Information Security Policy

New College Durham is committed to safeguarding & promoting the welfare of children and young people, as well as vulnerable adults, and expects all staff and volunteers to share this commitment.

Policy Title	Information Security Policy
Document Owners	Head of ICT / Data Protection Officer
Senior Management Responsibility	Senior Information Risk Owner
Directorates and Departments affected by this Procedure	All staff and students
Procedure Effective From	May 2021
Next Review Date	May 2026

Contents

We will consider any request for this procedure to be made available in an alternative format.

We review our policies and procedures regularly to update them and to ensure that they are accessible and fair to all. All policies and procedures are subject to equality and accessibility impact assessments.

We are always keen to hear from anyone who wants to contribute to these impact assessments, and we welcome suggestions for improving the accessibility or fairness of the policy.

To make suggestions or to seek further information and assistance please contact:

records@newdur.ac.uk or icthelpdesk@newdur.ac.uk

Equality Impact Assessed: 31/3/21
Accessibility Checked: 31/3/21

1. Introduction

This Information Security Policy is relevant to all Schools and Departments and to all staff and external parties employed or otherwise contracted to work at the College.

2. Scope of the Policy

This policy will seek to mitigate risk to business continuity, harm to individuals and breaches of the law.

To ensure risks to valuable business assets such as information and related processes, systems and networks are mitigated, it is the policy of the College to ensure effective information security procedures are in place.

Information has a natural lifecycle, from creation and origination through storage, processing, use and transmission to its eventual destruction or decay. The value of, and risks to, assets may vary during their lifetime, but the College recognises that information security remains important at all stages of this lifecycle.

The College recognises that the security that can be achieved through technical means is limited and should be supported by appropriate management and procedures.

Information managed by the College is not just held in electronic format and therefore this Policy covers the security of information held on all media.

3. Responsibilities

a) Management direction and support

Responsibility for approving and ensuring compliance with this Policy lies with the Senior Leadership Team.

The Senior Information Risk Owner (SIRO) for the College is the Deputy Chief Executive Officer. The SIRO acts as the advocate for information risk management at the highest level of the College's leadership team.

b) Policy Ownership

The Head of ICT and the Data Protection Officer are jointly responsible for the definition, maintenance, review and communication of information security policies; as well as maintaining associated guidelines and promoting compliance with them; and providing training to system and data owners to ensure necessary competences are maintained. They will also establish and maintain appropriate contacts with specialist security forums and professional associations in respect of this Policy.

The Head of ICT and the Data Protection Officer will also have joint responsibility for liaising with the Contracts and Purchasing Unit to ensure information security aspects of supplier relationships are identified and documented. Where a third party is asked to process data on behalf of the College, the information security checklist (appendix A) should be completed.

c) Compliance

Compliance with this Policy and any associated procedures is compulsory for all staff employed by the College. A member of staff who fails to comply with the Policy may be subjected to disciplinary action under the College disciplinary policy. It is the responsibility of Heads of Departments/School and their Senior Management to ensure that staff are aware of the existence of this Policy and its content.

d) ICT Infrastructure Ownership

The Head of ICT is responsible for planning and risk assessing the implementation of network infrastructure projects and approving the facilities offered by external providers.

e) System Ownership

A System Owner, as identified in the College's Information Asset Register[1], is responsible for addressing information risk in relation to their system by undertaking risk assessments during the business case stage of project implementation and accepting any residual risk. The System Owner will be responsible for maintaining guidelines on the acceptable use of their system and its operation. Specific tasks and processes will be elaborated as detailed below.

f) Data Ownership

A Data Owner, as identified in the College's Information Asset Register, is defined by the Data Protection Policy as the person who holds managerial and financial accountability for a data set and determines its purposes and means of processing. The Data Owner is also responsible for addressing information risk in relation to their system by undertaking risk assessments during the business case stage of project implementation and accepting any residual risk, but the Data Owner is expected to take the lead in determining access control decisions. Specific tasks and processes will be elaborated as detailed below.

[1] An **Information Asset** is records held in a structured form, usually a database. The **Information Asset Register** is a List of these, held as part of the College's **Register of Processing Activity** – detail can be seen in the **Records Management Policy** and **Data Protection Policy**

g) Suppliers

External suppliers who are contracted or otherwise notified that they have responsibilities in relation to the security of College information are responsible for carrying out their contractual obligations, which may include being a Data Processor on behalf of the College and required to work to instructions provided by the College as the Data Controller. It is expected that these instructions will be held by the Contracts and Purchasing Unit with the contract records.

4. Relationship with existing and future policies and standards

This Policy provides management direction for information security across all Schools and Departments and requirements are based on the ICT Business Impact Assessment, the College's legal, statutory, regulatory, contractual and business requirements.

This Policy consists of topic-specific policies, each jointly written by the Data Protection Officer and the Head of ICT working with stakeholders such as Human Resources, the Contracts and Purchasing Unit and Estates.

The following College policies and plans are related to this Information Security Policy:

- Management and Monitoring of Electronic Communications, Internet and Telephones Policy
- Records Management Policy
- Data Protection Policy
- Copyright and Intellectual Property Policy
- ICT Business Continuity Plan
- ICT Business Impact Assessment [Not yet published]
- ICT Change Management Policy
- ICT Patch Management Policy
- ICT Equipment Loans Policy
- ICT Equipment Replenishment Policy

The College will seek to facilitate compliance with BS ISO IEC 27001:2017, BS7799 2:2005 and BS10008:1. Compliance with this Policy will facilitate compliance with other information-related legislation, especially data protection law.

5. Identification and definition of assets and processes

a) ICT Infrastructure

ICT infrastructure is identified and resourced by the Head of ICT through capital requests and is based on strategic priorities and the ICT Business Impact Assessment [Not yet published].

b) Information Systems and Projects

New information systems and projects are identified via the Information Projects Approval Process and the Contracts and Purchasing Unit procedures. To determine the appropriate levels of security measures applied to information systems or projects, an Information Security Impact Assessment will be carried out to identify the probability and impact of security failures. Where Personal Data is held in a system a Data Protection Impact Assessment must also be carried out. Usually the System Owner or Data Owner will carry out these assessments in consultation with the relevant members of Academic Registry and the ICT Department. After approval via the Information Projects Steering Group a new system will be added to the Information Asset Register and a new project to the Projects Register.

The information added to the Information Asset Register will include the System Owner, Data Owner and appropriate support details. It will also include a rationale for access management.

c) Coverage

The risk posed to the College by potential failures in the security of information held in paper or manual systems will also be considered under this Policy. Responsibility for these assessments will lie with the Head of the Department or school managing the information.

d) Classification

The College uses the classification given to the asset in the registration process, according to the Business Impact Risk Assessment 'criticality rating', to determine the relative importance of the level of protection that will be given to the asset.

e) Segregation of duties

Where feasible, the College will segregate conflicting duties and areas of responsibility to reduce opportunities for unauthorised or unintentional modification or misuse of assets. Care will be taken that no single person can access, modify or use assets without authorisation or detection.

f) Contact with enforcing authorities

The College will establish and maintain appropriate contacts with other organisations, law enforcement authorities, regulatory bodies and network and telecommunications operators in respect of this Policy.

6. Evaluation and Review

The performance of this Policy will be reported on annually and it will be formally reviewed every five years by the Corporation.

In addition, the effectiveness of this Policy will be monitored as necessary on an on-going basis to ensure it is compliant with relevant legislation.

A. Mobile Device Policy

1. Objectives

This document specifies the College policy for the use, management and security of all mobile devices that may hold College information and/or connect to the College network and access the college electronic resources.

2. Responsibilities

The Head of ICT is responsible for this policy.

This policy applies to all staff and third parties (including but not limited to temporary staff, agency workers and associates) operating on behalf of the College or undertaking College functions and thereby accessing the above systems and who have been provided with a College Issued Mobile device. These will hereafter be referred to as 'Users'.

3. Scope and definitions

This Policy applies to, but is not limited to, College issued mobile devices and accompanying media that fit the following device classifications:

- Laptop or notebook
- Tablet computers such as iPads and Surface Pros
- Mobile/Smartphones
- Any mobile device capable of storing corporate data and connecting to an unmanaged network.
- Portable storage such as removable hard drives, USB memory sticks and data cards
- Portable audio visual equipment including data projectors, cameras etc

This policy applies to all college issued or loaned mobile devices (as defined above). Personally owned mobile devices cannot be used to access college information.

