

Glasgow Kelvin College

Finance and Resources Committee - 28 February 2023

**ICT Acceptable Use Policy
ICT Security Policy**

Report by the Director of Digital Services

1. Introduction

Members will be aware that the College has developed, in partnership with representatives of its recognised Trade Unions, a range of ICT policies and procedures for Glasgow Kelvin College. In accordance with the agreed Policy and Procedure Review Schedule, the ICT Acceptable Use Policy and ICT Security Policy has been revised and shared for consultation.

The purpose of this report is to apprise members of the outcome to the review of these policies and request approval from the Board of Management.

2. ICT Acceptable Use Policy

As cyber security standards evolve in response to increasingly complex and sophisticated cyber-threats, it is important that the administrative controls put in place by the College comply with those standards and provide a safe operating environment. In response to a recent Cyber Essentials assessment, it has been necessary to enhance the controls within the ICT Acceptable Use Policy. Changes to the policy are highlighted in red in the document in **Appendix 1**.

The main changes relate to:

- Page 6 – new section 2.4, Bring Your Own Device (BYOD). Additional controls have been added to accommodate the increase in the use of personal devices to access College resources by both staff and students.
- Page 7 – new section 2.5, Internet of Things (IoT). The College is starting to see a rise in the number of IoT devices such as Smart TVs, voice controls speakers, etc. A statement has been added to control the use on the network.
- Minor word changes have been made to pages 2 and 3, after consultation with Trade Unions.
- Page 10 – the Copyright, Designs and Patents Act has been added to the list of legislation.

3. ICT Security Policy

The ICT Security Policy contains no changes to report. In accordance with the Policy and Procedure Review Schedule, the policy has been reviewed and a copy has been provided in **Appendix 2**.

4. Impact on Students

No impact on students identified as a consequence of this report.

5. Resource Implications

No resource implications are identified as a consequence of this report.

6. Equality

No equality implications are identified as a consequence of this report.

7. Risk and Assurance

There are no risks identified as a consequence of this report.

8. Data Protection

There are no data protection issues as a consequence of this report.

9. Recommendations

Members of the Finance and Resources Committee are recommended to:

- i) note the content of this report and its Appendices;
- ii) approve the ICT Acceptable Use Policy; and
- iii) approve the ICT Security Policy.

10. Further Information

Further information on the content of this report can be obtained from Jason Quinn, Director of Digital Services (jqinn@glasgowkelvin.ac.uk).

DRAFT: 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:	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: <https://www.glasgowkelvin.ac.uk/equality-diversity/>

Contents

1.	Introduction and Scope.....	1
2.	Authorisation and Conditions of Use	1
2.1.	Authorisation	1
2.2.	Conditions of Use.....	2
2.3.	Accessing Services or Data Remotely (or on-campus mobile devices)	4
2.4.	Bring Your Own Device (BYOD)	6
2.5.	Internet of Things (IoT)	7
3.	Security and Data Protection.....	7
3.1.	Filtering	7
3.2.	Cyber Security	7
3.3.	Monitoring	8
4.	Supporting Policies and Legislation.....	9
4.1.	College Policies	9
4.2.	External/Legislation	9

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 significant 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 login.

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 login 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 leaving 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>

DRAFT ICT Security Policy

**Document Control Information****Reviewed by Finance and Resources Committee:****28 February 2023****Date of Next Review:****March 2026****Approved by the Board of Management:****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.

