Glasgow Kelvin College

ICT Acceptable Use Policy

Document Control Information	
Reviewed by SMT:	January 2023
Date of Next Review:	June 2026
Approved by the Finance and Resources Committee:	February 2023

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: https://www.glasgowkelvin.ac.uk/equality-diversity/

Contents

1. Introduction and Scope

The aim of the Glasgow Kelvin College Acceptable Use Policy (AUP) is to reflect the established culture of openness, trust and integrity. The purpose of this policy is to outline the acceptable (and prohibited) use of College computer equipment and network access. Inappropriate use exposes the College to a range of risks including virus attacks, compromise of network systems and services, and legal issues. This policy also prohibits accessing College ICT facilities to cause harm or offense to others.

The policy covers all users including staff, students, partners and guests of the College ICT resources.

The policy is intended to protect users and their data, and the College as a whole from illegal or damaging actions by individuals, either knowingly or unknowingly. Inappropriate use by individuals will be managed in accordance with College policies and procedures, including the Disciplinary Policy and the Code of Student Behaviour. It will also be reported to law enforcement agencies if appropriate.

All internet access originating from the College network is subject to the JANET Acceptable Use Policy:

https://community.jisc.ac.uk/library/acceptable-use-policy

Any breach of the JANET AUP will be deemed a breach of the College AUP.

The policy will be reviewed at least every three years or when required by modifications to the regulatory frameworks or when, in the option of the College management or the Board's Auditors, there is any signification change in the structural, legislative, or operational aspects affecting the College.

2. Authorisation and Conditions of Use

2.1. Authorisation

Users are provided access to the College ICT Systems when they meet the following categories:

- members of staff;
- students; or
- partners of the College (i.e. learning network staff, individuals on work experience, contractors, auditors etc.)

Access will not be restricted on the grounds of disability, impairment or any other protected characteristic.

By logging on to a College system, whether on its premise or remotely, users are confirming acceptance of this policy by either clicking accept or ticking an acceptance button prior to logon.

When staff employment or a course of study finishes, access to ICT resources will be revoked automatically and the user accounts will be closed as per internal procedures.

2.2. Conditions of Use

ICT resources and Information Systems are provided primarily to support College business such as teaching, training, study and administrative support of these activities. However, reasonable personal use is also permitted provided there is compliance with this policy. Individuals should exercise due care and attention whilst using College ICT resources to ensure that the corporate reputation remains a priority and no inflammatory posts could be attributed to the College on either internal or external information systems or social media.

Users must not masquerade as someone else and should always keep their logon identity and password private (exceptions will be made for users who have additional support needs). Users should choose a hard to guess password, of which guidance can be found within the College password change procedure which is available from the Intranet.

Each user has a personal duty to follow the AUP as diligently as possible, in most cases the College will prefer to inform users of a contravention to the AUP informally while advising corrective action. However, repeated or a serious breach to the AUP will trigger disciplinary procedures.

The following acts can be construed as a misuse and a breach of the AUP:

- Installing software that is not explicitly permitted by the ICT Department;

- The printing, displaying, storing, internet browsing or transmitting of unacceptable or offensive material. This will include material which is:

    - racially, religiously, or sexually offensive;
    - contains profanity, is hateful, discriminatory, or anti-social;
    - obscene, indecent or pornographic; and
    - likely to promote terrorism or violence.

- The creation or transmission of material which is intentionally designed or likely to cause annoyance, inconvenience, intimidation or anxiety. This includes cyber- bullying or harassment in any form. Users should ensure that appropriate language and tone should be used in communications at all times in line with College policies and procedures;

- Intentionally affecting security systems or the disruption of network communications, including:

    - Intentionally clicking on known malicious links or running malicious software;
    - implementing a Denial of Service attack;
    - excessive or inappropriate use of College network bandwidth;
    - port scanning or information gathering (reconnaissance activity) of network systems exercises;
    - network monitoring/sniffing;
    - disclosing user logon information out with the College;
    - an attack that intentionally disrupts, prevents and/or removes access to computing services within the College or any external organisation; and
    - circumventing user authentication or security of any host, network or account.