Devices such as Mobile phones, laptops, portable devices etc. can be loaned to employees and provided by the College on a short-term basis as required and are covered under this policy.

College Information means information relating to or connected with the College's business or affairs whether or not such information constitutes 'confidential' information.

Confidential information is information which should not be made public and includes personal data as well as information processed under contract with a funding provider or contracted partner.

4. Processes

College mobile devices are configured to connect to network or ICT facilities including, but not limited to, College information systems, staff email, College managed storage (i.e. Z drive, J drive and OneDrive folders).

The use of any mobile device to process and access College information creates risks including those relating to data protection, virus infection, copyright infringement, unintentional or unlawful compromise of data and even loss or theft of device and / or data.

The College is committed to processing all personal data in accordance with the Data Protection legislation regardless of the device used to access the information. College users are required to keep College information and personal data secure. This applies equally to College information held on College systems and devices or accessed / held on personally owned mobile devices.

The College reserves the right to refuse to allow access to devices or software where it considers that there is a security or other risk to its information or ICT facilities.

The College is the owner of all College information and the contents of College systems together with everything which is created on, transmitted to, received on or printed from, or stored or recorded on each Mobile device, in each case during the course of the College's business or otherwise on the College's behalf.

Monitoring of College ICT activity logs (relating to Staff usage) using College issued devices will be carried out in accordance with the Policy on the Management and Monitoring of Electronic Communications, Internet and Telephones.

Mobile device loan schemes should incorporate the principles of the ICT Equipment Loans Policy into their terms and conditions, making the person borrowing the device(s) aware of their responsibilities.

Mobile device users are responsible for:

- the security of College information and of the device on which the information is held

- storing College information on the mobile device only for so long as absolutely necessary

- deleting College information from the mobile device when no longer required or sooner if required by the College to delete it

- ensuring (where possible) the device has up to date operating system and anti-virus protection

Confidential information should only be stored within and accessed from College information systems and College managed storage to ensure security of and appropriate secure access to the information.

Confidential information should not be stored or transferred to a cloud computing service (such as personal OneDrive, Dropbox accounts etc.) unless it is under a College negotiated contract.

Only store the minimum amount of information necessary (to carry out any required task) on a mobile device. Any confidential information should be deleted from the device as soon as the information is no longer required.

Mobile phones and iPads purchased by the College must be enrolled and registered on the college Mobile Device Management system (MDM) and must have a strong (four or more alphanumeric characters/ pattern) password/ passcode / PIN enabled to reduce opportunity for unauthorised access. Passwords / passcodes / PINs must be kept secure. The device should be set to automatically lock if inactive or locked manually as soon as the device is no longer being used. All new iPads and laptops will be placed onto the asset register whilst a separate register exists for mobile phones.

Mobile devices used to regularly access/store confidential information should where feasible be subject to additional protection measures (such as encryption) to reduce opportunities for loss or compromise of information. College laptops/tablets will be encrypted as standard. Portable storage devices for staff (i.e. hard drives or USB memory sticks) will be encrypted if being written to.

Mobile devices should, where possible, have operating system and anti-virus updates enabled. “Jailbroken” or “rooted” devices or those mobile devices which have otherwise circumvented the installed operating system security requirements (making them vulnerable to compromise) are not permitted and any user found to have attempted to Jailbreak or Root a college device will be subject to disciplinary action.

College issued mobile devices are configured to standard security and other settings and tariffs before delivery to the User. Any changes required to these settings and any tariffs must be requested via the ICT Service Desk.

College issued mobile devices must not be left unsecured whether on or off College premises. When unattended the device must be locked (password / passcode / PIN protected) and the mobile device should be secured wherever possible. College laptops and iPads must be stored in the designated laptop trollies if unused whilst onsite and the trolley locked.

Users must take responsibility for a mobile device and not leave it unattended.

ICT staff will ensure College issued mobile devices are not left unattended at any point in the delivery or installation process. This will include signed receipt of collection/delivery by the User.

College issued mobile devices must be uniquely identified, asset tagged (International Mobile Equipment Identity IMEI number recorded against user for mobile phone) and configured for the user. Issue/loan records will be kept accurate and up to date. The record will then be electronically filed appropriately.

The devices are College property and as such must be returned to ICT upon change of user or termination of employment. They must not be sold, given away or otherwise be disposed of by the user

ICT will oversee any re-image before issuing to another user (or secure erasure when disposing of devices at end of life). If devices are not returned (after a reminder process) the matter will be passed to the Head of School / Department as a disciplinary matter. The matter may also be passed to the Police for consideration of further action or for recovery via civil litigation.

The use of mobile devices overseas can lead to potentially significant costs, for example through data roaming, as well as risks to the device. Any user wishing to use the device abroad will need to contact ICT prior to any overseas venture. Failure to do so may make the user liable for any additional charges.

In the event of loss or theft of any Mobile device the User must act promptly to minimise the risk of compromise to College information by immediately:

- Report the loss of the device to ICT immediately

- changing their College network log-in password and notifying ICT Service Desk of the loss of the device

- changing any other passwords that may have been used on the device

Appropriate steps will be taken to ensure that College information on or accessible from the Mobile device is secured, including remote wiping of the mobile device. The remote wipe will destroy all data on the mobile device. Any data that is personal in

nature (such as photographs, text, documents etc.), may be lost. Users should, therefore, regularly backup all personal data stored on the mobile device.

Any actual or suspected misuse of mobile devices or breach of this policy should be reported to the ICT Services Service Desk.

B. Mobile Working Policy

1. Objectives

To ensure the security of information accessed whilst remote working.

2. Responsibilities

The Head of ICT is responsible for this policy.

3. Processes

Remote access to login to the college network will be by one of the approved methods below:

- Virtual Desktop Infrastructure (VDI)
- Virtual Private Network (VPN)

Virtual Desktop access can be accessed via both the web portal (https only) or by downloading the applications and is available for all staff and students to use.

VPN is available only by application which is installed only on Staff laptops and only when necessary.

For support purposes all 3rd Parties will use VDI and a unique support account with the relevant permissions for the systems they support. Any other access outside of this must be approved by Head of ICT.

College systems and file stores via remote access or cloud storage is available to collaborate with your external agencies securely and efficiently.

All devices, personal or College owned should have the operating system patched to the latest recommended levels and the device should have a Firewall enabled and anti-virus/anti-malware system which is active and up-to-date.

All college portable laptops and tablets will have disk encryption enabled and the corporate security suite installed.

It is not allowed for work or college data to be transferred onto personal device. All USB or external hard drives that contain college information must be encrypted.

Printing of college work should only be done at home in exceptional circumstances. Once used paper documents should be shredded or brought onsite and filed.

Do not leave yourself logged in to college systems whilst not working or if leaving the device unattended. If you are leaving the device for a short time please ensure

the computer is locked. Do not write down or save locally any college related credentials.

Do not leave any laptops or mobile devices unattended or allow access to another person, allow another user to use your device whilst you are logged onto a college system or share your credentials. It is not permitted to show or share any work to a non NCD individual unless approved as an external or guest user.

Do not remove paper files from the workplace unless this is already an approved working practice.

Failure to observe the above may contribute to a data breach or information security incident which could impact the College's business significantly. Breaches of the College's Information Security and Data Protection Policies could lead to disciplinary action.

Users must co-operate with the College to enable access, inspection and other authorised activities in relation to the device used to access College information. This may involve providing the College with access to a personal device.

Any actual or suspected misuse of mobile devices or breach of this policy should be reported to the ICT Services Service Desk.

Any staff member connecting to a college system should consider the security of the networking facility or wireless they are connecting to. If the employee uses their own computer equipment they will be responsible for any repairs or technical support

The college telephony system can be used when working remotely. All calls made or received from a college number can be made accessible from a personal device.

As compliance criteria on the College becomes more complex ICT may need to apply further security controls from time to time. Any such changes will be communicated as necessary. Such security controls may be applicable to college owned and privately-owned devices, should the user not wish their privately owned device to be subject to security controls then that device may not be allowed to connect to the college network or access to information.

