

SAFE USE OF INFORMATION AND COMMUNICATION TECHNOLOGY POLICY

Best Practice – Quality Area 7

PURPOSE

The Information and Communication Technology (ICT) environment is continually changing. Services and the GRPSA office have access to a variety of technologies via fixed, wireless and mobile devices. While ICT is a cost-effective, timely and efficient tool for research, communication and management of a service, there are also legal responsibilities in relation to information privacy, security and the protection of employees, families and children.

State and federal laws, including those governing information privacy, restricted personal devices, copyright, occupational health and safety, anti-discrimination and sexual harassment, apply to the use of ICT. Illegal and inappropriate use of ICT resources includes pornography, fraud, defamation, breach of copyright, unlawful discrimination or vilification, harassment (including sexual harassment, stalking and privacy violations) and illegal activity, including illegal peer-to-peer file sharing.

GRPSA has adopted the National Model Code for taking images or videos of children while providing Early Childhood Education and Care to promote a child safe culture.

This policy should be read in conjunction with the following GRPSA policies:

- *Child Safety and Wellbeing Policy*
- *Children's use of ICT Policy*
- *Code of Conduct Policy*
- *Educational Program and Practice Policy*
- *Privacy and Confidentiality Policy*
- *Supervision of Children Policy*

POLICY STATEMENT

VALUES

Goulburn Region Preschool Association Inc is committed to:

- Professional, ethical, and responsible use of ICT
- Providing a safe workplace for management, educators, staff, and others using the service's ICT facilities
- Safeguarding the privacy and confidentiality of information received, transmitted, or stored electronically.
- Ensuring that the use of the service's ICT facilities complies with all service policies and relevant government legislation.
- Providing management, educators and staff with online information, resources, and communication tools to support the effective operation of the service.

Staff initials: _____ Date: _____

SCOPE

This policy applies to the Approved Provider, Nominated Supervisors, educators, staff, students on placement and volunteers at Inc. Services. This policy does **not** apply to children. (*refer to Children's Use of ICT policy*).

This policy applies to all aspects of the use of ICT including:

- artificial intelligence (AI)
- internet usage
- electronic mail (email)
- electronic bulletins/notice boards
- electronic discussion/news groups
- weblogs (blogs) – refer to *Definitions*
- social networking (including but not limited to Facebook, X, Instagram, WhatsApp, Snapchat, TikTok, LinkedIn, Pinterest)
- file transfer
- file storage
- file sharing
- video conferencing
- streaming media
- instant messaging
- online discussion groups and chat facilities
- subscriptions to list servers, mailing lists or other like services
- copying, saving or distributing files
- viewing material electronically
- printing material
- portable communication devices including mobile and cordless phones.
- cameras and/or photo taking and videoing devices.

PROCEDURES

The Approved Provider is responsible for:

- Ensuring that paramount consideration is applied in all decisions and actions related to the operation and delivery of education and care services that consistently prioritise children's safety, rights and best interests above all other considerations.
- Ensuring that the use of the service's ICT complies with all relevant state and federal legislation (refer to *Legislation and standards*), and all service policies (including *Privacy and Confidentiality Policy* and *Code of Conduct Policy*).
- Authorising the access of educators, staff, volunteers, and students to the service's ICT facilities, as appropriate.
- Providing clear procedures and protocols that outline the parameters for use of the service's ICT facilities (refer to Attachment 1 - Service Device Agreement for Educators and Approved Provider Staff)
- Issuing GRPSA devices to services to be used in educational programs and documentation to take photos, videos and audio of children; recording digital information including but not limited to observations, transition statements, referrals, assessments, family details on GRPSA issued devices.

