Dumfries and Galloway College
One step ahead

ICT SECURITY POLICY

Responsibility: Head of Corporate Services
Issue Date: 12th November 2020
Equality Impact Assessment: 19th November 2020

Version: 1

Table of Contents

ICT Security Policy

1. *Purpose*

The purpose and benefits of this policy are to raise awareness and clearly inform how Dumfries and Galloway College manages, secures and protects its Information and Communication Technology systems and data.

2. *Scope*

This procedure is to be implemented at all College sites and applies to all College staff, student and third parties who manage data and services for or on behalf of the College.

3. *References*

The policy is aligned with other policies within the College, namely:

- Data Protection Policy
- Code of Conduct Policy
- Equality and Diversity Policy
- Student Behaviour Policy
- Risk Management Policy

4. *Definitions*

ICT	Information Communications Technology
Processes	A series of actions taken to accomplish a goal.
Procedures	An agreed way of completing a task
Standards	A stated level of acceptance
Guidance	Help and advice on how to achieve a goal.

5. *Policy Statement*

5.1 The Dumfries and Galloway College ("The College") ICT policy has a structure which logically groups Core, User and Management sections. This is to ensure that the relevant sections are read and understood.

The Core section must be read and adhered to by all persons involved with College ICT systems and information.

The User section must be read and adhered to by all users of the Colleges systems and data.

The Management section must be read and adhered to by any individual or entity managing a device connected to the College network or service for or on behalf of the College.

The ICT Security Policy statements are high level strategic statements written with the following principles.

- They are needed by the College
- They clearly define the desired maturity level
- They are achievable
- They are measurable

All **processes** created must conform to these policy statements.

All **procedures** created must conform to any agreed process.

All processes and procedures must also conform to all applicable organisational **standards**.

Guidance may also be provided to ensure that any procedure and process is competed in line with current best practice.

5.2 **Roles and Responsibilities**

Role	**Responsibilities**
Senior Leadership Team	Initiate, Define and Authorise Policy
ICT Manager	Creating Procedures, Standards and Controls
ICT Staff	Implement Procedures, Standards and Controls
ICT Users	Be familiar with and adhere to the ICT Security Policy at all times.

6. Procedure

6.1 **Core**

All persons involved with College ICT systems and information must read and comply with these policies.

6.1.1 **Information Security**

Documents the governing body's direction on and commitment to information security and communicate it to all relevant individuals.

- The Information Security Policy supports the College and IT strategic visions by defining the high-level approach taken to reducing associated risks to its reputation, finances and operations.

- Information managed by the College shall be appropriately secured to protect confidentiality, integrity and availability.

- Information will be managed so that the College can ensure appropriate legal, regulatory and contractual obligations are complied with.

- The College will develop and communicate information security policies, processes and procedures that all staff, students and third parties are required to comply with.

- The College acknowledges that information security is the responsibility of every member of staff, student and third parties. The College is committed to a programme of awareness, training and education to address this.

6.1.2 **Data Risk Classification**

To determine the level of protection that should be applied to types of information, thereby preventing unauthorised disclosure an information classification scheme should be established that applies throughout the organisation, based on the confidentiality of each piece of information.

- All College staff, students and third parties who store, process, transmit and share information on behalf of the College have a personal responsibility for ensuring that appropriate security controls are applied.

- Appropriate security controls vary according to the classification of the information.

- All College information must have a classification assigned by the owner.

6.1.3 **Data Handling**

To protect information contained in documents in accordance with legal requirements, ensure critical information remains available when required, preserve the integrity of critical information and protect sensitive information from unauthorised disclosure.

- The College will ensure appropriate security controls for the handling of data are in place by providing secure services for the creation, storage, processing, transferring, sharing and deleting of information.
- A service catalogue will be maintained and available for users to search.

- Services will clearly state what classification of information can be used with them.
- All users of a service will comply with any processes and procedures as a requirement of using the services.

6.2 **User**

If you use College managed network connected devices and services, then you must read and comply with these policies.

6.2.1 **Acceptable Use Policy**

To ensure users are legally and contractually bound to protect the organisation's information, business applications and systems, and the organisation's security obligations are met.