Contents

1. Security Policy Framework	3
2. Infrastructure, End User Computing & physical locations	3
2.1. Physical Security	3
2.2. Network Connection	4
2.3. End User Computing	5
2.4. Server Management.....	6
2.5. Mobile Devices	6
3. Secure Configuration	7
3.1. Firewall	7
3.2. Malware Protection.....	8
3.3. Patch Management	8
3.4. Identity & Access Management.....	9
3.5. Password Service Management	9
3.6. Encryption.....	10
4. Service Lifecycle	10
4.1. Asset Management	10
4.2. Configuration Management.....	11
4.3. Service Development Lifecycle	11
4.4. Disposal.....	12
5. Detection	12
5.1. Monitoring.....	12
5.2. Logging.....	13
6. Response & Recovery	13
6.1. Incident Response	13
6.2. Business Continuity.....	14
6.3. Disaster Recovery & Backups.....	14
7. External Partnerships.....	15
7.1. Third party	15
8. Remote access	15
8.1. VPN Access	15

1. Security Policy Framework

The security policy provides management direction and support for information security. It is primarily directed at staff within the College who are service owners, system procurement and general information services but more so ICT Services staff who are responsible for the development and maintenance of ICT systems. The policy will guide the creation of processes and procedures to minimise the risk of security breaches and events.

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

2. Infrastructure, End User Computing & physical locations

2.1. Physical Security

To restrict physical access to authorised individuals, ensure that critical equipment is available when required and to prevent important services from being disrupted by loss of, or damage to, equipment or facilities.

- 2.1.1 Physical access to critical facilities, such as data centres, network and telecommunication equipment should be restricted to authorised personnel. Authorisation should be issued in accordance with a documented process, be reviewed regularly and revoked promptly when no longer required.

- 2.1.1.1 Server Room Access

- Access to server rooms will be controlled by a Building Management System swipe entry locking system where only the following groups of staff will have access:

- Senior Management;
 - ICT staff;
 - Estates staff;
 - Health & Safety staff; and
 - Security staff.

- Racks and cabinets that hold key servers and storage devices will be locked at all times and the keys held by the ICT Department.

- Switches and routers (or general networking equipment) will be held within lockable cupboards or areas. They will only be accessible by the staff groups listed above.

- 2.1.1.2 Staff areas

- Where possible, (excluding areas such as public access, reception, advice, etc) staff areas should be locked either

with a key or an automatic door lock system when the last member of staff leaves the area. This helps to physically secure ICT equipment and any digital content on unlocked devices.

2.1.1.3 Classrooms and teaching areas

Classrooms (and similar rooms for teaching) will be secured by lockable doors. If members of staff don't have a master key to access a room they should obtain the room key from Estates. Staff should lock the rooms after they are finished with them and return the key to Estates.

PCs in classrooms will only be secured with a physical lock if the PCs are a high-value or they are deemed to have a higher risk of theft (i.e. the location may have a history of break-ins).

2.1.1.4 Outreach PCs

All outreach PCs that are owned by the College should be secured with a lockable device, thus protecting the device and its contents from theft.

2.2. Network Connection

To prevent unauthorised users or devices from gaining access to information systems and networks.

To ensure that the configuration of network devices is accurate and does not compromise the security of the network.

2.2.1 All network connected devices must be authorised by the College's ICT department and be compliant to Cyber Essentials Plus standards.

2.2.2 Must meet the appropriate security standards to protect against the compromise of confidentiality, integrity and availability of the information that they process.

2.2.3 Network attached devices should be segregated appropriately where necessary.

2.2.3.1 Network Segmentation

The College's Local Area Network (LAN) is segmented into various zones to provide a logical structure for systems, servers and endpoint devices to be best secured.

Endpoint devices are either allowed or blocked from entering the server/system zones to help secure systems and data. The table below outlines broad rules that should be followed to secure the network:

Server Zone (where servers and systems are located)	Endpoint Rules	Allowed	Endpoint blocked rules
Open Access Zone (Contains Moodle, File Servers, Mail servers, etc.)	ICT staff PCs, General Staff PCs and Student PCs are allowed.		There are no limitations – all endpoints can access this zone without restrictions
Shielded Access Zone (Contains Finance system, Student Records, HR, etc.)	ICT staff PCs and General Staff PCs are allowed.		Student PC are blocked from accessing this zone.
Management Access Zone (Contains services that end users will never need to access such as Hosts, Storage, network devices)	ICT staff PCs are allowed		General Staff PCs and Student PCs are blocked from accessing this zone.