Staff initials: _____ Date: _____

- Authorising Child Link users for each GRPSA location and ensuring the access is current.
- Ensuring staff are informed of their obligations under the National Law, Devices in Education and Care Services, Part 6A, 175A – 175J.
- Embedding the National Model Code to promote a child safe culture when it comes to taking, sharing and storing images or videos of children in early childhood education and care.
- Complying with the Child Information Sharing Scheme (CISS) and Family Violence Information Sharing Scheme (FVISS) when considering whether and what information about a child can be shared with other organisations.
- Embedding a culture of awareness and understanding of security issues at the service (refer to Attachment 1 - Guidelines for all social media and networking platforms)
- Ensuring that effective financial procedures and security measures are implemented where transactions are made using the service's ICT facilities, e.g. handling fee and invoice payments, and using online banking.
- Ensuring that the service's computer software and hardware are purchased from an appropriate and reputable supplier.
- Identifying the need for additional password-protected email accounts for management, educators, staff, and others at the service, and providing these as appropriate
- Identifying the training needs of educators and staff in relation to ICT, and providing recommendations for the inclusion of training in ICT in professional development activities
- Ensuring that procedures are in place (use of cloud-based storage) for the regular backup of critical data and information at the service.
- Ensuring secure storage of all information at the service, including backup files (refer to *Privacy and Confidentiality Policy*).
- Adhering to the requirements of the *Privacy and Confidentiality Policy* in relation to accessing information on the service issued devices, including emails.
- Considering encryption of data for extra security.
- Ensuring that reputable anti-virus and firewall software are installed on service computers, and that software is kept up to date.
- Developing procedures to minimise unauthorised access, use and disclosure of information and data, which may include limiting access and passwords, and encryption.
- Ensuring that the service's liability in the event of security breaches, or unauthorised access, use and disclosure of information and data is limited by developing and publishing appropriate disclaimers.
- Developing procedures to ensure data and information (e.g. passwords) are kept secure, and only disclosed to individuals where necessary e.g. to new educators and staff.
- Developing procedures to ensure that all educators, staff, volunteers, and students are aware of the requirements of this policy.
- Ensuring that no information is stored on endpoint data storage devices or stored on a backup drive.
- Ensuring compliance with this policy by all users of the service's ICT facilities.
- Developing and maintaining the GRPSA website and social media pages.
- Ensuring that written permission is provided by parents/guardians for authorised access to the service's computer systems and internet by persons under 18 years of age (e.g. a student on placement at the service) (refer to Attachment 4)

Staff initials: _____ Date: _____

All Early Childhood Staff are responsible for:

- Ensuring that paramount consideration is applied in all decisions and actions related to the operation and delivery of education and care services that consistently prioritise children's safety, rights and best interests above all other considerations.
- Complying with all relevant legislation and service policies, protocols and procedures, including those outlined in Attachments 1, 2 and 3.
- Using GRPSA issued devices in educational programs and documentation to take photos, videos and audio of children; recording digital information including but not limited to observations, transition statements, referrals, assessments, family details.
- Accessing Child Link via GRPSA issued devices and only accessed by Child Link authorised users.
- Adhering to the National Law, Devices in Education and Care Services, Part 6A, 175A – 175J.
- Adhering to the National Model Code to promote a child safe culture when it comes to taking, sharing and storing images or videos of children in early childhood education and care.
- Complying with the guidelines for the Child Information Sharing Scheme (CISS) and Family Violence Information Sharing Scheme (FVISS) when considering whether and what information about a child can be shared with other organisations.
- Keeping allocated passwords secure, including not sharing passwords and logging off after using a computer.
- Maintaining the security of ICT devices.
- Accessing accounts, data, or files on the service's computers only where authorisation has been provided.
- Co-operating with other users of the service's ICT to ensure fair and equitable access to resources.
- Ensuring confidential information is transmitted with password protection or encryption, as required.
- Ensuring no illegal material is transmitted at any time via any ICT medium.
- Using the service's email, messaging, and social media facilities for service-related and lawful activities only
- Ensuring that no endpoint data storage devices such as USB devices and hard drives are used.
- Not using personal mobile phones or other personal devices (including smart watches) during work time while engaging directly with children, other than on rostered breaks, unless written authorisation has been given by EC Managers (or through another means if written authorisation is not reasonably practicable).
- Gaining a written authorisation from EC Managers if use of restricted devices for essential purposes is required.
- Essential purposes for which use and / or possession of a personal electronic device may be authorised for purposes other than taking images or recording videos of children include:
 - Communication in an emergency situation involving a lost child, injury to child or staff member, or other serious incident, or in the case of a lockdown or evacuation of the service premises
 - 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