Identification

Unique IT Accounts are associated with each User. These accounts are used to grant specific access to services and information associated with the Users role. Those who have received an IT Account from the College must not:

- Share their IT Account, or use another Users IT Account
- Disclosed their password to anyone, even College staff
- Use your IT Account username or password to register for non-College services

Information & Software

The College provides managed software to create, access, process, transfer, share and delete information. Users must ensure that they:

- Comply with the Data Protection Policy
- Do not cause a breach in confidentiality
- Do not cause a breach in copyright law
- Do not cause a breach in licences or contracts

Email

College email addresses and associated College email systems must be used for all official College business, in order to support audit purposes and institutional record keeping. All staff and students of the College must regularly read their College email and archive or delete unwanted or unnecessary emails at regular intervals.

It is not permitted to use personal email accounts for work purposes at any time. Personal email accounts do not have the same level of security as College accounts and as such provide a serious risk to the Colleges networks.

Guidance on acceptable email use can be found in the email guidelines in the quality manual on AdminNet.

College owned devices / equipment / services

The College provides computing and communication devices, specialist equipment and information services to support the educational, research, administrative and business functions of the College.

Personal use of College devices is permitted under these conditions:

- Activities are lawful
- At the user's own risk
- Withdrawn if deemed to be excessive

- Must not interfere with contractual, professional, course or research obligations
- Must not hinder the use of others

Prohibited use:

- Personal commercial activity
- Access or disseminating material of a pornographic, criminal or offensive nature including material promoting terrorism except when prior written authorisation has been granted by the appropriate body.

Consumer devices / equipment / services

Users may use personal consumer devices to access College resources where authorised by the appropriate body. Only information classified as Low risk can be used with consumer devices, equipment and services.

By doing so the User agrees to the following:

- The College retains the rights to inspect, conduct a remote audit, and remotely wipe the device
- All College information stored on a consumer device remains the property of the College
- The waiver of College liability
- Not to share the device with other individuals
- Manage the device in accordance with the ICT Security Policy, Management, End User Computing section.

Responsibilities

All Users have responsibilities to protect the confidentiality, integrity and availability of College information. These include:

- Report information incidents promptly: breaches of confidentiality, failures of integrity and loss of availability
- Provide physical security of mobile devices

- Report loss or theft of devices
- Change passwords on notification of compromise

Monitoring and Logging

The College may monitor communications, files and emails as detailed in the Monitoring and Logging sections within the ICT Security Policy.

Disciplinary

Any breach of this policy can result in disciplinary action.

6.2.2 User Password

To prevent unauthorised users from gaining access to password-protected critical or sensitive information, business applications, systems, networks or computing devices.

- College usernames and passwords are unique and used to grant access to information and resources specific to individual needs.
- They are used to identify and log user activity on College systems and services.
- Passwords must be kept confidential, they should never be shared or disclosed to anyone, the College will never ask for your password.
- A password used to access College resources must not be used to access any external third-party resources.
- Users must report and change passwords if it has been, or it is suspected that it has been compromised.

6.2.3 Remote Working

The College appreciates that there may be circumstances where remote working is required. In normal circumstances this will be facilitated using a

college issued devices which has been fully configured for security purposes. We do though appreciate that there may be times where the use of home devices may be required though we expect these would be exceptional circumstances.

To ensure that critical and sensitive information handled by staff working in remote environments is protected against the full range of security threats. To protect College information from security threats staff working from home or other remote locations should:

- Be authorised to do so
- Have received relevant security training
- Do so from an approved secure device
- Do so by an approved and authorised process

All devices should be protected against loss or theft by using an appropriate access control mechanism, encryption at rest and in transit, and for mobile devices (e.g. laptop) a tamper proof label with device identification details.

6.2.4 Clean Desk

To ensure information stored in or processed by office equipment is not disclosed to unauthorised individuals.

- All sensitive/confidential information in hardcopy or electronic form is secured in workspace at the end of the day or when unoccupied for an extended period.

- Computer screens must be locked when workspace is unoccupied.

- File cabinets containing Restricted or Sensitive information must be kept closed and locked when not in use or when not attended.

- Keys used for access to Restricted or Sensitive information must not be left at an unattended desk.

- Laptops must be either locked with a locking cable or locked away in a drawer when not in use

6.3 Management

If you manage a device or service which is connected to the network, then you must read and comply with these policies.

6.3.1 End Point Security

6.3.1.1 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.

- 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.

- All visitors to critical facilities must be supervised at all times.

- Environmental and power protections should be in place when required.

6.3.1.2 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.