C. Human Resource Security Policy

1. Objectives

To ensure that employees and contractors:

- understand their responsibilities and are suitable for the roles for which they are considered
- are aware of their roles and fulfil their information security responsibilities

To protect the College's interests as part of the process of changing or terminating employment.

2. Responsibilities

The Director of Human Resources is responsible for this policy.

The Head of ICT and the Data Protection Officer are responsible for ensuring due diligence takes place in respect of the below on contracts identified by those departments responsible for the contract.

The Director of Business Development, Director of Human Resources and the Procurement and Contracts Manager are responsible for ensuring terms and conditions of any contracts used by the College within their areas comply with this policy.

College Managers are responsible for ensuring responsibilities for information security within roles are identified in job descriptions and responsible for monitoring employee and external contracts to ensure the terms and conditions of contract are held to.

3. Processes

a) Screening

During the recruiting process for staff, background verification checks proportional to the business risk are carried out by the Human Resources department. Standard background checks are detailed in the College's Policy on Recruitment and Selection

In relation to specific security roles within ICT, Academic Registry and Senior Management it is expected that the recruiting manager will ensure that the candidate:

- Has the necessary competence to discharge the security aspects associated with their role
- Can be trusted to take on the role

If screening is a requirement of a contract between the College and a third party, the relevant manager must ensure the provisions are monitored. In the case of ICT contractors, any supplier managing a hosted system will only be approved to do so if the Head of ICT has approved their system security and the Data Protection Officer has approved their contractual clauses for data processing.

b) Terms and Conditions of Employment

The College's contract of employment states:

- The employee's obligation of confidentiality
- The employee's legal responsibilities and rights (especially in relation to Data Protection and Copyright Law)
- The employee must abide by all College policies, this includes the Acceptable Use Policy; the Information Security Policy; the Data Protection Policy and the Records Management Policy. These policies cover the expectation of the College in relation to the handling of information and records.
- Action to be taken if the employee or contractor disregards the organisation's security requirements.
- That responsibility for information security and confidentiality will persist beyond the end of employment.

Most roles within the College include the need to handle and process personal data and therefore the Data Protection Policy covers staff responsibilities in more detail.

Contractors with access to the College Network are required to sign the Acceptable Use Policy – System Support.

c) Management responsibilities

Managers must ensure employees and contractors:

- Are appropriately briefed on their information security roles and responsibilities prior to starting work
- Are guided to the correct guidelines and policies
- Are motivated to fulfil the Information Security policies of the College
- Achieve a level of awareness on Information Security relevant to their roles and responsibilities within the College
- Conform to all relevant terms and conditions of contract
- Continue to have appropriate skills and qualifications in relation to their role

There is an anonymous reporting channel to report violations of Information Security policies and procedures, initially anyone wishing to report a violation should email trackit@newdur.ac.uk or help@newdur.ac.uk. Managers should

encourage staff to use this in a timely manner to ensure any possible security incidents are investigated promptly.

d) Awareness, Education and Training

Employees and, where relevant, contractors will receive regular training on Information Security. Training and awareness programmes will be organised by the Academic Registry and the ICT Department. Changes to the Information Security policy will be communicated to all staff and changes to processes will be communicated to appropriate staff.

e) Disciplinary Process

The disciplinary process for Information Security breaches is contained within the College's Disciplinary Procedure.

f) Termination and change of employment

Information Security responsibilities and duties that remain valid after termination of contract are defined, communicated to the employee or contractor and are enforced as necessary by the Director of HR or by the College Manager that is responsible for the contract.

D. Asset Management

1. Objectives

To identify College Assets and define appropriate protection responsibilities

To ensure that information receives and appropriate level of protection in accordance with its importance to the organisation.

To prevent unauthorised disclosure, modification, removal or destruction of information stored on media

2. Responsibilities

The Head of ICT and the Data Protection Officer are responsible for this policy.

The Director of Finance is responsible for ensuring compliant Financial Procedures are in place.

The Information Compliance Co-ordinator has responsibility for maintaining the Information Asset Register using information provided by the ICT Department and relevant System and Data Owners.

Other responsibilities will be detailed in policies referred to below.

3. Processes

a) Inventory of physical assets

For detail please see the Asset Registration Process of the Financial Procedures.

b) Ownership of physical assets

For detail please see the Asset Registration Process of the Financial Procedures.

c) Acceptable use of physical assets

For detail please see the Asset Registration Process of the Financial Procedures.

d) Inventory, ownership and use of information assets

The College has an Information Asset Register which is maintained with details of new information systems, including ownership. Details of the responsibilities of asset owners are detailed in Section 3 of the umbrella policy.

The College has an Asset Register which details where equipment is located and any ownership logged.

Classification of this data is provided in the College Fileplan which is part of the Records Management Policy.

Security classification of this data is based on the requirements of any funding or validation partners and will be implemented on a case by case basis by the department owning the data.

e) Return of IT assets

For detail please see ICT Equipment Loan Policy.

f) Management of removable media

All removable media relating to staff will be required to be encrypted, otherwise when connected the device will be marked as Read Only, preventing any college data being insecurely stored on a removable device. Removable media should not be relied upon to store important due to the risk of degraded or lost media.

All removable media will be stored in a safe manner to prevent damage, loss or theft.

CD and DVDs with sensitive information are required to be destroyed and devices such as USBs, external hard drives, disks etc. should be safely and securely formatted using an appropriate application.

Upon initial connection or insertion all removable media will be scanned by the college security software with any malicious content blocked or deleted and any programs or software attempting to run automatically will not be allowed to execute.

g) Disposal of media

Any physical device such as a Storage Area Network, server or desktop shall either have the drive(s) removed and destroyed or securely wiped by software to an acceptable standard.

Processes for the secure disposal of information on paper media or removable media (ie. USBs, DVDs) are detailed in the College's Guidance on disposal of confidential waste.

i) Physical media transfer

Removable media, including paper documents, will only be used to transport information if it is a contractual requirement from a third party, the College is

following instructions as a Data Processor and the College is satisfied that the integrity of the information is protected in transit.

When confidential information on media is not encrypted, additional physical protection of the media will be considered.

E. Access Control Policy

1. Objective

To align access to information and information processing facilities with business and information security requirements.

To make users accountable for safeguarding their authentication information.

To allow authorised and prevent unauthorised access to networks, systems and applications.

Business requirements for access controls will be based on:

- Business continuity based on an assessment of the criticality of the system
- Breach of the law and contract

2. Responsibilities

The Head of ICT and the Data Protection Officer are responsible for this policy.

System and Data Owners should determine appropriate access control rules, access rights and restrictions for specific user roles towards their assets, with the amount of detail and the strictness of the controls reflecting the associated information security risks.

The Information Compliance Co-ordinator will maintain a register of Network Shares, SharePoint Sites and Team Sites showing the Owner of each. The Information Compliance Co-ordinator will also manage an annual audit of permissions across these sites.

3. Access to Information Systems

Access to these systems must be proportional to the sensitivity of the data held and is determined by the Data Owner and implemented by the System Owner.

Access controls applied should also reflect any relevant legislation or contractual obligations regarding limitation of access to data or services as defined in the Information Asset Register entry for the system.

System Owners must ensure:

- segregation of access control roles, e.g. access request, access authorisation, access administration;
- requirements for formal authorisation of access requests are enforced (if formal authorisation not required then rationale will need to be documented)

- periodic review of access rights
- removal of access rights
- archiving of records of all significant events concerning the use and management of user identities and authentication information
- effective management of roles with privileged access
- formal Procedures and defined responsibilities exist

There will be no changes in user permissions that are initiated automatically by an information system and not initiated by an administrator

4. Access to networks and network services

The network must be designed and configured to deliver levels of performance, security and reliability suitable for the College's business needs, whilst providing a high degree of control over access.

Controls will be used where practical to partition the network into domains on the basis of security requirements. The applications that reside within these domains will have defined System Administrators implemented.

Access controls should be used to prevent unauthorised access to network resources. Appropriately configured firewalls should be used to help protect the College's critical computer systems. The college uses various Micro Segmentation techniques to achieve this. When a new server or subnet is created then the device or network will be configured as appropriate on VMWare NSX within the relevant environment.

Users will only be provided with access to the network and network services that they have been specifically authorised to use.

Access to the College network will require a logon. All users must authenticate onto the college domain via Active Directory and then any college system thereon in and where Multi Factor Authentication (MFA) can be used it will be enabled. Where possible any logon screen will have any system identifiers removed.