Staff initials: _____ Date: _____

- 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
- Any other instance that is deemed as an essential purpose by EC Managers (such as offsite excursions).
- Never using a personal electronic device to photograph children, ~~or~~ record audio or visual images of children for any purpose, or receive transferred data from a service issued device, including to document children's learning.
- Deleting photos, videos and audio of children off GRPSA issued devices after 12 months.
- Ensuring electronic files containing information about children and families are kept secure at all times (refer to *Privacy and Confidentiality Policy*).
- Notifying the approved provider of any damage, faults or loss of service issued devices.
- Signing an acknowledgement form upon receipt of a service issued laptop (refer to attachment 3 – Authorised user agreement for GRPSA Laptops)
- Ensuring families, volunteers, students, visitors and contractors do not take photos, videos or audio of other children or staff at the service.
- Maintaining professional respectful relationships with parents/guardians.
- Completing the authorised user agreement form if under 18 years of age (students/trainees). (refer to attachment 4 – Authorisation for underage access to GRPSA ICT facilities – Students/Trainees)

Breaches of this policy

- Ensuring that paramount consideration is applied in all decisions and actions related to the delivery of education and care services that consistently prioritise children's safety, rights and best interests above all other considerations.
- Individuals who use restricted personal devices and/or service issued devices for unlawful purposes may be liable to criminal or civil legal action. This could result in serious consequences, such as a fine, damages and/or costs being awarded against the individual, or imprisonment. GRPSA will not defend or support any individual using an unauthorised restricted personal device and/or service-issued devices for an unlawful purpose.
- If GRPSA determines that a potential breach of this policy has occurred, an investigation will be conducted.
- If an investigation is conducted due to a potential breach of this policy, specific directives may be issued to those involved in the investigation, including but not limited to: being stood down with pay, or placing restricted personal devices in an allocated secure location whilst working directly with children.
- GRPSA will report to external authorities as required under Law and Regulations.
- Individuals who fail to adhere to this policy may have their access to the service's ICT facilities restricted/denied and/or be liable to counselling, disciplinary action or dismissal.
- GRPSA may block access to internet sites where inappropriate use is identified.
- Management, educators, staff, volunteers, and students who fail to adhere to this policy may have their access to the service's ICT facilities restricted/denied.
- Termination of employment in cases of serious or repeated misconduct.

Staff initials: _____ Date: _____

Parents/guardians are responsible for:

- Reading and understanding this *Information and Communication Technology (ICT) Policy*.
- Complying with all state and federal laws, the requirements of the Education and Care Services National Regulations 2011, and all service policies and procedures.
- Maintaining the privacy of any personal or health information provided to them about other individuals.
- Not contacting GRPSA staff regarding work matters via personal means, such as personal social media, messaging apps and personal phone numbers.
- Responsible and respectful use of social networking when referring to any Goulburn Region Preschool Association Inc Service or staff member or associated service.
- Ensuring they do not take photos, videos or audio of children, staff, students, volunteers, visitors and contractors.
- Respecting the privacy of families by ensuring photos of children viewed on online learning platforms (Xplor) are not distributed, and photos/videos are only shared of the family's own child/children.
- Not posting defamatory comments about GRPSA, GRPSA employees or the Victorian Department of Education on any online platforms, including social media.
- Signing enrolment form – regarding arrangements for photos and videos as explained on the enrolment form.

Volunteers and students, while at the service, are responsible for following this policy and its procedures.