- All network connected devices must be authorised and managed by a competent authority.

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

- Network attached devices should be appropriately resourced to manage their current and predicted processing requirements and segregated appropriately where necessary.

- Segregated appropriately where necessary.

6.1.3.3 **End User Computing**

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

All end user computing devices that connect to College services and access College information with a classification of "Medium" or "High" 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
- Identity and Access Management

6.1.3.4 **Server Management**

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

- Servers should be configured to prevent unauthorised access or updates and to function as required.

- 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.

- 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
    Encryption
    Identity and Access Management

6.1.3.5 **Mobile Device**

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.

- The College will protect information stored or processed via mobile devices and prevent unauthorised access when lost or stolen.

- Documented configuration standards will be deployed through a management system.

- All mobile devices must use an appropriate access control mechanism (e.g. password, pin, biometric) and have a lock out time set.

- All mobile devices must be encrypted, be capable of being remotely wiped and must be appropriately protected from malware.

6.3.2 **Secure Configuration**

6.3.2.1 **Firewall**

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

- The College will operate a default inbound deny policy on all firewall devices to block unauthorised inbound connections.
- Access to the management interface of the firewall will be appropriately restricted to authorised personnel.
- There will be a managed process for documenting the requests for firewall changes.
- 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.
- All firewall change requests will be subject to a review, security assessment and must be approved by a competent authority.

- To ensure existing firewall rules are appropriate there will be periodic reviews.
- There will be a documented approval process, including risk assessment and risk management process when there is a business need for an exception.

6.3.2.2 **Malware Protection**

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

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

6.3.2.3 **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.

- The College will meet it's legal and contractual obligations through a software asset management process.
- The College will protect its users, services and information by only using licensed and supported software.
- Software shall be removed from devices when no longer supported or required for business function.

- All software updates must be applied in line with an approved business processes (e.g. within 14 to 30 days of vendor release).

- There will be a documented approval process, including risk assessment and risk management process when there is a business need for an exception.

- Any systems not compliant with this policy shall be removed from the network.

6.3.2.4 **Identity and 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.

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

- 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.

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

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

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

- Administrative accounts must be used for administrative activities only.

- 2 factor authentication will be implemented where available and required.

6.2.3.5 **Password Service Management**

To restrict access to business applications, systems, networks and computing devices to authorised users.

- All users should be authenticated using a unique username and password before accessing College resources.

- Password should never be requested in the form of clear text (e.g. via email, http).

6.2.3.6 **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.

- All devices must be appropriately encrypted and use authorised services to ensure the protection of information at rest and in transit.

- Encryption technologies used must be managed to ensure that they remain secure and have documented key management processes.

- There will be a documented approval process, including risk assessment and risk management process when there is a business need for an exception.

6.3.3 Service Lifecycle

6.3.3.1 **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.

- All hardware and software should be recorded in an accurate and up-to-date asset register.

- There should be regular checks for discrepancies, and these should be investigated and resolved.

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

6.3.3.2 **Configuration Management**

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

- Changes should be tested, reviewed and be part of a documented change management process.

- The change management process covers all types of change, such as upgrades, changes to systems and networks, software or application and to business information.

- Any request for change must:
  - Be accepted by an authorised individual
  - Approved by an appropriate business representative
  - Include a risk assessment
  - Tested
  - Include a back-out plan

- 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
System and information reviewed to ensure that security classifications have not changed

6.3.3.3 **Service Delivery Lifecycle**

To ensure that business applications (including those under development) meet business and information security requirements.

- Development activities should be carried out in accordance with a documented system development lifecycle methodology.
- System development activities should be performed in specialised development environments, which are isolated from the live and testing environments, and protected against unauthorised access.
- Quality assurance of key security activities should be performed during the system development lifecycle.
- Information security requirements should be documented and agreed before detailed design commences.
- Information security requirements for systems under development should be considered when designing systems.
- 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.
- 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.

- Systems under development should be subject to security testing, using a range of attack types (including vulnerability assessments, penetration testing and access control testing).

- Rigorous criteria (including security requirements) should be met before new systems are promoted into the live environment.

- New systems should be installed in the live environment in accordance with a documented installation process.
- Post-implementation reviews (including coverage of information security) should be conducted for all new systems.

6.3.3.4 **Compliance**

To comply with laws and regulations affecting information security.

