Cyber 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	**Cyber Security Policy**
Document Owners	**Executive Director of ICT and Corporate Services / Head of ICT**

Directorates and Departments affected by this Procedure	**All staff and students**
Procedure Effective From	**Jan 2022**
Next Review Date	**Jan 2027**

Contents

1. Introduction 2
2. Purpose 2
3. Responsibilities 2
4. Relationship with existing policies and standards 3
5. Identification and definition of assets and processes 3
6. External Support 4
7. Risk Mitigation 4
8. Security Controls (practical measures) 6
9. Security Monitoring 8
10. Evaluation and Review 9

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:

icthelpdesk@newdur.ac.uk

Equality Impact Assessed:
Accessibility Checked:

1. Introduction

The risk of data theft, scams, a security breaches can have a detrimental impact on the College's systems, technology infrastructure, and reputation. This Cyber Security Policy is relevant to all students and to all staff and external parties employed or otherwise contracted to work at the College.

2. Purpose

The purpose of this policy is to protect the College's data and infrastructure, outline protocols and guidelines that govern cyber security measures, and define the rules for acceptable use.

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 systems and networks are mitigated, it is the policy of the College to ensure effective cyber security procedures are in place.

3. Responsibilities

a) Management

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 risk management at the highest level of the College's leadership team.

b) Policy Ownership

The Executive Director of ICT and Corporate Services and the Head of ICT are jointly responsible for the definition, maintenance, review, and communication of cyber security policies; as well as maintaining associated guidelines and promoting compliance with them; and providing training materials 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 Executive Director of ICT and Corporate Services and the Head of ICT will also have joint responsibility for liaising with suppliers to ensure security information and alerts are identified and documented.

c) Compliance

Compliance with this Policy and any associated procedures is compulsory for all users accessing College networks. A user who fails to comply with the Policy may be subjected to formal action under the College's prevailing procedures. It is the responsibility of Heads of Departments/School and their Senior Management to ensure that staff and students are aware of the existence of this policy and understand the contents and the obligations it conveys on users.

d) ICT Infrastructure Ownership

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

e) Suppliers

External suppliers who are contracted or otherwise notified that they have responsibilities in relation to the security of college systems and infrastructure are responsible for carrying out their contractual obligations.

4. Relationship with existing policies and standards

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

The following College policies and plans should be read in conjunction with this Cyber Security Policy:

- Information Security Policy
- ICT Business Continuity Plan
- ICT Disaster Recovery Plan
- ICT Equipment Loans Agreement
- ICT Equipment Replenishment Policy

5. Identification and definition of assets and processes

a) ICT Infrastructure

ICT infrastructure is identified and resourced by the Executive Director of ICT and Corporate Services and the Head of ICT and is based on priorities detailed in the ICT Strategic Plan and the ICT Business Impact Assessment.

b) Classification

The College determine the relative importance of the level of protection that will be given to the asset by utilisation of a classification given to the asset in the registration process. This classification is derived from the Business Impact Risk Assessment.

c) Segregation of duties

The College will segregate conflicting duties and areas of responsibility to reduce opportunities for unauthorised or unintentional modification or misuse of assets. The College systems/process will ensure that no one can access, modify, or use assets without authorisation or detection.

6. External Support

Cyber threats are recognised and mitigated through college security procedures and protocols. The College subscribe to the Jisc Service who provide our digital infrastructure and network. Jisc's primary function is to monitor and resolve any security incidents that occur on the network and work closely with the education community to detect, report, and investigate incidents that pose a threat to the security of information systems.

Other services such as the National Cyber Security Centre (NCSC), Police Cyber Alarm Scheme, Association of Colleges (AoC), the Department for Education (DfE) and our external suppliers, provide information and alerts to support our ongoing security monitoring.