- unauthorised copying, including downloading from the internet, of copyrighted material including, but not limited to, digitisation of photographs from magazines, books, music, applications or other copyrighted sources;

- utilising ‘proxies’ or VPN services to circumvent the College security systems;

- using computer resources to commit fraud, deception or other criminal act;

- vandalism of deliberate physical damage to College equipment;

- accessing another user’s account;

- impersonating another user whether real (via the user account) or artificial (via ‘doctored’ data). For example, sending messages that appear to originate from another person;

- sending chain or bulk (‘spam’) messages;

- use of College systems for commercial gain, running a business, non-College related advertising, crypto mining or political lobbying;

- using unauthorised or unlicensed applications including games, screensavers, drivers, browsers and plug-ins;

- adding hardware devices to the College network without explicit authorisation from the ICT Department;

- introducing viruses or malware (e.g. viruses, worms, Trojan horses, email bombs) designed to impact systems performance, integrity, security, availability of harvest data;

- breaching or attempting to breach security controls including:

    - interfering with or disabling anti-virus software;
    - attempting to change ‘safe search’ settings;
    - disabling Windows/Mac update services;
    - encrypting key College data/systems without authorisation and;
    - changing system policies which reduces security (firewalls, modifying logs, disabling encryption on managed devices, etc)

- any action, or lack of action, which may interfere with the security of College systems or a data breach of Personally Identifiable Information (PII) or sensitive data as per the Data Protection Act 2018 and the General Data Protection Regulations (GDPR);

- exporting, processing or transfer of other users’ PII or sensitive data outside of secure College systems; and

- contravening the JANET AUP (as referenced on page 3)

It is important that any personal data breaches, or indeed suspected breaches, across the College are reported as soon as possible to the Vice Principal, Curriculum and the Director of Corporate Services as per the College Data Breach procedure.

Under the terms of the Data Protection legislation, data controllers have no longer than 72 hours to report a breach to the Information Commissioner’s Office after having become aware of it. The College will abide by this statutory requirement.

2.3. Accessing Services or Data Remotely (or on-campus mobile devices)

The College provides a number of services (email, files, VLE, intranet, etc.) which can be accessed remotely or via guest WiFi services such as Eduroam. It should be noted that the Internet Protocol (IP), MAC address and browser version data may be recorded when using these systems. This means that location and device browser information can be harvested (see section 3.3 for monitoring activity).

The following requirements shall also apply to user remotely accessing services and data:

Applies to all users

- users shall only access any remote services using a device that continues to receive security updates from the vendor and ensure that security patches are applied within 14 days of release; and

- devices should have adequate and up-to-date anti-virus/malware software installed.

Applies to Staff and Partners only (not students)

- in line with the College Data Breach procedure it is important that individuals inform the ICT Services Desk immediately if a mobile device (whether College owned or personal) that has been used to access College data is lost or stolen. The ICT Service Desk will take steps to attempt to remotely wipe College data and apply measures to minimise the potential for data loss. The ICT Service Desk will notify the Vice Principal, Operations, the Director of Corporate Services or a member of the Privacy Network if a personal device containing data has been lost or stolen;

  GDPR - Policies and Procedures

- it is strongly recommended that mobile devices are encrypted and are protected with a pin of at least 8 digits;

- accessing College systems/data is not permitted on personal devices outside of the European Economic Area;

- any application used on a mobile device must be downloaded from either the Apple App or Google Play (no 'jailbroken' devices should be used);

- any devices accessing core or critical data/applications (HR data, Student Records, payroll) must be connected using a College encrypted laptop and Virtual Private network (VPN);

- if using a College owned mobile phone/tablet, the device must be enrolled in the Mobile Device Management system;

- individuals should use College assigned storage to store, transfer, process and access required data: USB storage is not permitted either remotely or on campus unless explicitly approved by the ICT Department; and

- PII data should never be sent outside of the College via email. If you need to send PII data external to the College then you must ensure:

    - There is a data sharing agreement in place,
    - The data file is suitably encrypted (i.e. using 7-zip with key [protection)
    - The data is shared and transferred using your OneDrive as per the following process – then unshared once the transfer has been completed.

2.4. Bring Your Own Device (BYOD)

The College provides staff with remote computing resource and controlled secure access to its services and information via organisationally owned, centrally managed and allocated mobile devices such as laptops, tablets and phones.

Personal devices for personal use should only be connected to the College EduRoam Wi-Fi network, where Internet access is permitted. For those wishing to access additional College services and information from a personal device, classified as BYOD (Bring Your Own Device), then there are a number of essential requirements that need to be met before this can be authorised.

Applies to Staff

- Devices must be registered with the College so that critical technical security aspects of the device can be managed to ensure the protection of College data and services;

- The device must meet the BYOD Technical Security Standard defined by the College;

- The device must be authorised for use with College services and data;

- Users obtaining a second-hand device shall ensure it is reset to its factory settings prior to the first access of college data. This is primarily to avoid exposure to malware;

- Users shall not store college information in a way that can be accessed by any other user of the personal device.

Applies to Students

- Whilst on campus, BYOD must not be connected to the College wired network and devices are only authorised to connect to the College EduRoam Wi-Fi network using a valid student username and password.

