

DRAFT: ICT Acceptable Use Policy

Document Control Information

Reviewed by SMT:	May 2026
Date of Next Review:	June 2029 – TBC
Approved by the Finance and Resources Committee:	May 2026 – TBC

The Board of Management (or any person/group with delegated authority from the Board) reserves the right to amend this document at any time should the need arise following consultation with employee representatives. This Policy has been subject to an Equality Impact Assessment, which is published on our website: [Policies and Reports - Glasgow Kelvin College](#).

Contents

1. Purpose.....	1
2. Relationship to Other Policies and Frameworks	1
3. Scope.....	1
4. Principles of Acceptable Use	2
5. Accounts, Identity and Access	2
6. Devices, Remote Working and BYOD	2
7. Information Security and Data Protection.....	3
8. Monitoring and Privacy	3
9. Unacceptable Use.....	3
10. Use of Artificial Intelligence (AI)	4
10.1 General Principles.....	4
10.2 Staff Use of AI	4
10.3 Student Use of AI	5
10.4 Assistive Technologies.....	5
11. Approved Services and External Platforms.....	5
12. Reporting Concerns and Incidents.....	5
13. Compliance and Enforcement.....	5
14. Review	6

1. Purpose

This ICT Acceptable Use Policy (AUP) sets out the expectations for how Glasgow Kelvin College's ICT systems, digital services and data must be used by staff, students, partners and other authorised users. The policy defines acceptable and unacceptable use, supports a secure and trustworthy digital environment, and ensures that technology is used responsibly, lawfully and in a way that protects the College, its community and its information assets.

This policy is deliberately principles-based. It establishes what is expected of users, while detailed technical controls and procedures are defined elsewhere.

2. Relationship to Other Policies and Frameworks

This policy forms part of the College's Information Security Management System and should be read alongside other [policies](#), including but not limited to:

- Information Security Framework (governance, roles, risk and assurance)
- ICT Security Policy (technical security principles and controls)
- Data Protection Policy and associated privacy notices
- ICT Incident Response Procedure
- Code of Learner Behaviour and Staff Disciplinary Procedures
- Dignity and Respect Policy and Equality and Diversity Policy
- Social Media Procedures
- Artificial Intelligence guidance for staff and students
- JANET / Jisc Acceptable Use Policy (as the College's internet connectivity is provided via the JANET network)

All use of the internet and external network services via College systems must comply with the Jisc Acceptable Use Policy. Jisc is the UK body that provides and manages JANET, the network used by the College for internet connectivity. Where Jisc requirements impose additional restrictions, those requirements apply.

This policy supports the College's cyber resilience objectives, including user behaviour and awareness expectations aligned with national guidance issued by the National Cyber Security Centre (NCSC).

3. Scope

This policy applies to all users of College ICT systems and services, including:

- Staff, students, Board members and volunteers
- Contractors, partners and third-party users with authorised access
- It applies to the use of ICT resources:
 - On College premises
 - Remotely (including home working)
 - Via College-approved cloud services (such as Microsoft 365)

- Using College-owned or authorised personal devices (also known as Bring Your Own Device or BYOD)

4. Principles of Acceptable Use

Users of College ICT resources must:

- Use systems only for authorised purposes related to learning, teaching, research or College business
- Act lawfully, ethically and professionally
- Protect the confidentiality, integrity and availability of College information
- Respect the rights, privacy and dignity of others
- Safeguard their accounts and devices from misuse or compromise
- ensure that their use of digital systems, including email, messaging and social media, reflects professional standards and does not bring the College into disrepute

Reasonable personal use is permitted provided it does not interfere with College operations, breach policy or law, or introduce additional risk.

5. Accounts, Identity and Access

- Users must only access information, systems and services they are authorised to use
- User credentials such as passwords, multi-factor authentication tokens, devices, must be kept secure and never shared
- Multi-factor authentication must be used where required
- Accounts will be suspended or disabled when no longer required, including at the end of employment or study

Users must not attempt to gain unauthorised access to systems, elevate privileges, or bypass security or identity controls.

6. Devices, Remote Working and BYOD

ICT systems may be accessed only using devices that meet College security requirements.

Users must:

- Keep devices up to date with security patches and updates
- Ensure appropriate malware protection is in place where required
- Report the loss or theft of any device used to access College systems immediately

- Use secure network connections when working remotely

Personal devices may be permitted for limited access where approved, but users must not assume the same level of access or support as College-owned devices. Personal devices are subject to proportionate security controls and investigation only insofar as they are used to access College systems or data, in accordance with law and College policies.

