a service issued device for personal reasons, this will be dealt with as a disciplinary matter.

A service-supplied device is specific to the service and must not be shared across multiple services. Where a device is used for work related to education and care that does not involve the direct provision of care, it may be used across multiple services under the same approved provider, provided its use is authorised at each service.

Examples include but are not limited to:

- an approved provider who uses the device at more than one of their services
- a manager of multiple services using the device for a compliance review.

3.5. Video, Radio and Television

The role of video, radio, TV and multimedia games is given thoughtful consideration and will not form part of the daily program. From time to time, the program may incorporate technology. However, it is not a core component of the education and care program.

Movies may be screened during some school holiday programs, or excursions to cinemas might occur; movies will be G and PG rated and monitored by JAG People. Parents/Guardians will be informed of any movie viewing, which will be relayed through the displayed program information.

Parents can access additional information about films being scheduled on the program by visiting the Children and Media Australia media website: <https://childrenandmedia.org.au/>

3.6. Social Media

All JAG People must ensure the reputation of the organisation, its employees and stakeholders are not harmed during the use of any technology or sharing platforms such as social media. JAG People must ensure when they are using social media or online platforms, their views are not seen as the views of the organisation and are not demeaning, derogatory, inflammatory, misrepresentative, harassing or discriminatory of the organisation or any employee.

Images, videos or recordings of children, families, or staff in uniform are not permitted to be sent, used, posted or shared on social media platforms or other online forums unless written authorisation is obtained by Parent/Guardian or Team member.

The personal information, including names of children and families obtained during work, remain the organisation's property, are deemed confidential and must not be shared.

3.7. Photography and Videos

JAG People are not permitted to record, video or photograph other JAG People unless prior permissions have been sought.

Any images or videos taken of children can only be taken on a JAG issued device in and in accordance with images and photos of children procedure.

Images and videos of children are stored on a secure, password-protected JAG issued devices. They are only stored for the duration required. In many cases, this will mean images and videos can be deleted as soon as they are used for their intended purpose. Images and videos are not to be transferred to external storage devices (USBs).

Authorisation from families to take, use and store images and videos of children will be obtained from families upon enrolment, and kept within their enrolment details on Kidsoft. If authorisation is not obtained, JAG people will ensure that no photos and videos will be taken of these children

Images and videos of children must not be distributed or used in marketing materials unless prior written authorisations are sought.

All data including photographs is stored in secure, role-based cloud folders, not locally. Retention and destruction of records is managed under the *Record Keeping & Archiving Policy*. Children are discouraged from photographing or videoing other children or JAG People unless

prior communications and authorisations are sought for the purposes of the educational program.

3.8. Computers and Gaming Devices

The use of computers, phones, hand-held electronic games and PlayStation and Xbox or other consoles is discouraged except for:

- access to a dedicated computer for homework, research or other supervised tasks/activities
- themed days or events specifically planned to allow children access to and interact with such games (e.g., during holiday programs). Use of these devices at such times will be carefully monitored and supervised by staff.

3.9. Staff Personal Devices

A personal device is one that is owned or controlled by an individual – but does not include a service-supplied or service authorised device – that can take, store or transfer images or videos.

This policy applies to any device capable of filming, recording, taking or capturing images or videos, and/or storing or transmitting images or videos. Examples include but are not limited to:

- mobile phones
- smartwatches with cameras
- smartwatches that can take, receive, store or transmit an image, even if the smartwatch does not have a camera
- tablets
- computers
- cameras
- wearables, such as smart/camera glasses
- USB drives
- memory cards
- hard drives.

Team Members are not permitted to access personal devices whilst they are working directly with children. Personal electronic devices should be stored in a secure location, not on the person.

Personal devices are only used in essential or emergency situations as per the Education and Care Services (Supply, Authorisation and Use of Devices) Order 2025, and only if an appropriate JAG device is not available. The limited use of a personal device is permitted, if authorisation from a member of the senior leadership team is given in writing.

Essential purposes for which use and/or possession of a personal device may include:

- communication in an emergency situation involving a lost child, injury to child or staff member, or other
- personal health requirements, e.g. heart or blood sugar level monitoring
- disability, e.g. where a personal electronic device is an essential means of communication for an educator or other staff member
- family necessity, e.g. a worker with an ill or dying family member

- technology failure, e.g. when a temporary outage of service-issued electronic devices has occurred
- local emergency event occurring, to receive emergency notifications through government warning systems, for example, bushfire evacuation text notification.
- Work, Health and Safety purposes

The Approved Provider may grant written authorisation for a staff member to possess or control a personal device capable of taking, storing and transmitting images and videos while working directly with children in limited situations. Staff who need access to a personal device must first complete the *Personal Device Access Request Form*. This is then reviewed by the Approved Provider, PMC, or delegate, and either approved or denied.