EVALUATION

In order to assess whether the values and purposes of the policy have been achieved, the Approved Provider will:

- Regularly seek feedback from everyone affected by the policy regarding its effectiveness.
- Monitor the implementation, compliance, complaints, and incidents in relation to this policy.
- Keep the policy up to date with current legislation, research, policy, and best practice.
- Revise the policy and procedures as part of the service's policy review cycle, or as required.
- Require all staff to read, initial and sign each page of this policy when reviewed or onboarded, and send a completed copy to the Approved Provider.
- Notify parents/guardians at least 14 days before making any changes to this policy or its procedures.

Staff initials: _____ Date: _____

ATTACHMENTS

- Attachment 1: Guidelines for all social media and networking platforms
- Attachment 2: Service Device Agreement for all Staff
- Attachment 3: Authorised User Agreement for GRPSA Laptops and iPads
- Attachment 4: Parent/guardian authorisation for under-age (under 18) access (students/trainees) to the Goulburn Region Preschool Association Inc ICT facilities – (service issued devices)

AUTHORISATION

This policy was adopted by Goulburn Region Preschool Association Inc. on 12th November 2012

Reviewed and updated: 27th November 2017

Reviewed and updated: May 2019

Reviewed and updated: August 2021

Reviewed and approved: July 2025

Reviewed and approved: August 2026

REVIEW DATE: AUGUST 2028

ACKNOWLEDGEMENT OF READING THE SAFE USE OF INFORMATION AND COMMUNICATION TECHNOLOGY POLICY

I, _____ (name), have reviewed and read the
Safe Use of Information and Communication Policy.

Signature: _____ Date: _____

ATTACHMENT 1

Guidelines for all social media and networking platforms

Maintain confidentiality –Don't disclose or discuss confidential information, make commitments, or engage in activities on behalf of GRPSA unless you are authorised to do so.

Be professional –when engaging in social media and networking platforms.

Protect and respect privacy –Always protect your own privacy and personal information, and don't share the private details of others. Don't disclose details of private conversations unless you have obtained explicit consent from the relevant parties.

Be impartial – Avoid statements that advocate or criticise policies of GRPSA, external organisations, government, or political parties. Avoid conflicts of interest through endorsement or criticism of third-party providers, partners, products, or services.

Be respectful – Be courteous and polite, and sensitive to diversity. Avoid arguments and don't make personal attacks. Do not post obscene, defamatory, threatening, harassing, discriminatory or hateful content.

Be accurate – Make sure the information you publish is correct and cite sources where appropriate – people may make decisions based on information you post.

Accountability – Always take responsibility for your actions. If you make a mistake, admit it, and where possible make public corrections in consultation with management.

Correct processes – Use the appropriate processes and follow policies for resolving complaints regarding your employment. Don't use social media to publicly complain about your employment.

Think first – Review your content before you post it. Remember that you are responsible for your actions. You should consider the impact your activities could have on yourself and/or GRPSA. Use your common sense and best judgement. If you're not sure, check with management.

If in doubt, leave it out.

I, _____ have read the Goulburn Region Preschool Association Inc Safe Use of *Information and Communication Technology (ICT) Policy* and agree to the conditions of use of the service's ICT facilities.

Signature (staff)

Date

ATTACHMENT 2

Service Device Agreement for all Staff

GRPSA Electronic Device Use Agreement

This agreement outlines the responsibilities and expectations for all staff regarding the use of service issued electronic devices, including but not limited to mobile phones, tablets/iPads, laptops, desktop computers, digital cameras, and smartboards/smart TV's or any other electronic device not otherwise identified.

1. Purpose

This agreement ensures that all staff employed by GRPSA utilise service issued devices in a manner that upholds child safety, maintains professional integrity, and complies with GRPSA policies and procedures, including legislative and regulatory obligations.

2. Scope

This agreement applies to all staff members employed by GRPSA who have access to or use any service-provided electronic devices.