2.5. Internet of Things (IoT)

Devices that can be classified as Internet of Things (IoT) such as Smart TVs, wearable health monitors and home automation devices are not permitted on the College network without prior permission from the ICT department. Requests for connectivity should be made through the ICT Service Desk clearly describing the business use requirement. If approved, devices will only be permitted to connect to an authorised and secure Wi-Fi network, which will be facilitated by the ICT Department. Devices must meet the IoT Technical Security Standard.

3. Security and Data Protection

3.1. Filtering

The College utilises automated recording, filtering and monitoring software (Spam filter, URL filters, application filters, file auditing, administrative auditing software, etc.) to protect College systems, user data and other sensitive information. These cannot be guaranteed failsafe and users have a responsibility to be vigilant when using College systems and processing data.

Opening emails and browsing websites should always be carried out with diligence and care.

The College will filter and attempt to scan and block content or Internet activity which is deemed as being unsuitable or malicious, containing viruses or exploits. This includes pornographic, gambling and sites that provide a security threat.

The College appreciates the cooperation from users and promotes a reporting culture with regards to Cyber incidents. Users are asked to inform ICT if they receive a suspicious email or notice irregular activity on their devices. Email should be sent to **ictservicedesk@glasgowkelvin.ac.uk**

3.2. Cyber Security

Cyber-attacks are an increasing threat to organisations. The attacks are mostly initiated through the theft of user credentials (i.e. the hacking of a member of staff user account). Essentially attackers view people as being vulnerable and open to exploitation.

The College has taken steps to increase the understanding of staff around cyber security, which will ensure the College is better protected and that staff can better protect their personal digital identity outside of the College.

To mitigate these risks staff are required to complete the Workrite cyber awareness training module. This module is mandatory and staff will complete it on an annual basis. New entrants will be required to complete the module as part of their induction

process. This will help staff to understand threats better which assists them when working at the College and will also increase staff awareness in their personal online world.

The College has introduced Multi Factor Authentication (MFA) for remote access on all College staff accounts. Which provides a strong base for using MFA on personal accounts (i.e. Gmail, Facebook, Twitter and other social accounts).

Information relating to MFA will be routinely provided by the ICT Team. A short information clip to support staff using MFA is accessible at this College video.

3.3. Monitoring

While the College ICT department aims to provide a high level of privacy all users should be aware that the data they create on the College systems remains the property of the College. Glasgow Kelvin College reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy. Systems are monitored to ensure that the Confidentiality, Integrity and Availability of systems and data is maintained.

Users should be aware that data held within the College is not routinely inspected and user data will normally be treated as confidential. An examination of user data will only be carried out in response to an alleged violation to the AUP or for governance/legal reasons such as GDPR compliance or Police Investigation. The College recognises that it has a duty of care in such investigatory work.

It should also be noted that when accessing College systems remotely your IP address is recorded and can be used responsibly by College security systems to prevent malicious activity – this can be with automated alerting systems or pro-actively by the ICT department. You can review your sign-in data here (https://mysignins.microsoft.com/) – it is recommended you review this periodically.

The data the College collects, is subject to its processes and retention periods, these can be found in the College Privacy Notice.

GKC - Student Privacy Notice

GKC - Staff Privacy Notice

The retention periods for data and logs can be found in the College Document Retention Schedule.

GDPR - Policies and Procedures

Line managers of staff who leave the College will receive access to emails and files to ensure no important data is purged as a consequence of an individual leavings its

employment. To ensure business operations it may also be necessary to grant line managers access to staff files/emails if they are on prolonged sick or annual leave. Formal approval will be sought from SMT before access is granted.

4. Supporting Policies and Legislation

4.1. College Policies

https://www.glasgowkelvin.ac.uk/more/about-us/executive-information/policies-and-procedures/

- Disciplinary Policy and Procedure
- Grievance Policy and Procedure
- Dignity and Respect Policy
- Equality, Diversity and Inclusion Policy
- Password Change Procedure
- ICT Security Policy
- Data Protection Policy
- Data Breach Procedure
- Social Media Procedure
- Privacy Notice
- Document Retention Schedule
- Commendations and Complaints Handling Procedure
- Code of Learner Behaviour
- Staff Guide to Challenging Behaviour
- Student Online Etiquette
- Student Association Partnership Agreement
- Student Charter
- Ethos and Values Framework
- Encryption Procedure

4.2. External/Legislation

- JANET terms and conditions ○ https://community.jisc.ac.uk/library/acceptable-use-policy

- Data protection Act/GDPR Legislation ○ https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/

- National Cyber Security Centre, Cyber Essentials Plus accreditation ○ https://www.ncsc.gov.uk/cyberessentials/overview

- Scottish Government Cyber Resilience Framework ○ https://www.gov.scot/publications/cyber-resilience-framework/

- Copyright, Designs and Patents Act https://www.gov.uk/government/publications/copyright-acts-and-related-laws