

ICT Acceptable Use Policy – Students



Purpose

This policy exists to ensure that students use Gleeson College ICT infrastructure, systems, and internet access responsibly, safely, and in a manner that supports their learning.

Scope

This policy applies to all Gleeson College students accessing ICT systems, services, devices, or networks at school or via remote access.

Definitions

ICT (Information and Communication Technology): All College-provided or authorised digital systems, including networks, devices, applications, internet access, and data storage services.

User: Any student who has been granted access to and uses Gleeson College ICT systems, devices, or network services.

Network: The College's digital communication infrastructure, including internet access, servers, and connected systems used for teaching and learning.

Personal Information: Any information that can identify an individual, such as name, address, phone number, email address, or date of birth.

Unauthorised Access: Accessing systems, accounts, or data without permission, including attempting to bypass security measures or use another user's credentials.

Malware: Malicious software designed to disrupt, damage, or gain unauthorised access to systems, including viruses, ransomware, and similar threats.

Monitoring and Logging: The recording and review of network activity and system usage to support security, compliance, and operational management.

Policy

Context

Effective and responsible use of ICT supports Gleeson College's vision of being a faith-filled community where individuals develop and use their talents in service to others. This policy promotes a safe, supportive and respectful digital environment aligned with the College mission.

It reflects the Gleeson 10 values, particularly **Dignity and Respect**, **Truth**, and **Justice**, by guiding appropriate behaviour, integrity, and responsibility in all digital interactions.

Guiding Principles

- ICT access is provided to support learning and educational outcomes.
- Students are expected to act responsibly, ethically, and respectfully when using ICT.
- The College prioritises safety, security, and wellbeing in all digital environments.
- ICT usage is monitored to ensure compliance with College expectations.

Policy Statement

Acceptable Use

- ICT resources are to be used for educational purposes only.
- Recreational use of the network is not permitted.
- Students must comply with College behavioural expectations when using ICT.

User Responsibility and Conduct

- Students must not share personal contact information without parental approval.
- Students must not arrange to meet individuals encountered online without parental consent.
- Students must report any harassment, threatening communication, or unsafe content to staff immediately.
- Students must not use offensive, discriminatory, or inappropriate language.
- Students must not engage in harassment or distribute false or defamatory information.

System Security

- Students are responsible for safeguarding their account credentials.
- Passwords must not be shared or recorded in accessible ways.
- Any suspected security breach must be reported immediately.

- External storage devices must be scanned for malware before use.
- Students must not:
 - Attempt unauthorised access to systems or data
 - Introduce malware, ransomware, or viruses
 - Use VPNs or bypass filtering/security controls
 - Interfere with ICT infrastructure or systems
 - Engage in illegal or inappropriate activities

Privacy and Data Use

- ICT systems must be used only for educational purposes.
- Students are expected to manage their OneDrive storage responsibly.
- Chain emails and spam are not permitted.
- Only relevant academic forums or subscriptions should be used.

Plagiarism and Copyright

- Students must not plagiarise content.
- Copyright laws must be respected.
- Permission should be sought when reusing copyrighted materials where required.

Access to Inappropriate Material

- Accessing inappropriate, illegal, or harmful material is strictly prohibited.
- Any accidental exposure must be reported immediately to a teacher.

Monitoring and Compliance

- Network activity is logged and monitored for security, compliance, and operational purposes.
- Gleeson College reserves the right to access data and communications on its systems to ensure appropriate use.

Consequences

- Parents/caregivers will be notified of policy breaches.
- Students may lose network access privileges.
- Repeated or serious breaches may lead to further disciplinary action.
- Police involvement may occur where appropriate.

Liability

Gleeson College does not guarantee uninterrupted or error-free ICT services and is not liable for:

- Data loss
- Service interruptions
- Accuracy or quality of accessed information
- Financial obligations incurred through ICT use

Roles and responsibilities

Students will:

- Use ICT resources responsibly and for educational purposes
- Follow all security and behavioural expectations
- Report issues, risks, or concerns promptly

The College will:

- Provide secure and monitored ICT systems
- Maintain appropriate safeguards and filtering
- Enforce policy compliance and respond to breaches

Basis of Discretion

The Principal or delegate may apply discretion in enforcing this policy where circumstances require, in the best interests of the student and College community.

Supporting Policies & Procedures

- [BYOD Code of Conduct](#)
- [Cyber Safety Guidelines](#)
- [CESA Cloud Computing Policy](#)