2.3. End User Computing

To ensure end user computing devices operate as intended and do not compromise the security of computer installations or other environments.

2.3.1 All end user computing devices that connect to College services and access College information/data must be actively managed by a competent authority and at a minimum comply with the following policies:

- Firewall,
- Malware Protection,
- Patch Management,
- Service Password Management,
- Encryption; and,
- Identity and Access Management.

2.3.2 System Settings and Updates

The College's endpoint devices are configured to provide a further layer of security while not impacting on the end-user experience. This provides a balance between functionality and security.

Windows endpoint devices are configured with the following:

- End-users are not provided with administrator rights to the local device,
- Staff devices will be configured to auto-lock after a period of time,
- Endpoint devices will be configured to download Operating System updates automatically,
- 3rd party software will be updated as per the 'Vulnerability

- Remediation Procedure' which is reviewed every two years; and,
- Security patches will be applied as per the Cyber Essential Plus patching standard.

2.4. Server Management

To ensure servers operate as intended and do not compromise the security of computer installations or other environments.

- 2.4.1 Servers should be configured to prevent unauthorised access or updates and to function as required.
- 2.4.2 The configuration should disable non-essential user accounts, applications, communication services, protocols and restrict access to powerful utilities, commands and system configuration settings to trusted individuals.
- 2.4.3 All servers must be actively managed by a competent authority and at a minimum comply with the following policies:
 - Firewall,
 - Malware Protection,
 - Patch Management,
 - Service Password Management; and,
 - Identity and Access Management.

2.5. Mobile Devices

To ensure mobile devices do not compromise the security of information stored on them or processed by them and prevent unauthorised access to information in the event they are lost or stolen.

- 2.5.1 The College will protect information stored or processed via College owned mobile devices and prevent unauthorised access when lost or stolen.
- 2.5.2 Documented configuration standards will be deployed through a management system.
- 2.5.3 All mobile devices must use an appropriate access control mechanism (e.g. password, pin, biometric) and have a lock out time set.
- 2.5.4 All mobile devices must be encrypted, be capable of being remotely wiped and must be appropriately protected from malware.
- 2.5.5 To gain access to College systems users will require to:

- Possess a valid Active Directory username and password,
- be a member of a relevant user group,
- accept the terms of the ICT Acceptable Use Policy; and,
- Using a College issued device.

The system and firewall allow ICT to track and report on the user's internet use. This is a requirement of using the JISC provided JANET internet connection.

2.5.6 Internet Access for Personal Mobile Devices

The College offers a wireless 'on boarding system' to Staff and Students. This allows users to connect personal mobile devices to the College's Wi-Fi network and access Internet resources – most internal resources are blocked as the device is not College owned and trusted.

3. Secure Configuration

3.1. Firewall

To prevent unauthorised network traffic from gaining access to networks or leaving networks.

- 3.1.1 The College will operate a default inbound deny policy on all firewall devices to block unauthorised inbound connections.
- 3.1.2 Access to the management interface of the firewall will be appropriately restricted to authorised personnel.
- 3.1.3 There will be a managed process for documenting the requests for firewall changes.
- 3.1.4 All such requests must contain at a minimum the details of the requestor, the changes required, duration and the business need for the firewall change.
- 3.1.5 All firewall change requests will be subject to a review, security assessment and must be approved by a competent authority.
- 3.1.6 To ensure existing firewall rules are appropriate, and in line with CE+, there will be periodic reviews.
- 3.1.7 There will be a process where exceptions can be made due to a business need, this should be approved by a member of the SMT/OMT team.
- 3.1.8 Incoming traffic is scanned for viruses, spyware, vulnerabilities and malicious code unless it is encrypted or from a trusted source.
- 3.1.9 All internet user activity should be logged and identified using the

College's Active Directory system.