When logging onto the corporate network, a notice is displayed informing the user of access is for authorised user only and informs the user of some basic acceptable use of the system. An Active Directory password policy will implement complicated password, amount of logon attempts and lockout settings. Passwords will be hidden when typed.

Only devices owned by the College, or its recognised partner organisations, may be connected to the "wired" network.

Privately owned devices may only be connected to the "wired" network in special circumstances and must be approved by the Head of ICT prior to any attempt to

connect to the College network. College owned laptops must be enrolled onto Active Directory, have the necessary certification and configured and connect via a radius server.

BYOD devices may be connected to the college wireless network following the onboarding registration process.

All devices whether privately owned, or owned by other organisations, may require a baseline the hardware and software requirement to be allowed to connect. Usage must conform to College policies.

Regardless of ownership of a device, its connection to College networks is conditional on ICT having the right to inspect its configuration, test its security and monitor its network traffic in accordance with normal operational network management procedures.

Every networked device needs to be registered on the College Network Access Control device. Plugging a device into the network without registration will cause the device to be put into a quarantined vLAN until approved.

Networked devices on the "wired" network may be administered by ICT.

Administration of networked devices on the "wired" network is restricted to, and undertaken by, ICT Services.

Users of privately-owned networked devices are, and will be assumed by IT Services to be, responsible for ensuring that their devices are configured, actively maintained and used in accordance with College policies.

ICT can only connect devices to the "wired" network when the device meets all relevant requirements set out in the "Connecting devices to the network" section of this document.

Staff, Students and visitors are authorised to access the wireless network service after completing an automated registration process.

5. User access management

a) User registration and de-registration

Refer to User Management Procedure (Appendix B of this document)

b) User access provisioning

Users who require access to areas of the network, systems or applications need to have the necessary authorisation before they will be granted the appropriate permission.

Access to necessary Systems and Sites is usually granted at the start of employment following the User Management Procedure. Further access to Systems should be

granted by the System Owner who is responsible for approving and granting the necessary permissions. This would usually be done through the appropriate Helpdesk.

SharePoint and Teams Sites will be managed by the Site Owners. A Register of Sites, that identifies Owners, will be held by the Information Compliance Co-ordinator.

c) Management of privileged access rights

The allocation of privilege rights (e.g. local administrator, domain administrator, super-user, root access) shall be restricted and controlled and not provided by default.

Privileged access rights will be accorded following the principles of least privilege and will only be amended upon approval of either Head of ICT or Enterprise Applications Manager.

Authorisation for the use of such accounts shall only be provided explicitly, upon an ICT Helpdesk request from Senior Management.

Privileged accounts must not be used for standard activities unless it is otherwise impossible to operate the program.

All end user computers on the network will not have local administrator passwords set, but instead will have Microsoft Local Administrator Password Solution (LAPS) deployed.

Administrators of the New College Domain will use their own administrator account with the relevant permissions assigned. The central administrator account will not be used for day-to-day administration and only used when appropriate.

ICT systems that require administration access will again either have a unique username and password or will be linked to the users own administrator account.

d) Management of authentication information of users

All users are required to agree and sign the Acceptable Use Policy which clearly states users cannot disclose their password to any other user for any purpose.

New users or existing users who request a new password will be given a unique password by ICT and will be required to change it upon first login. If the request is via other means than physical attendance, challenge questions will be asked and verified (e.g. date of birth) before a new password is issued.

Where it is necessary for an account to be shared, ICT, or the individual designated as responsible for managing that account, must have full knowledge of the users that have been authorised to share the account.

e) Review of user access rights

System, Site and Data Owners will review users' access rights at regular intervals in order to ensure permissions are appropriate and secure.

On an annual basis Academic Registry will prompt owners of systems, network shares and sites[2] to review the permissions in their area.

Authorisations for privileged access rights for centralised systems will be reviewed by the Head of ICT at frequent and regular intervals.

System Owners, ICT and Academic Registry must ensure these checks are part of their 'working instructions' and records of completion are held as long as a normal request on the ICT helpdesk.

f) Removal or adjustment of access rights

The access rights of all employees and external party users to information and information processing facilities will be removed upon termination of their employment, contract or agreement, or adjusted upon change.

Processes are in place to ensure after any changes, such as promotion, movement of role, demotion or termination of employment user access rights should be reviewed and re-allocated.

Human Resources is responsible for notifying ICT of staff departure to allow suspension of access to their College account.

It is not usually permissible for a member of staff to access the account of a current member of staff. See the Policy on the Management and Monitoring of Electronic Communications, Internet and Telephones for detail.

h) User responsibilities

The Acceptable Use Policy informs all users of the need to keep login details confidential and under no circumstances to share the information to either individuals or corporations.

[2] Sites include those set up in MS SharePoint and MS Teams

Passwords are not to be written down and new passwords are issued after vetting. The user must then log in at the first opportunity at which stage the system will prompt the user to change the password.

Users of College IT facilities must not masquerade as another user or tamper with audit or activity logs or deliberately attempt to gain access to areas of the system which are restricted to them.

Provision of Single Sign On (SSO) or other authentication information management tools reduces the amount of authentication information that users are required to protect and thus can increase the effectiveness of this control. The college will implement SSO on systems where appropriate.

6. System and application access control

a) Access restrictions within systems

System Owners will be responsible for the management of access within their systems and must ensure only designated staff have access to the system admin functions. Access to permissions which allow deletion of information should be restricted.

A record must be held of current access permissions within Information Systems.

b) Secure log-on procedures for a system

Access to systems must require a logon. Users must authenticate onto a system and where possible systems will implement complicated password with encryption to circumvent any traffic analysing. Passwords will be hidden when typed and not displayed on screen.

If the system allows then a warning notice will be displayed on logon informing the user of access is for authorised users only and it may display acceptable use terms if possible.

Where possible any logon screen will have any system identifiers removed.

Both unsuccessful and successful logons will be logged where possible to identify user access and aid in identifying any attacks.

c) Password management systems

The college uses Active Directory for the domain logon system. The system has complex password requirement, with a maximum age of 180 days, last 5 passwords remembered and a minimum password length of 8 characters. Passwords are not displayed in plain text.

Systems should require complex passwords, a lockout when multiple password failures are detected and where possible passwords should be changed within a timeframe according to security guidelines.

Password management systems will be interactive and will ensure quality passwords. Wherever possible access to the college system and associated applications should be subject to Multi Factor Authentication.

d) Use of privileged utility programs

Privileged utility programmes must only be controlled by ICT. There are programmes which can override the application and authentication controls of other systems.

All programs, where applicable, should have a requirement for credentials. Additionally, programs are distributed by ICT on a requirement of need where possible. This can be either by having specific builds for departments and/or the control and distribution of applications via group policy and permissions. Micro segmentation is also deployed within the college, this aids control of who is able to access utility programs.

e) Access control to program source code

Access to any college proprietary program source code will be controlled on the basis of business and security requirements.

An access to source code process for every system/database must be created, documented, approved, enforced and communicated to all relevant employees and partner organisations.

F. Cryptography

1. Objectives

To ensure proper and effective use of cryptography[3] to protect the confidentiality, authenticity and/or integrity of information.

This policy further requires that any applicable governing regulation, contractual requirement or other standard will be followed with respect to cryptography.

2. Responsibilities

The Head of ICT is responsible for this policy.

This policy applies to all New College Durham employees, affiliates, subsidiaries, contractors, and other personnel or entities subject to the policy and requirements of the College.

3. Policy for Cryptographic Controls

When analysing whether data needs to be protected with cryptography, it is important to realise that data needs to be protected when in transit and when at rest. Whether encryption is needed will be decided based on the importance of the information and the risks for the type of storage or transit.

a) Approved encryption methods for data at rest

When storing sensitive data uses of Encryption will be considered where necessary.

b) Encryption methods for data in motion

The transfer of sensitive data will only take place through a secure channel. A secure channel is an encrypted network connection. ICT will advise where necessary. The user should be aware of the data connection being used to transmit sensitive data and if encryption is enabled for that connection.

Encryption will be required for:

- The transport of sensitive files
- Access to sensitive data via a web site, web application or mobile app. Encryption is required for accessing sensitive data from anything with a web interface, including mobile devices (i.e. use of HTTPS to encrypt sensitive data). Any website published by the college with by HTTPs.