3. Legislative and Policy References

Staff agree to comply with the following, where applicable:

- Education and Care Services National Law and Regulations (2011)
- National Quality Framework (NQF)
- National Quality Standard (NQS) – particularly Quality Areas 2 (Children's Health and Safety), 4 (Staffing Arrangements), 5 (Relationships with Children), and 7 (Governance and Leadership)
- Child Protection Legislation and GRPSA's Child Safety and Wellbeing Policy
- Child Safe Standards
- National Model Code of Conduct for Taking Images and Videos of Children
- GRPSA's Policies as listed below:
 - Child Safety and Wellbeing Policy
 - Children's Use of ICT Policy
 - Code of Conduct Policy
 - Educational Program and Practice Policy
 - Privacy and Confidentiality Policy
 - Safe Use of Information and Communication Technology Policy
 - Supervision of Children Policy.

4. Appropriate Use of Service Devices

Staff agree to:

- Use service issued devices strictly for educational, communication, documentation, or administrative purposes as per job responsibilities.
- Follow all policies regarding photography, video, and audio recordings of children, ensuring consent procedures are followed and child privacy is maintained.

- Immediately report any device malfunction, loss, or suspected data breach to the Approved Provider.
- Store and use devices in a secure and safe manner, ensuring they are not accessible to children unless part of supervised activities.
- Not use personal accounts or apps to store or transmit sensitive information, images, or records related to children or the service.

Staff must not:

- Use the ICT facilities to make any personal communication that could suggest that such communication was made in that person's official capacity as an employee or volunteer of Goulburn Region Preschool Association Inc.
- Use service issued devices for anything other than work related purposes.
- Assist any election campaign.
- Lobby any government organisation without prior GRPSA approval.
- Conduct any outside business or engage in activities related to employment with another organisation.

5. Emails on Service Devices

Staff agree to:

- Always include a subject description in the subject line.
- Check the content of emails, attachments and email addresses before sending.
- Check before sending – ensuring content is respectful, professional and accurate.
- Exercise care to avoid inappropriate disclosure of email addresses to a whole group of recipients, using blind copying (BCC) when sending emails to multiple recipients.
- Ensure confidential information and documents are sent to their intended recipients.
- Be cautious about opening files or launching programs that have been received as an attachment via email from the email itself.
- Never open emails if unsure of the sender.
- Check email accounts on a regular basis and forward relevant emails to the Approved Provider or relevant staff member.
- Remove correspondence that is no longer required from the computer regularly.
- Respond to emails as soon as is practicable.
- 'Reply all' when there are multiple recipients in the original email.

Staff must not:

- Create, copy, transmit or retransmit chain emails or other unauthorised mass communication.
- Exchange any confidential or sensitive information held by Goulburn Region Preschool Association Inc unless authorised as part of their duties.

6. Information stored on Service Issued Computers/Electronic Devices

Staff agree to:

- Ensure computer records containing personal, sensitive and/or health information, or photographs of children are stored securely so that privacy and confidentiality is maintained. This information must not be removed from the service without authorisation, as security of the information could be at risk (refer to *Privacy and Confidentiality Policy*).
- That if management authorisation is given for removing computer records containing personal, sensitive and/or health information, or photographs of children; staff must ensure that the information is transported, handled, and stored securely so that privacy and confidentiality is always maintained.
- Not view or interfere with other users' files without permission.