- 3.1.10 A Demilitarised Zone (DMZ) will be provisioned on the firewall as a 'Best Practice' measure to serve internal web resources from the College to the outside world.

3.2. Malware Protection

To protect the organisation against malware attacks and ensure malware infections can be addressed within defined timescales.

- 3.2.1 The College will address the malware threat by installing anti-malware software on all appropriate devices.
- 3.2.2 The anti-malware software will be kept up to date, with signature files updated at least daily.
- 3.2.3 Files must be scanned upon download and access.
- 3.2.4 Web pages must be scanned when accessed through a web browser, connections prevented to malicious websites.
- 3.2.5 There will be a documented process, including risk assessment when there is a business need for exceptions.
- 3.2.6 The College will utilise sandboxing technology where it is appropriate to do so and to minimise the risk of malicious files entering the organisation.
- 3.2.7 The College may mandate the use of application whitelisting where it is deemed necessary.

3.3. Patch Management

To address technical system and software vulnerabilities quickly and effectively in order to reduce the likelihood of vulnerabilities being exploited and serious business impact arising.

- 3.3.1 To help in the identification of threats that may lead to an information security incident, maintain the integrity of important security-related information and support forensic investigations.
- 3.3.2 The College will protect the integrity of its information and systems by gathering security logs to help identify threats and support investigations.
- 3.3.3 All systems will be assessed and configured to log appropriate security event information (e.g. failed login attempts), and the logs should be protected against unauthorised access and accidental or deliberate modification.

- 3.3.4 Security logs should be analysed/reviewed regularly, and log retention schedules are to be defined for each system.

3.4. Identity & Access Management

To ensure that only authorised individuals gain access to business applications, systems, networks and computing devices, that individual accountability is assured and to provide authorised users with access privileges that are sufficient to enable them to perform their duties but do not permit them to exceed their authority.

- 3.4.1 The College will utilise an Identity and Access Management (IAM) system.

The following procedures outline the creation and decommissioning processes:

- Creating GKC Staff Accounts - Procedure
- Staff leaver - mail and file retention - Procedure

- 3.4.2 The IAM ensures that unique account credentials are approved and created in a timely manner to allow access to information, services and locations necessary for the roles function.

- 3.4.3 That access permissions are granted on a need only basis and removed when no longer required.

- 3.4.4 That accounts are disabled or removed when no longer needed.

- 3.4.5 Standard user accounts are to be assigned by default, with a documented approval process for administrative accounts.

- 3.4.6 Administrative accounts must be used for administrative activities only, the Administrator Accounts Procedure outlines this.

- 3.4.7 Multi – Factor Authentication will be implemented for staff where there is an elevated risk (i.e. Management and staff who process key data).

- 3.4.8 The above principles should also be adhered to when providing access to non-ICT administered systems including:

- Student Records Systems,
- Timetabling system,
- Finance systems; and,
- Estates Building Access systems.

3.5. Password Service Management

To restrict access to business applications, systems, networks and computing

devices to authorised users.

- 3.5.1 All users should adhere to the College's 'Password Change Procedure'.
- 3.5.2 All users should be authenticated using a unique username and password before accessing College resources.
- 3.5.3 Password should never be requested in the form of clear text (e.g. via email, http).

3.6. Encryption

To protect the confidentiality of sensitive information, preserve the integrity of critical information and confirm the identity of the originator of transactions or communications cryptographic solutions should be approved, documented and applied throughout the organisation.

- 3.6.1 All mobile devices must be appropriately encrypted and use authorised services to ensure the protection of information at rest and in transit.
- 3.6.2 Encryption technologies used must be managed to ensure that they remain secure and have documented key management processes.
- 3.6.3 There will be a documented approval process, including risk assessment and risk management process when there is a business need for an exception.
- 3.6.4 Due to the multi-user use of Student laptops and the decreased sensitivity of data they access there is no benefit to encrypting learner devices.