[3] **Cryptography** is the technology used to encrypt and de-crypt data to protect it from unauthorised access

- All network traffic for remote access to the College virtual desktop environment
- Privileged access to network or server equipment for system management purposes (e.g. network switches) will be encrypted and services such as Telnet will be disabled.

c) Encryption of Email

Where any sensitive Data Handling is required via email then the appropriate encryption via software or the use of certificates will be implemented.

d) Use and management of SSH keys

Web servers (or devices with a web interface) that support secure (HTTPS) connections will have a SSL certificate installed.

4. Policy for Key Management

All encryption keys covered by this policy are protected to prevent their unauthorised disclosure and subsequent fraudulent use.

a) Secret Key Encryption Keys

Keys used for secret key encryption, also called symmetric cryptography, are protected as they are distributed to all parties that will use them. During distribution, the symmetric encryption keys must be encrypted using an RSA key of at least 2048 bits.

b) Public Key Encryption Keys

Public key cryptography, or asymmetric cryptography, uses public-private key pairs. The public key is passed to the certificate authority to be included in the digital certificate issued to the end user. The digital certificate is available to everyone once it issued. The private key should only be available to ICT where the digital certificate is issued.

Keys are generated securely, stored in a secure way and destroyed when no longer needed.

c) Loss and Theft

The loss, theft, or potential unauthorised disclosure of any encryption key covered by this policy must be reported immediately to ICT, which must then apply proper actions that will be required regarding revocation of certificates or public-private key pairs.

Staff should consider the use of encryption whenever the confidentiality of an asset is important. Cryptography can be used when sending data and when storing data, both can be relevant.

Confidential and privacy sensitive information that is stored on removable media such as DVD's and USB sticks must be protected via encryption. Devices such as laptops and mobile phones will have encryption enabled where possible.

ICT will ensure that that key management is in place. You need to make sure keys are generated securely, stored in a secure way and destroyed when no longer needed. ICT will also ensure that multiple people have access to keys to avoid loss of keys when people leave the organisation.

d) Selecting strong cryptographic algorithms

It is important to select a strong algorithm when creating certificates to protect College assets, VPN or websites.

Where feasible the College will use the following strong algorithms:

- Symmetric encryption: AES (four sizes, 128 bits is already good). Also suitable according to ENISA are RC6, Serpent, Twofish

- Asymmetric encryption RSA (2048 bit recommended, at least 1200 bits required). Also suitable according to ENISA is Elliptic Curve cryptography with at least 256 bits key.

- Hash functions: SHA2 (four sizes, 256 bits is recommended).

- Digital signatures: RSA (good 2048 bits, ok 1200 bits).

Encryption Key Management will to be considered otherwise keys can be compromised and disclosure of private keys use to secure sensitive data and hence, compromise of the data.

5. Process for exceptions

Any exceptions to the above must be approved by the Head of ICT in writing with detailed reasonings why any exception is required. The exception will be considered against the possible security implications for the college and what mitigation, if possible can be put into place.

G. Physical and Environmental Security

1. Objectives

To prevent unauthorised physical access, damage and interference to the organisation's information and information processing facilities.

2. Responsibilities

The Senior Leadership Team is responsible for maintaining a Disaster Recovery Plan which details specific responses to environmental threats.

The Director of Estates and Facilities is responsible for maintaining a policy on the security of College premises, including contractor management.

The Director of Human Resources is responsible for policies on the appropriate notification of changes to posts.

The Administration Manager is responsible for policies in relation to visitors.

The Purchasing and Contracts Manager will ensure a secure process is in place for delivering and loading areas.

Heads of Department will be responsible for reviewing physical access in their areas.

3. Policy for Secure areas

The College's security measures are described in the Estates Policy. A 24-hour security presence is maintained.

Physical access across the college campus to server rooms and racks rooms are restricted to ICT, Estates and Security. No other staff member or student should access these areas. These areas will not have external windows.

Physical access to the Records Store is restricted to specific staff within Academic Registry, Estates and Security.

Physical access to information processing areas (workrooms and offices) is controlled by keys which are registered by Security to individual users.

Keys and Access Fobs are only available to staff who require access and records are held by security. Use of Fob access is monitored and an audit trail is maintained.

Visitors are subject to policies and procedures maintained the Administration Manager.

Changes to physical security due to a change of post will be the responsibility of the relevant department head.

Within ICT secure areas the scope of the contractors responsibilities is determined by ICT, described in the contract and subject to Health and Safety procedures.

Entry to the College for the purpose of delivery or collection of goods is monitored by the Contracts and Purchasing Unit. Deliveries are supervised at all times.

4. Policy for Equipment

a) Equipment siting and protection

The college has two server rooms, a main server room located in the main building and a smaller server room located in the Sports building. The primary server room is located behind locked doors, accessible only via key and fob. The key and fob distribution/room access programming is controlled by the Security department and all recipients must sign for the key and/or fob. The request for a recipient to be given the key and fob must be approved by the Head of ICT. The smaller server room is accessed by key only.

Both the primary and the backup server room are air conditioned with redundancy and the room temperatures are monitored with alerts sent to primary contacts should a defined threshold be breached.

All edge cabinets are placed in small, ventilated rooms and are protected by locked, unmarked doors. Access to the keys to the cab rooms are controlled by Security and the request for a recipient to be given the key must be approved by the Head of ICT.

b) Supporting utilities

The server rooms are equipped with alternative methods of redundant power. Uninterruptible Power Supplies (UPS) are present which provides power should the primary power source fail and also protects the equipment from power spikes, surges, fluctuation etc. The primary server room is also linked to a diesel power generator which can supply electricity over an extended period of time.

c) Cabling security

Power and telecommunication lines are underground and once presented to the college building, they are in secure runs in the ceiling and below the floor. Cable management prevents any interference. Patch rooms, maintenance cabinets etc. are all locked and accessible only by the relevant personnel.

d) Equipment maintenance

All equipment that are used by the college, such as the UPS and Fire Suppression systems, are supported, maintained and inspected by appropriate 3rd party contractors. Equipment is serviced according to the schedules and tested before being placed into operation after maintenance. These systems are monitored by personnel in the college and some communicate with the 3rd parties direct who monitor and triage the systems remotely.

e) Removal of assets

Any person who requires assets that are portable and may at any time be offsite, or the borrowing of equipment for home use, are required to sign and document an Equipment Loan Form. This form will record what equipment has been loaned, the asset number, who it has been loaned to, the duration of the loan and an approval signature.

f) Security and removal of equipment and assets off-premises

Equipment taken off site should not be left unattended should be secured at all times. If possible the device should be password protected and encrypted.

Any equipment must be stored as appropriate to the device and protected from the elements.

No equipment should be directly swapped or given to other staff members without ICT approval. All devices should be handed back to ICT and then redistributed to other members of staff.

g) Secure disposal or re-use of equipment

Any equipment that is disposed of must be destroyed or securely wiped before leaving the premises. Any disposal companies hired by the College must be certified in the secure and safe disposal of electrical equipment.

Any equipment that is used off-site must be encrypted where possible. All laptops will be encrypted, removable media with college information will be encrypted and mobile phones will be protected by encryption.

h) Unattended user equipment

ICT will ensure that any unattended equipment that is used by the department will be logged off when the task is completed. All remote sessions will be terminated gracefully.

Access to unattended equipment will be granted via password or security pin. All devices will have a secure logon system.

i) Clear desk and screen policy

Where a member of staff manages personal or confidential data their manager should ensure that they have adequate processes and security in places to ensure the protection of that data.

This may include consideration of the siting of the information processing facility and/or the provision of lockable drawers and cabinets and screen guards to ensure information is not left on desks or disclosed inappropriately on computer screens.

H. Operations Security

1. Objectives

To ensure correct and secure operations of information processing facilities.

To ensure that information and information processing facilities are protected against malware.

To protect against loss of data.

To record events and generate evidence.

To ensure the integrity of operational systems.

To prevent exploitation of technical vulnerabilities.

To minimise the impact of audit activities on operational systems.

2. Operational Procedures and Responsibilities

ICT will prepare appropriate documented operating procedures for all operational information systems, to ensure a correct and secure operation. Documented procedures are required for system development, maintenance and testing work, especially if it requires the support or attention of other organisational functions.