JAG will keep a written record of prior authorisation given for the use of personal devices for a minimum period of 3 years. The record includes:

- service details
- person's details
- reasons for the authorisation
- duration of the authorisation.

A written authorisation is valid for not longer than 3 months after which time the above process will be repeated.

Third-party professionals

When attending a service and working directly with children, third-party professionals (such as an allied health professional, HHQ or ECA providers) can use a device that is:

- issued by their business or institution
- used only for work purposes (not personal use)
- used by approved photography or videography service providers only for the purpose of capturing authorised images (e.g. preschool photos, end-of-year concerts), in line with the service's authorisation processes and under the direct supervision of staff.

3.10. Children's Devices

Children are generally not permitted access to phones or other devices at any time during sessions of care. The exception to this provision is via prior arrangement between the Service Leader and families for the purposes of a programmed activity incursion or club (example – Homework Club) facilitated by the service, or under an arrangement to support a child's individual needs.

Where the use of phones or other devices is permitted, a *Technology Agreement* must be signed by the child and their parent/guardian. Where access is allowed, staff will carefully monitor the use of devices in children's possession. Guidelines in relation to this will be followed in accordance with school policy. The service will make decisions around the individual restriction of devices where children are found to be misusing them, and address this with families using behaviour guidance strategies.

Children will only have access to technology, devices or the internet whilst under the direct supervision of JAG Team Members.

Educators can provide storage for mobile phones or other devices if required, however JAG, its services, and its people cannot be held responsible for the loss, theft or damage of any devices children bring to the service.

3.11. Recording Devices

Children and visitors are generally not permitted to film or record anything while on site unless there is specific authorisation from the Service Leader onsite. No personal recording devices are authorised to be used in service. If recording or photography is required, this should be achieved with a JAG device, and with prior authorisation.

3.12. Lost Equipment

JAG strongly discourage children from bringing valuables to the program; this includes electronic and technology devices. JAG will not be responsible or liable should they be lost while attending the program.

3.13. eSafety for Children and Young People

JAG recognises every child's right to feel safe and supported, including when using online platforms and technology. Our services are committed to being proactive in the prevention and protection of children from the effects of cyberbullying, image-based abuse and illegal or restricted content.

Any harmful or unlawful content or behaviour involving devices, technology or the internet will be documented in an incident report and treated in accordance with the *Incident Management Policy and Procedures*.

All JAG People are mandatory reporters. In accordance with the *Safeguarding Children and Young People Policy*, safeguarding concerns or instances of child-related misconduct must be communicated to management, the regulatory authority and state-based child protection reporting authorities.

3.14. Performance and Breaches

Any conduct found to contravene this policy will be investigated and result in disciplinary action in line with our *Managing for Performance Policy and Procedures*.

To promote and maintain expected standards of conduct, it is important that all JAG People are able to raise a concern about the conduct of another employee freely and without intimidation. JAG will ensure:

- all reports of non-compliance will be taken seriously and investigated as a matter of priority
- all reasonable steps are taken to protect JAG People who make a complaint in good faith from being disadvantaged, victimised or discriminated against for reporting a breach
- false reports made vexatiously or in bad faith are investigated and actioned in accordance with *Managing for Performance Policies and Procedures*.

3.15. Safeguarding Children

We safeguard children through our procedures, practices and clear staff expectations. JAG policies and practices reflect relevant legislation, including the National Principles for Child Safe Organisations, and are designed to protect children in both physical and online environments. JAG provides systems, policies and procedures that equip JAG people with the knowledge, skills and awareness required to keep children safe.

Service practices are continuously reviewed and improved to ensure current legislation, digital safety standards and safeguarding expectations remain embedded throughout the business. We actively support children to develop safe and respectful online behaviours and encourage them to speak up if something online makes them feel unsafe or uncomfortable.