4. Service Lifecycle

4.1. Asset Management

To help support risk-based decisions regarding hardware / software, reduce the risk of information security being compromised by weaknesses in hardware / software, protect assets against loss, support development of contracts and meet compliance requirements for licensing.

- 4.1.1 To assist risk-based decisions, reduce risk of compromise by weaknesses in hardware and software, protect assets against loss, meet compliance requirements and inform contracts, all hardware and software should be recorded in an accurate and up-to-date asset register.
- 4.1.2 There should be regular checks for discrepancies, and these should be investigated and resolved.

- 4.1.3 The asset register must be protected against unauthorised change and be independently reviewed.

4.2. Configuration Management

To ensure that changes are applied correctly and do not compromise the security of business applications, computer systems or networks.

- 4.2.1 Changes should be tested, reviewed and be part of a documented change management process.
- 4.2.2 The change management process covers all types of change, such as upgrades, changes to systems and networks, software or application and to business information.
- 4.2.3 Any request for change must:
- Be accepted by an authorised individual,
 - Approved by an appropriate business representative,
 - Tested; and,
 - Include a back-out plan.
- 4.2.4 Once the changes have been made the following must happen:
- Changes are communicated to relevant stakeholders,
 - System documentation is updated to reflect changes,
 - Changes are reviewed to ensure only changes that have been authorised have taken place; and,
 - System and information reviewed to ensure that security classifications have not changed.

4.3. Service Development Lifecycle

- 4.3.1 To ensure that business applications (including those under development) meet business and information security requirements. System development activities should be performed in specialised development environments, which are isolated from the live and testing environments, and protected against unauthorised access.
- 4.3.2 Quality assurance of key security activities should be performed during the system development lifecycle.
- 4.3.3 Information security requirements should be documented and agreed before detailed design commences.
- 4.3.4 Information security requirements for systems under development should be considered when designing systems.

- 4.3.5 System build activities (including coding and package customisation) should be carried out in accordance with industry good practice; performed by individuals provided with adequate skills / tools; and inspected to identify unauthorised modifications or changes.
- 4.3.6 Systems under development (including application software packages, system software, hardware, communications and services) should be tested in a dedicated testing area that simulates the live environment, before the system is promoted to the live environment.
- 4.3.7 Systems under development should be subject to security testing, using a range of attack types (including vulnerability assessments, penetration testing and access control testing).
- 4.3.8 Rigorous criteria (including security requirements) should be met before new systems are promoted into the live environment.

4.4. Disposal

To ensure the secure disposal of information assets and comply with legal, regulatory and contractual obligations.

- 4.4.1 When Technology assets have reached the end of their useful life they should be securely disposed.
- 4.4.2 Asset management processes must be updated with the final disposition of the technology asset's media and hardware.
- 4.4.3 All storage mediums will be securely erased in accordance with current industry best practices.
- 4.4.4 Approved third-party disposal service must render all data / information unreadable and provide a certificate of destruction. These certificates must be retained and asset registers updated with the locations of the certificates.
- 4.4.5 No computer equipment should be disposed of via skips, dumps, landfill etc.

5. Detection

5.1. Monitoring

To assess the performance of business applications, computer systems and networks, reduce the likelihood of system overload and detect potential or actual malicious intrusions.

- 5.1.1 The College has regulatory and operational requirements to monitor activity across its network and systems.

- 5.1.2 Information relating to this monitoring (e.g. logs) should be retained long enough to meet these requirements.
- 5.1.3 All monitoring activities must be authorised, and regularly performed to help identify suspicious or unauthorised activity.
- 5.1.4 All personnel authorised to perform monitoring functions must do so in accordance to the relevant ethics, procedures and safeguards.
- 5.1.5 Monitoring activities include scanning systems for known vulnerabilities, this activity must be restricted to authorised individuals and the results presented to the system owners.
- 5.1.6 Any misuse of ICT Systems or Equipment will be managed in line with the Acceptable Use Policy and Disciplinary Policies and Procedures.