All operating procedures are formal documents and any changes are to be authorised by the process owner.

Responsibilities and procedures for the management and secure operation of College resources and all connected PCs, laptops and networks are to be established. This is to include appropriate operating instructions and incident response procedures.

a) Documented operating procedures

The College ICT personnel are responsible for the installation and configuration of systems within the college. Where 3rd party contractors are carrying out the installation the ICT will supervise and supply all relevant details to the 3rd party.

IT will install and test security patches prior to implementation of the new equipment (where practical). See the ICT Patch Management Policy for more detail.

ICT shall ensure that vendor-supplied patches are routinely acquired, systematically tested, and installed promptly based on risk management decisions.

ICT shall remove unused software, system services, and drivers (commonly known en masse as 'bloatware'), installing only what is required.

ICT and System Owners shall install and enable security features from the approved vendor prior to placing in a live environment. Relevant logging shall also be enabled. User privileges shall be set following the concept of providing the minimum amount of access required.

The use of passwords shall be enabled in accordance with the software manufacturer/developer's guidance.

ICT shall disable or change the passwords of default accounts.

All owners and ICT shall seek and implement best practices for securing that particular platform.

b) Change management

For detail see the ICT Change Management Policy.

c) Capacity management

The hard drive capacity of the College's file servers will periodically be monitored by ICT.

If free space on the file server hard driver becomes less than or equal to 20% of total capacity, users are requested to remove redundant files. If this is not possible, extra hard disk space will be installed.

Projections of future requirements should be made to prevent any bottlenecks and dependencies on the services by the College or third party organisations.

d) Separation of development, testing and operational environments

ICT will ensure that where possible development, test and operational systems are segregated in order to prevent unauthorised access, modification or misuse of information or services.

For each information or service, the need for separating development, production, test and operational facilities is determined through risk assessment.

The following levels of separation are considered and implemented, as appropriate, to mitigate any of the risks:

- Development and production software should, where possible, be run on different servers and isolated/segregated where feasible
- Development and test work are separated as far as possible.

- Access to compilers, editors and other system utilities are separated from operational systems when not required.
- Different logon procedures are used for production and testing systems, to reduce the risk of confusion or error. Users are encouraged to use different passwords for these systems.
- All domains/environments must be appropriately protected. Additional technology, both hardware and software, will be required to duplicate the development environment.

3. Protection from malware

ICT will deploy appropriate controls to mitigate the risks of viruses and malicious software (also known as 'malware').

All servers, PCs and laptops will have antivirus software installed. The software is to be configured to scan all files for viruses. The software should automatically check for updates on a daily basis. Additional features such as Behavioural Monitoring, Predictive Machine Learning, Suspicious Connections etc. shall be enabled.

The decision to accept or reject email will normally be taken by the individual recipient. However, there are cases where the College will reject messages to protect the network or for policy reasons. This could include messages containing material that is threatening, abusive or otherwise unlawful, or which would be considered as coming under the classification of prohibited use under the Acceptable Use Policy. This blocking is done via email security appliances, managed by ICT.

The College subscribes to services that help to identify emails that are malicious, Spam, Phishing etc. but these services cannot be guaranteed to be 100% successful and they may occasionally falsely identify valid messages as being suspect.

Incoming email will be subject to scanning and classification by the email security systems. The signatures used to analyse the content are dynamically updated on a regular basis by the email security appliance vendors.

All email messages should be treated with caution, links should not be followed and attachments not downloaded unless the recipient is 100% confident of the originator and is expecting the email.

Emails quarantined by the system will send a message to the user's mailbox to notify them that a suspected message has been detected. ICT will review and decide whether the email is legitimate or otherwise. If legitimate the email will be released, if not it will be deleted.

Employees will be provided with training on the use of these controls and made aware of the types of malware and the threats that it poses.

The college employs the use of services from the JANET/JISC ISP to filter traffic before the gateway. This includes mitigation from attacks like DDOS (Distributed Denial of Service, where a 'hacker' attempts to disrupt traffic on a server), traffic filtering and IP scanning and concerted attacks.

4. Backup

For more information see the ICT Business Continuity Plan.

- ICT will ensure that adequate back up facilities of the College's internal systems are provided to ensure that all essential business information and software can be recovered following a computer disaster or media failure:

- A minimum level of back up information (together with complete records of the backup copies and restoration procedures) are stored in a remote location, at a sufficient distance to escape any damage from a disaster at the main site. The college has implemented a '3-2-1 strategy' which means there will be 3 backup copies taken on different storage media.

- Back-up copies of essential business data, software and log files are to be taken at a frequency determined by the Data and System Owners in discussion with the Head of ICT. Back-up arrangements are to meet the requirements of business continuity plans.

- Back up information systems are regularly tested to ensure that they can be relied upon for emergency use when necessary.

- Restoration procedures are regularly checked and tested to ensure they are effective.

- Back-up data is given an appropriate level of physical and environmental protection, consistent with any necessary standards. Back-up data is to be regularly tested to ensure its viability for recovery when required.

5. Logging and Monitoring

a) Event logging

ICT are responsible for monitoring access or if a security breach has been detected or is suspected. Access to events logs will be restricted to security administrators.

Events logs will monitor all system events, log on and log off times and include:

- Authorised access:
- user ID
- date and time of event

- Privileged operations:
- use of Administrator or Root accounts which allow privileged access to servers and systems
- system start up and stop
- all changes to privileges and user rights
- Unauthorised attempts to access information and information systems
- Unauthorised attempts to system commands

For each audited event, the Audit Log Record will contain at least the following:

- Date, time and nature of event
- User, process or PC ID (the user ID and the physical identifier of the PC involved will be used to assist in the investigation of any specific security related incident)
- Success or failure of the event
- Identity of the object being accessed (e.g. sufficient information is recorded to uniquely identify which database records are affected)

System access controls must be set to ensure that only the IT support staff have read access to audit logs and only senior ICT staff have delete/archive access to audit information.

b) Administrator and operator logs

ICT will where possible maintain a log of all work carried out. Operator logs will include, as appropriate:

- Systems start and finish
- System errors and corrective action taken
- Confirmation of the corrective action taken
- Name or ID of the person making the log entry

c) Clock synchronisation

College devices are synchronised to an approved internet based time server.

6. Control of operational software

ICT will be responsible for the upgrading of core operational software, applications and libraries. No development code should reside in the operational environment.

Any non-standard and bespoke software will be assessed for compatibility and suitability via the appropriate processes.

Post implementation of new network software should be subjected to testing and monitoring to highlight any unexpected issues. Backups of the configuration and software should be maintained in case a rollback is required.

Third party software should be the supported version wherever possible.

7. Technical vulnerability management

a) Management of technical vulnerabilities

Microsoft software and operating systems will be patched on a monthly basis. Other operating systems that require patching will be patched in suitable windows. Any critical or high security patches will be dealt with on an individual basis upon an internal risk assessment.

b) Restrictions on software installation

ICT will be the only department authorised to install and deploy software within, and on devices belonging to, New College Durham.

8. Information Systems Audit Controls

The College will determine the value of auditing and develop a scope for the audits addressing relevant business risks that merit audit.

The audits will focus on the College information security to protect information assets that are relevant to executing critical business functions with an audit scope enabling effective and efficient planning of the required activities

Penetration tests will be planned and agreed in a way they minimise any risks to disruption business operations (e.g., by being performed out of business hours, by covering only part of the most critical systems at a time, etc.).

Audits can be achieved through the log analysis, system's configurations review, network traffic monitoring, Firewall and SIEM monitoring.

I. Communications Security

1. Objectives

To ensure the protection of information in networks and supporting information processing facilities.

To maintain the security of information transferred within an organisation and with any external entity.

2. Responsibilities

The Data Protection Officer, Director of Human Resources and Head of ICT are responsible for the policy on the Management and Monitoring of Electronic Communications, Internet and Telephones which contains policy information covering the use of systems and equipment for information transfer.

The Data Protection Officer is responsible for the policy on Records Management which contains policy statements on retention and disposal guidelines and the Use of Electronic Signatures Policy.

The Head of ICT is responsible for ensuring contracts with third parties that have access to the College network contain appropriate levels of confidentiality.

The contract owner is responsible for ensuring contracts with third parties that describe the use of College data contain appropriate levels of confidentiality and are reviewed according to the Data Protection Policy.