Where personal or unmanaged devices do not meet College security criteria, they will be subject to stricter technical controls which may result in reduced, limited or no access to College systems and services.

7. Information Security and Data Protection

Users have a personal responsibility to protect College information and data, including personal and sensitive data.

Users must not:

- Copy, store or transmit College information in unauthorised ways
- Remove data protection or security safeguards
- Disclose confidential information to unauthorised individuals or services

All suspected or actual data breaches or security incidents must be reported promptly in line with College procedures.

8. Monitoring and Privacy

The College monitors ICT systems and networks to:

- Protect systems and users
- Detect and investigate misuse or security incidents
- Meet legal, regulatory and contractual obligations

Monitoring is proportionate, authorised and subject to the College's privacy notices and data retention schedules. User content is not routinely inspected without due cause.

Where required for the investigation of security incidents or misuse, the College may take proportionate and lawful steps to preserve, analyse or restrict access to systems or data.

9. Unacceptable Use

Examples of unacceptable use include (but are not limited to):

- Circumventing security controls, filtering or monitoring
- Installing unauthorised software or hardware

- Creating, accessing or distributing illegal, offensive or harmful content
- Harassment, bullying, intimidation or discrimination
- Using College systems for fraud, deception or criminal activity
- Running non-College businesses or unauthorised commercial activity

Misuse may result in disciplinary action and, where appropriate, referral to external authorities.

10. Use of Artificial Intelligence (AI)

10.1 General Principles

The College supports the responsible use of Artificial Intelligence (AI) to enhance learning, teaching, research and business operations, while managing associated risks.

The College does not mandate the exclusive use of any single AI platform, but requires that all AI use complies with data protection, security and acceptable use requirements.

The use of AI does not replace or override existing obligations relating to confidentiality, data protection, academic integrity, intellectual property, or professional conduct. Users remain responsible and accountable for the accuracy, appropriateness and lawful use of any content generated using AI.

10.2 Staff Use of AI

Staff may use AI tools to support College business where appropriate. This includes College-approved tools (such as Microsoft 365 Copilot) as well as other AI services, subject to the requirements below. Staff must ensure that:

- They are authorised to access and use any information provided to an AI tool
- AI tools are used in a secure and responsible manner, aligned with College policies and guidance
- Outputs are reviewed and validated, particularly where used in decision-making or formal communications

Staff must not input College confidential, sensitive or personal data into public or consumer AI services (such as ChatGPT, Claude, Grok or similar tools). The use of such data is only permitted within College-approved, controlled AI services where data protection, security, and contractual safeguards are in place.

Where AI tools are accessed through College-controlled services (for example, where users are signed in with their College account and data is protected within that service), staff may use these tools in line with their authorised access and responsibilities.

If staff are unsure whether a particular AI tool or use case is appropriate, they must seek advice from Digital Services (ICT) before use.

Staff must follow College guidance on the safe and ethical use of AI and exercise professional judgement at all times.

10.3 Student Use of AI

Students may use AI as a learning support tool where appropriate and permitted. However:

- AI must not be used to generate assessment content unless explicitly permitted
- Misuse of AI in assessment may constitute plagiarism or academic misconduct
- Students are responsible for understanding and complying with College assessment and AI guidance

10.4 Assistive Technologies

The College recognises that assistive technologies, including AI-enabled tools, may be used to support accessibility and learning needs. Approved arrangements will be communicated through learner support services and do not constitute academic misconduct when used appropriately.

11. Approved Services and External Platforms

College business and learning activities must be conducted using College-approved platforms and services. Users must not transfer College data to unapproved systems or services without explicit authorisation.

12. Reporting Concerns and Incidents

Prompt reporting helps the College support users, protect systems and respond quickly to issues. All users must report:

- Suspected security incidents
- Data breaches
- Loss or theft of devices
- Misuse of ICT systems

Reports should be made promptly via the ICT Service Desk or designated reporting channels.

13. Compliance and Enforcement

Compliance with this policy is mandatory for all users of College ICT systems and services. Failure to comply with this policy may result in action under the relevant College procedures, including staff disciplinary procedures, the learner behaviour policy, partner or contractual agreements, and where appropriate, referral to external authorities.

14. Review

This policy will be reviewed at least every three years, or sooner where there are significant changes to technology, legislation or risk.