3.16. Optical Surveillance Devices

JAG does not install or operate CCTV systems in our services. Some host schools or venues may have CCTV cameras installed in shared areas (e.g., playgrounds, carparks, corridors). These systems are owned and managed by the school/venue, and operate under their policies and procedures

4. Key Terms

Term	Definition
Children and Media Australia	Formerly the Australian Council on Children and Media, they were renamed in March 2022 and are the peak body representing children's interests as digital and screen media users
Cyberbullying	Use of the internet to be cruel to a child or young person so they feel bad or upset (e.g., sending hurtful messages or creating fake accounts in their name)
Devices	Laptops, desktop computers, iPads, tablets, mobile phones, internet connection devices, printers/scanners, gaming devices, projectors and other associated hardware
Emergency	An emergency in relation to an education and care service means an incident, situation or event where there is an imminent or severe risk to the health, safety or wellbeing of a person at the Service (e.g., fire, flood, lockdown)
eSafety	eSafety refers to safeguarding children, young people and adults from online harm and promoting safer online experiences
Illegal or restricted content	Includes material that shows or encourages child sexual abuse, terrorism or other extreme violence, as well as content that should not be accessed by children, such as sexual activity, detailed nudity or violence
Image-based abuse	Images or videos shared without the consent of the person pictured; usually refers to images of an intimate nature
Information technology	Technology involving the use of computer systems, software and networks for processing, distribution and interaction with data
JAG Families	Parents, carers and children related to and including children attending the program.
Service Leader	Anyone who oversees the Service in one of the following roles: <ol style="list-style-type: none"> 1. The Approved Provider; if the approved provider is an individual, in other cases, a person with management or control of the Service 2. The Nominated Supervisor of the Service 3. A Responsible Person who has been placed in day-to-day charge of the Service in the absence of the Nominated Supervisor.

Term	Definition
Team Member	JAG People who work directly with children.
Social capital	The positive product of human interaction providing tangible and intangible outcomes, such as gathering information, learning a new skill, innovative ideas and creating future opportunities
Service Issued Device	Includes but is not limited to: Phones, tablets, smart watches, computers, laptops, cameras, video recording technology that are managed and controlled by the organisation in alignment with regulations 168 of the education and care services national law.
Device	Includes but is not limited to: Phones, tablets, smart watches, computers, laptops, cameras, video recording technology

5. References

Education and Care Services National Law and Regulations
Australian Council on Children and the Media
Australian Government eSafety Commissioner
Children Education and Care Services National Law Act 2010
Early Childhood Australia Code of Ethics (2016)
Educational and Care Services National Regulations
Framework for School Age Care
Guide to the National Law and National Regulations
National Quality Standards for Early Childhood Education and Care and School Care
United Nations Convention on the Rights of the Child (UNCRC)
Other Relevant Legislation
Regulation 73 – Educational program
Regulation 75 – Information about the educational program to be kept available
Regulation 76 – Information about educational program to be given to parents
Regulation 84 – Awareness of child protection law
Regulation 98 – Telephone of other communication equipment
Regulation 122 – Educators must be working directly with children to be included in ratios
Regulation 168 – Education and care service must have policies and procedures
Regulation 170 – Policies and procedures to be followed
Regulation 171 – Policies and procedures to be kept available
Regulation 172 – Notification of change to policies or procedures
Regulation 181 – Confidentiality of records kept by approved provider
Regulation 183 – Storage of records and other documents
Section 51 – Conditions on service approval
Section 165 – Offence to inadequately supervise children
Section 167 – Offence relating to protection of children from harm and hazards
Online Safety Act – Cth
Privacy Act 1988 – Cth
175B Approved provider may supply device for use in education and care service
175D Requirement to use service-supplied device in education and care service (other than family day care service)
175F Offences relating to capturing, storing or transmitting images of children
Related Policies
Employee Code of Conduct Policy
Incident Management Policy
Media policy
Managing for Performance Policy

Safeguarding Children and Young People Policy	
Whistleblower Policy	
Child Safe Environment Policy	
Related Procedures	
01P001 Programming Guidelines	
01P002 Holiday Program and Pupil Free Day Planning Procedures	
01P003 Safe Use of Technology, Devices and Internet Procedure	
02PO16 Images and Videos of Children Procedure	
Requesting Access to Personal Devices Procedure	
Other	
Quality Area 1, 5 & 6: Standards 1.1, 1.2, 5.1, 5.2, 6.1	
Technology Agreement	
Personal Device Access Form	
Personal Device Approval Register	
Office of Children’s Guardian Guide to Child Safety Standards	
Education and Care Services (Supply, Authorisation and Use of Devices) Order 2025	
Version	4.2
Change History	JAG Policy Change Register
Date Approved	22.04.2026
Date Implemented	29.04.2026
Document Owner	Quality Service Development
Document Approvers	CEO / Approved Provider
Next Review	12 Months