3. Network security management

a) Network Controls

Connections to the College's private network infrastructure are made in a controlled manner. All network switches are hardened against unnecessary protocols and services and can be accessed only using a Secure Shell cryptographic network protocol and controlled by an Access List.

Network management is critical to the provision of College services and must apply the following controls:

- Operational responsibility for networks will where possible be separate from computer operations activities.

- There must be clear responsibilities and procedures for the management of remote equipment and users.

- Where appropriate, controls must be put in place to protect data passing over the network (e.g. encryption).

- The network architecture must be documented and stored with configuration settings of all the hardware and software components that make up the network. All components of the network should be recorded in an asset register.

b) Security of network services

All hosts must be 'security hardened' to an appropriate level as decided by the Head of ICT. Operating systems will have their network services reviewed, and those services that are not required will be disabled.

The College deploys next-generation perimeter firewalling with Intrusion Protection System providing deep-packet inspection to attempt to mitigate a wide range of network attacks.

Web filtering is in place to block access to malicious destinations before a connection is established, using constantly updated signatures. Access to malware, ransomware, phishing and command & control callbacks over any port or protocol are blocked. This service also permits the blocking of categories or protocols of web traffic where deemed appropriate

Wireless Networks must apply controls to protect data passing over the network and prevent unauthorised access. Encryption will be used on the network where possible to prevent information being intercepted. Minimum mandatory requirements will be adhered to in configuration of any wireless network functionality.

c) Segregation in networks

The college uses appropriately configured firewalls to segregate external traffic from internal and has implemented a secure area (DMZ) for external facing services. Any external traffic which requires access to a LAN based server must be protected behind a web publishing server or a reverse proxy.

The college will employ the use of Micro Segmentation techniques to segregate internal machines and networks from devices, servers or systems that do not need to communicate with each other. The college deployed endpoints are subject to segregation on the network via various means. These include physical LAN separation, vLANs and Micro segmentation.

Extensive use of vLANS are deployed within the network, these separate and isolate traffic including the segregation of services such as Wi-Fi. Wi-Fi Secure Access Policies ensure we can control policies to the end user depending on who the user is and whether they connect to a managed or their own device.

Perimeter and internal firewall rules are periodically reviewed by ICT on an annual basis.

4. Information transfer

The College policy on the Management and Monitoring of Electronic Communications, Internet and Telephones provides information on the non-technical measures taken to protect information when communicated by eMail, sharing files and messages within M365 and by telephone.

Personal or confidential data must not be communicated by email. Guidance on how to share information via OneDrive is available from the staff intranet.

Arrangements for information transfer should be detailed in the relevant Data Sharing Agreement or Contract as described by the College's Data Protection Policy.

Appropriate levels of confidentiality should be applied within relevant contracts.

J. System Acquisition, Development and Maintenance

1. Objectives

To ensure that information security is an integral part of information systems across the entire lifecycle. This also includes requirements for information systems which provide services over public networks.

To ensure that information security is designed and implemented within the development lifecycles of information systems. Information security is integrated into the creation, modification, implementation and expansion by ongoing security practices such as the management of vulnerable points and securing system files. For applications, information security can be applied to the validation of data input and output and by encoding information using electronic keys.

To ensure the protection of data used for testing.

2. Responsibilities

The Head of ICT is responsible for ensuring the systems purchased, developed and used within the College network have the appropriate levels of technical security.

System Owners will be responsible for providing information to the Head of ICT to enable an Information Security Impact Assessment (ISIA) to be carried out.

3. Security Requirements of Information Systems

When purchasing a new system that processes personal information, a Business Case must be presented to the Business Systems Groups and should ultimately be approved by the SIRO.

System Owners/Head of ICT must conduct an ISIA during the requirements phase when developing, implementing major changes to, or acquiring an information system, to:

- Identify the security requirements necessary to protect the information system; and,
- Assign a security classification to the information, assess the risks associated and work on mitigation where possible.

The Data Owner/ICT must ensure that information system development or acquisition activities test the information system to verify that it functions as intended, enforcing change control processes to identify and document modifications or changes which may compromise security controls or introduce security weaknesses and ensure authentication, access control, etc. are established.

System owners must ensure that sufficient controls are in place to mitigate the risk of information loss, error or misuse from information systems. Information systems must be assessed to verify the adequacy of, and document the details of, the security controls used.

Where feasible different tiers of applications need to be separated across different platforms or servers (e.g., web interface must be on a different server from the data base). Micro segmentation and East/West traffic must also be considered and acted upon.

Information systems should have a documented and maintained System Security Plan. The Plan should include:

- A summary of risks identified in the Security Threat and Risk Assessment
- Roles and responsibilities for the system and security management

Specific procedures and standards used to mitigate risks and protect the information system;

The College will also monitor logging through software and services including network monitoring software, the use of Syslog servers, external SEIM monitoring, Windows event viewers and other logging systems.

Where “apps” are used for processing information, an ISIA must be completed before the use of the app. Apps should be downloaded only from official vendor provided app stores via Mobile device Manager.

Employees should always consider potential risks before downloading apps on their mobile devices. Some apps have been found to have harmful effects and may inadvertently release information from the mobile device to third parties.

Tests where possible should:

- Demonstrate information security requirements are derived from compliance requirements in information security policies, guidelines and regulations;
- Demonstrate a Data Protection Impact Assessment (DPIA) has been completed for all information systems with personal information;
- Demonstrate users and operators have a clear understanding of roles and responsibilities;
- Ensure multi-factor authentication is used commensurate with the sensitivity and value of the information;
- Develop Business Continuity Plans and supporting Disaster Recovery Plans.

When purchasing a cloud solution that will host any college data then security must be addressed and must be assessed by ICT before approval and purchasing. ICT will review the third party’s information security arrangements and provide written

authorisation for the processing to commence. There is a checklist included at Appendix A which should be completed if the third party cannot produce adequate documentation.

4. Security in development and support process

System Owners must ensure that software and systems developed internally follow established policies, standards and best practices for secure development process. The established policies and standards must be applied consistently to all developments within the College.

A secure development process is a necessity in developing a secure information system. Within a secure development life-cycle of information systems, the following aspects must be considered:

- Security of the development environment;
- Security in the software development methodology;
- Secure coding guidelines for each programming language used;
- Inclusion of security requirements starting from the design phase;
- Security checkpoints within the development milestones;
- Security in the version control and updates;
- Required application security knowledge; and,
- Developer capability of avoiding, finding and fixing vulnerabilities.

a) Secure Development

Secure programming techniques must be used both for new developments and in code re-use scenarios where the standards applied to development may not be known or are not consistent with current best practices. Secure coding standards must be considered and where relevant mandated for use.

Program code must not be altered unless authorised to do so;

Any variations to program code must be documented; and,

All changes to existing code must ensure applicable standards have been applied for program security.

If development is outsourced, the College must obtain assurance that the external party complies with the policies for secure development.

b) Changes to software for operational information systems

System Owners must implement a change request which must:

- Require that change requests originate from authorised employees;
- Perform an impact assessment of the proposed modifications;

- Document fallback plans;
- Document approval of changes proposed prior to the commencement of the work;
- Document the acceptance tests and approval of the results of acceptance testing;
- Update any system, operations and user documentation with the details of changes;
- Maintain version control for all changes to the software; and
- Log all requests for change.

c) Changes to the operating system

ICT or 3rd party stakeholders must notify information System Owners and other affected parties of operating system changes to allow:

- Sufficient time for the review and testing of information systems prior to implementation;
- Review of System Security to ensure information systems will not be compromised by the change;
- Information system testing with the changes to the operating system in a test environment;
- Update of business continuity plans if required.

d) Applying vendor supplied patches and updates

A software update management process must be maintained for off-the-shelf purchased software to ensure:

- The most up-to-date approved patches have been applied; and,
- The version of software is vendor supported.

e) Outsourced engineering security

System Owners must ensure that contracts and other binding agreements incorporate the college security principles and procedures for outsourced information systems or any developments for the college.

f) Outsourced information system development

System and Data Owners must consider the following when outsourcing information system development:

- Procurement policy for licensing, ownership and intellectual property rights;
- Escrow arrangements in the event of the failure of the external party;
- Testing of the information system for common vulnerabilities and malicious code;

- Rights of access for audit and certification of the quality and accuracy of the work; and,
- Contractual requirements for quality and security functionality of the information system.