7. Prohibited Use

Staff must not:

- Use service issued devices for personal social media, personal streaming or personal entertainment.
- Create or exchange messages that are offensive, harassing, obscene or threatening.
- Use devices in a way that compromises child safety, breaches confidentiality, or violates professional boundaries.
- Download, share, or store inappropriate, offensive, or unauthorised content.
- Take or share images or videos of children outside of approved platforms or without written parental consent.
- Use artificial intelligence (AI) to upload or generate photos of children as part of observational documentation.
- Use artificial intelligence (AI) to generate text relating to children's learning and development.
- Allow unauthorised persons to use service issued devices.
- Carry out activities that are illegal, inappropriate, or offensive to fellow employees or the public. Such activities include, but are not limited to, hate speech or material that ridicules/discriminates against others on the basis of race, nationality, creed, religion, ability/disability, gender or sexual orientation.
- Use the ICT facilities as a platform to gain unauthorised access to other systems.
- Use the ICT facilities to access, download, create, store, or distribute illegal, offensive, obscene, or objectionable material (including pornography and sexually explicit material). It will not be a defence to claim that the recipient was a consenting adult.
- Use the service's or personal GRPSA email address relating to 'private' matter.
- Harass, slander, intimidate, embarrass, defame, vilify, seek to offend, or make threats against another person or group of people.
- Breach copyright laws through making copies of, or transmitting, material or commercial software.

8. Child Safety and Protection

Staff acknowledge that:

- Any misuse of electronic devices that places a child at risk or breaches safeguarding protocols will be treated as a serious breach of professional conduct and potential breach of Law.
- They have a mandatory obligation to report suspected child abuse or inappropriate conduct in accordance with GRPSA's *Child Safety and Wellbeing Policy* and State/Federal legislation.

9. Breach of Agreement

Any breach of this agreement may result in:

- Individuals who use restricted personal devices and/or service issued devices for unlawful purposes may be liable to criminal or civil legal action. This could result in serious consequences, such as a fine, damages and/or costs being awarded against the individual, or imprisonment. GRPSA will not defend or support any individual using an unauthorised restricted personal device and/or service-issued devices for an unlawful purpose.
- If GRPSA determines that a potential breach of this policy has occurred, an investigation will be conducted.
- If an investigation is conducted due to a potential breach of this policy, specific directives may be issued to those involved in the investigation, including but not limited to: being stood down with pay, or placing restricted personal devices in an allocated secure location whilst working directly with children.
- GRPSA will report to external authorities as required under the Law and Regulations.
- Individuals who fail to adhere to this policy may have their access to the service's ICT facilities restricted/denied and/or be liable to counselling, disciplinary action or dismissal.
- GRPSA may block access to internet sites where inappropriate use is identified.
- Management, educators, staff, volunteers, and students who fail to adhere to this policy may have their access to the service's ICT facilities restricted/denied.
- Termination of employment in cases of serious or repeated misconduct.

10. Acknowledgement

I, _____ the undersigned, have read, understood, and agree to comply with the terms outlined in this Service Device Agreement. I understand that my use of service devices is subject to ongoing monitoring and review and that any breach may result in disciplinary action or termination of employment.

Signature

Date

ATTACHMENT 3

Authorised User Agreement for GRPSA Laptops and iPads

I, _____ ,

- Acknowledge that I have received a device belonging to GRPSA
- Will ensure that the device:
 - is used for work-related purposes only
 - is password protected at all times
 - will not be loaned to unauthorised persons
 - will be returned to GRPSA on cessation of employment.
- Will notify the approved provider as soon as practicable if the device is damaged, faulty or lost
- Have read the Goulburn Region Preschool Association Inc Safe Use of *Information and Communication Technology (ICT) Policy* and agree to the procedures and the conditions of use of the service's ICT facilities

Signature

Date

ATTACHMENT 4

**Parent/guardian authorisation for under-age (under 18) access (students/trainees) to the
Goulburn Region Preschool Association Inc ICT facilities (service issued devices)**

Student's name: _____

Date of placement: _____

I, _____ , am a parent/guardian of

I have read the Goulburn Region Preschool Association Inc *Information and Communication Technology (ICT) Policy* and agree to the conditions of use of the service's ICT facilities for the above-named student.

I also understand that Goulburn Region Preschool Association Inc provides no censorship of access to ICT facilities.

Signature (student)

Date

Signature (parent/guardian)

Date