5.2. Logging

To help in the identification of threats that may lead to an information security incident, maintain the integrity of important security-related information and support forensic investigations.

- 5.2.1 The College will protect the integrity of its information and systems by gathering security logs to help identify threats and support investigations.
- 5.2.2 All systems will be assessed and configured to log appropriate security event information (e.g. failed login attempts), and the logs should be protected against unauthorised access and accidental or deliberate modification.
- 5.2.3 Security logs should be analysed/reviewed regularly, and log retention schedules will be defined in the College's Document Retention policy.

6. Response & Recovery

6.1. Incident Response

To identify and resolve information security incidents quickly and effectively, minimise their business impact and reduce the risk of similar incidents occurring.

The College's Incident Response Procedure should be followed and will ensure the following principles:

- 6.1.1 The College / College will identify, respond to and recover from security incidents to minimise the business impact and reduce the risk of similar incidents occurring.

- 6.1.2 The incident response team is responsible for managing information security incidents.
- 6.1.3 A review will take place after each incident to identify the root cause and highlight any improvements that can be made to the process.

6.2. Business Continuity

To provide relevant individuals with a documented set of actions to perform in the event of a disaster or emergency affecting business applications and technical infrastructure, enabling critical business processes to be resumed within critical timescales.

- 6.2.1 The Business Continuity procedures should be followed with the following principles adhered to: Business continuity plans should be documented for each key service and provide a set of actions to perform when enacted.
- 6.2.2 Each plan should be prepared by or in conjunction with the service owner and relate to likely scenarios.
- 6.2.3 Roles and responsibilities should be defined and documentation/training available.
- 6.2.4 Business continuity plans should be reviewed and tested on a regular basis.

6.3. Disaster Recovery & Backups

To enable critical business processes to be resumed to an agreed level, within an agreed time following a disruption, using alternative processing facilities.

The Disaster Recovery procedures should be followed with the following principles adhered to:

- 6.3.1 Due to Virtual Machine technology a general documented backup and restore procedure will be sufficient for Disaster Recovery and backups.
- 6.3.2 Critical business information and software require a backup schedule to ensure restoration can occur within an agreed time.
- 6.3.3 Backups should be protected from loss, damage, unauthorised access and subject to the same level of protection as the live information e.g. encrypted.
- 6.3.4 Backups should be regularly verified by successfully testing restoration.
- 6.3.5 Alternative facilities must be ready for immediate use.

7. External Partnerships

7.1. Third party

To protect critical and sensitive information when being handled by external suppliers or when being transmitted between the organisation and the supplier.

- 7.1.1 To protect College information when being transmitted between or handled by an external third party, information security requirements need to be considered at all stages of the relationship.
- 7.1.2 All third parties should be identified and recorded in a register which assigns a business owner, security contact and is categorised High, Medium, Low in terms of information security.
- 7.1.3 All third parties should agree a baseline of security arrangements for any information held, and specialised controls put in place which meet business and security needs as a result of a risk assessment.
- 7.1.4 Termination of third-party relationships should ensure the revocation of physical and logical access, and the return or secure destruction of information assets.
- 7.1.5 A Business Continuity Plan (BCP) may also be required depending on the nature of the third-party service.

8. Remote access

8.1. VPN Access

A Virtual Private Network (VPN) is a service that is offered by the College for staff. This allows staff on College owned laptops to connect to the College's VPN service and access most network resources from a remote location.

The VPN system is provided by an enterprise class security vendor and is secured with the following:

- Enterprise standard SSL encryption,
- a proprietary application (i.e. standard Operating System clients will not work with the system),
- network rules which only allow the user to access the network resource or server that they require,
- Active Directory group membership – only members of the VPN security group will be allowed to connect to the system; and,
- all requests must be made through the ICT Helpdesk and approved by a relevant authority.