System and Data Owners must ensure that the outsourced information system meets the requirements defined in this policy (see Appendix A).

g) Testing during development

System and Data Owners must ensure that new and updated systems undergo thorough testing and verification during the development processes. A detailed schedule of test activities, inputs and expected outputs under a range of conditions must be prepared as part of testing and verification processes.

Independent acceptance testing must be undertaken to ensure that the system works as expected and only as expected. The extent of testing must be in proportion to the importance and nature of the system.

h) System acceptance process

System Owners must ensure that system acceptance criteria are defined as part of the system development and acquisition process.

Prior to implementing new or upgraded information systems, System and Data Owners must ensure:

- Acceptance criteria are identified including privacy, security, systems development and user acceptance testing;
- Security accreditation to proceed with implementation is attained.

A DPIA must be completed for new or upgraded information systems.

5. Protection of test data

System Owners must implement procedures to ensure that:

- Using test data extracted from operational information systems is authorised and logged to provide an audit trail;
- Test data is protected with appropriate controls; and,
- Data from operational information systems is removed from the test environment once testing is complete.

Sensitive or personal information from operational information systems should not be used as test data unless it is essential to ensure the functionality of the product and then only if the risk has been considered in the project's DPIA. Where personal

or sensitive data must be used for testing purposes, sensitive details and content should be removed, depersonalised or de-identified.

If sensitive or personal data from operational systems has to be used for testing purposes, the following conditions must be met:

- System and Data Owners must provide a strong business case for the use of operational data containing sensitive or personal data for testing purposes;
- DPIA must be completed specific to the use of operational data in test;
- Use of production data for testing purposes must be approved by a Project Board
- The data to be used for testing purposes in the production-like environment must be handled with the same care and diligence as in the production environment with the same or more stringent security controls;
- Where sensitive or personal information is used, System Owners must ensure that only information fields necessary for testing be used (e.g., if successful results can be achieved using the last four digits of a National Insurance Number, avoid using the whole number);
- System Owners must ensure that the smallest subset of sensitive or personal information is used, which is necessary to complete the testing (e.g., if successful results can be achieved using a minimum number of records);
- After testing activities are completed, System Owners must ensure that test data is securely erased
- The documentation must demonstrate why the use of sensitive or personal information is necessary.

Live data, personal or otherwise should not be used for testing unless with the agreement of the Data Owner in full knowledge of any risks involved.

'Real' Personal Data must not be used for creating training materials.

K. Supplier Relationships

1. Objectives

To ensure protection of the organisation's assets that are accessible by suppliers.

To maintain an agreed level of information security and service delivery in line with supplier agreements.

2. Responsibilities

Supplier contracts will be concluded in line with the responsibilities and processes described in the Data Protection Policy.

The Head of ICT will be responsible for assuring the level of compliance for any third party processing data on behalf of the College.

The Data Protection Officer and Purchasing and Contracts Manager will be responsible for maintaining and engaging relevant contract clauses in the College's Terms and Conditions of Contract.

The contract owner will be responsible for ensuring appropriate consultation takes place to ensure the correct level of protection is applied within the original contract and any subsequent variations.

3. Information Security in Supplier Relationships

Where a third party is required to process data on behalf of the College, the Contracts and Purchasing Unit must ask the Head of ICT to review the third party's information security arrangements and provide written authorisation for the processing to commence. There is a checklist included at Appendix A which should be completed if the third party cannot produce adequate documentation.

The College will also utilise data sharing agreements or schedules in all situations when the information being disclosed can be classified as personal or confidential data. These will detail the College's instructions to the supplier or sub-contractor on how to manage the data in situ and under transfer and will include responsibilities in the event of security incidents and an obligation to protect NCD data. The College's standard data processing schedules are held in the standard 'terms and conditions of contract', held by the Contracts and Purchasing Unit.

All authorised third parties who require access to IT infrastructure will also be directed to read this Policy and the Data Protection Policy.

Access to College IT facilities by third parties for the purposes of system support is not provided until a copy of the Acceptable Use Policy for System Support has been

signed by an appropriate representative. See Appendix C for the workflow showing when it will be appropriate to grant a third party access to the College Network and/or Information Systems.

Where a contract owner is responsible for monitoring and managing supplier or sub-contractor service delivery they will periodically make checks to ensure the supplier or sub-contractor is meeting their contractual obligations.

The Appendix A checklist may be used to verify the level of service originally agreed is being maintained.

L. Information Security Incident Management

1. Objectives

To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.

2. Responsibilities

Data breaches will be logged, investigated and managed according to the responsibilities and processes described in the Data Protection Policy.

Security weaknesses will be raised to the SIRO by the Head of ICT.

3. Management of information security incidents and events

Any incident involving the unauthorised accessing, disclosure or loss of information within the College must be reported as soon as possible either via the ICT Helpdesk to the Head of ICT or to the Data Protection Officer.

If the Head of ICT is implicated in proceedings, notification of the incident should be made to the SIRO. If both the SIRO and the Head of ICT are implicated, the incident should be reported to the Principal.

Where personal data has been lost, disclosed or accessed by unauthorised persons, the Data Protection Officer will investigate and make recommendations to improve security as per the Data Protection Policy.

4. Management of information security improvements

Employees are encouraged to report suspected security weaknesses to the Head of ICT, either directly or via the ICT Helpdesk, these may include:

- Ineffective security controls
- Breach of information integrity, confidentiality or availability expectations
- Human errors
- Non-compliance with policies or guidelines
- Breaches of physical security arrangements
- Uncontrolled system changes
- Malfunctions of software or hardware
- Access violations

The Head of ICT will ensure that appropriate technical and procedural measures are taken to address identified security weaknesses.

M. Information Security Aspects of Business Continuity Management

1. Objectives

Information Security continuity is embedded in the College's Business Continuity Plan.

To ensure availability of information processing facilities.

2. Responsibilities

The Head of ICT is responsible for this policy.

3. Planning information security continuity

The Head of ICT alongside the System Owners must ensure business continuity and recovery plans address information security requirements consistent with the classification of the information.

System Owners/Head of ICT should perform a business impact analysis for information security aspects to determine the information security requirements applicable to adverse situations.

Information security requirements remain the same in adverse situations, compared to normal operational conditions.

The college has a Disaster Recovery Plan which is informed by the ICT Business Continuity Plan and the ICT Business Impact Assessment [not yet published].

4. Redundancies

Information security controls that have been implemented must continue to operate during an adverse situation. If security controls are not able to continue to secure information, other controls must be established, implemented and maintained to achieve an acceptable level of information security.

The implementation of system redundancies can introduce risks to the integrity or confidentiality of information and information systems, which need to be considered when designing information systems.

System Owners must identify business requirements for the availability of information systems. Where the availability cannot be guaranteed using the existing systems architecture, redundant components or architectures must be considered.

Where applicable, redundant information systems must be tested to ensure the failover from one component to another component works as intended.

N. Compliance

1. Objectives

To avoid breaches of legal, statutory, regulatory or contractual obligations related to information security and of any security requirements.

To ensure that information security is implemented and operated in accordance with organisational policies and procedures.

2. Responsibilities

The Data Protection Officer is responsible for the College's policy on Copyright and Intellectual Property, Data Protection and Records Management.

The Information Compliance Co-ordinator is responsible for planning training in Data Protection and Information Security for all staff on an annual basis.

The Head of ICT and the System Owner for the College's Student Information System will ensure annual 'health checks' are scheduled in line with the requirements of the College's funding provider.

3. Compliance with legal and contractual requirements

The detail of how the College manages compliance with the law is contained within the policies mentioned above.

The College manages compliance with this Information Security Policy with the assistance of our Internal Auditors and may from time to time contract with specialist companies to undertake specific technical testing.

On an annual basis all staff are required to renew their training in Data Protection and Information Security and reminded of their obligation to comply with these college policies.

On an annual basis 'health checks' will be undertaken on systems which the College uses to process data defined in the ESFA funding contract.

Cryptographic controls are used in compliance with relevant agreements, legislation and regulations.

Appendix A: Supplier Questionnaire

Please see separate document published by ICT

Appendix B: User Management Procedure

Please see separate document published by ICT

Appendix C: Third Party Access to Data