- The College recognises the critical importance of compliance and will establish a process to identify, interpret and comply with all relevant laws and regulations affecting information security. This will cover:

    1. Information security-specific legislation
    2. General legislation which has security implications
    3. Regulations
    4. Contracts

- The compliance process should be documented, signed off by executive management, and kept up-to-date.

- Compliance will be regularly reviewed by key stakeholders from across the College.

6.3.3.5 **Disposal**

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

- When Technology assets have reached the end of their useful life they should be securely disposed of.
- Asset management processes must be updated with the final disposition of the technology asset's media and hardware.
- All storage mediums will be securely erased in accordance with current industry best practices.
- 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.
- No computer equipment should be disposed of via skips, dumps, landfill etc.

6.3.4 **Detection**

6.3.4.1 **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.

- The College has legal, regulatory and operational requirements to monitor activity across its network and systems.
- Information relating to this monitoring (e.g. logs) should be retained long enough to meet these requirements.

- All monitoring activities must be authorised, and regularly performed to help identify suspicious or unauthorised activity.

- All personnel authorised to perform monitoring functions must do so in accordance to the relevant ethics, procedures and safeguards.

- Monitoring activities include scanning systems for known vulnerabilities, this activity must be restricted to authorised individuals and the results presented to the system owners.

6.3.4.2 **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.

- The College will protect the integrity of its information and systems by gathering security logs to help identify threats and support investigations.

- 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.

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

6.3.5 Response and Recovery

6.3.5.1 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 will identify, respond to and recover from security incidents to minimise the business impact and reduce the risk of similar incidents occurring.

- The incident response team is responsible for managing information security incidents.

- A review will take place after each incident to identify the root cause and highlight any improvements that can be made to the process.

6.3.5.2 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.

- Business continuity plans should be documented for each service, provide a set of actions to perform when enacted and should be the result of a risk assessment.

- Each plan should be prepared by or in conjunction with the service owner and relate to likely scenarios.

- Roles and responsibilities should be defined and documentation/training available.

- Business continuity plans should be reviewed and tested on a regular basis.

6.3.5.3 Disaster Recovery

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

- Disaster recovery plans should be documented for each critical business process to ensure they can be resumed using alternative facilities to an agreed level and timeframe.

- Alternative facilities must be ready for immediate use.

6.3.5.4 Backups

To ensure that, in the event of an emergency, essential information or software can be restored within critical timescales.

- Critical business information and software require a backup schedule to ensure restoration can occur within an agreed time.

- Backups should be protected from loss, damage, unauthorised access and subject to the same level of protection as the live information e.g. encrypted.

- Backups should be regularly verified by successfully testing restoration.

- The type of backup should be identified as:

Backup Type	Recovery Time	Method
Online storage	Instantaneous	Direct Attached Storage (DAS), Storage Area Network (SAN)
Near-line storage	Minutes	Automated tape library
Off-line storage	Hours	Manual IT staff restoration

6.3.6 **External Partnerships**

6.3.6.1 **Third Party**

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

- 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.

- 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.

- 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.

- Termination of third-party relationships should ensure the revocation of physical and logical access, and the return or secure destruction of information assets.

- A Business Continuity Plan (BCP) may also be required depending on the nature of the third-party service.

6.3.6.2 **Cloud**

To help ensure cloud specific risks are reduced to a level acceptable by the organisation.

- Any purchase or use of a cloud service must align with strategic goals, be centrally registered, approved, regularly reviewed and supported by a contract.

- There must be a risk assessment performed for the full lifecycle of the service including: creation, processing, storage, transmissions and destruction of information.

- The risk assessment should also take into consideration the classification of data assigned and its suitability for use in the cloud.

7. Distribution

All Staff
Repository

Revision Log		
Date	Section	Description
12.11.2020	Front page	Change of Job Title from Vice Principal Corporate Services and Governance to Head of Corporate Services
12.11.2020	Throughout the Policy Document	Revision to whole Policy document to reflect changes to D & G College management, security and protection of its ICT systems and data
December 2021	7 - Distribution	Changed Quality Manual to Repository

THIS FORM TO BE UPDATED WHENEVER THERE IS A CHANGE IN ANY SYSTEM DOCUMENT				
Document Name	Document Owner	Revision Number	Date of Issue	Date of Withdraw
ICT Security Policy	Head of Corporate Services	1	12.11.20	