7. Risk Mitigation

A cyber-attack risk is listed in the College's strategic risk register which reflects that the impact of a cyber-attack would be catastrophic in nature. The evolution of the criminal fraternities focused on Cybercrime makes the probability of such attacks at the College as "possible". The College has adopted the following mitigation and controls in response to these clear and present risk: -

a) Multi Factor Authentication (MFA)

MFA is a technique which prompts the end user for a method of live interaction with systems to ensure the user can authenticate. The method we have adopted is keycode authentication which is requested after a user enters their credentials. This process has been implemented for all staff when access College systems internally and externally. MFA is also implemented for students accessing College systems externally. MFA reduces the effectiveness of phishing attacks (stealing user credentials).

b) Data Loss Prevention (DLP)

DLP uses intelligent systems to try and prevent data being sent or saved, either maliciously or accidentally, to a third party who should not be receiving the data. DLP is implemented with a set of security rules that will scan data and action alerts and blocks. The rules are fully customisable, flexible and offer good resistance against breaches.

c) Micro-Segmentation

Micro-segmentation is a network security technique that enables us to logically divide the data into distinct security segments down to the individual workload level, and then define security controls and deliver services for each unique segment. This provides flexible control and improves data security by reducing the attack surface.

d) Back Up Strategy

The backup strategy includes three copies of our data on two different media (disk and tape) with one copy off-site for disaster recovery. This strategy is designed and developed in line with the College Information Security Policy and ICT Business Continuity Plan.

e) Security Information and Event Management (SIEM)

SIEM is a subsection within the field of computer security, where software products and services combine security information management and security event management. They provide real-time analysis of security alerts generated by applications and network hardware.

f) Updates and Patches

Regular updates and patches are applied to browsers, operating systems, and other applications to limit the attack surface and plug application vulnerabilities. Software providers regularly release patches to fix identified vulnerabilities. Updates are applied as soon as they are released.

g) Anti Virus/Firewalls

The firewall inhibits malicious software from entering the College network while antivirus removes corrupt files and software from college computers and network.

h) Insurance Policy

Cyber security investment often follows some form of breach or incident therefore the College have taken a proactive approach in adjusting the current cyber security insurance policy to extend and include cyber extortion threat, reward payments and cyberterrorism. This was to cover cyber-attacks specifically to respond to the increasing attacks experienced in the sector.

8. Security Controls (practical measures)

a) Device Security

To ensure the security of all College issued devices and information, employees are required to:

- Keep all College issued devices, including tablets, computers, and mobile devices, password protected.
- Ensure devices are secured and locked when not in use.
- Refrain from sharing private passwords with co-workers, personal acquaintances, senior personnel, and/or shareholders.
- Ensure devices are regularly update with the latest security software.

College employees are obligated under the equipment loans agreement and acceptable use policy as part of the equipment loan procedure.

b) Email Security

Protecting email systems is a high priority. Criminals send emails containing malicious links which have led to data theft, scams, and carry malicious software like worms and bugs. Therefore, the College requires all employees to:

- Verify the legitimacy of each email, including the email address and sender name.
- Avoid opening suspicious emails, attachments, and clicking on links.
- Look for any significant grammatical errors.
- Avoid clickbait titles and links.
- Contact the ICT department regarding any suspicious emails.

c) Transferring Data.

The College recognises the security risks of transferring confidential data internally and/or externally. To minimise the chances of data theft, we instruct all employees to:

- Refrain from transferring classified information to employees and outside parties.
- Only transfer confidential data over college networks.
- Obtain the necessary authorisation from senior management.
- Verify the recipient of the information and ensure they have the appropriate security measures in place.
- Adhere to the College data protection and privacy policies.
- Immediately alert the ICT department of any breaches, malicious software, and/or scams.

d) Working remotely

The College provide remote working employees with equipment that is essential to their job duties. Equipment can be issued via the College equipment loans procedure or via the equipment entitlement procedure. Employees will access the College systems via a virtual desktop to ensure security controls are maintained. The College will, where required, install a virtual private network (VPN) connection.

Equipment is College property. Users must adhere to the College equipment agreement an acceptable use policy. Users are required to keep equipment safe and avoid any misuse. Specifically, they must:

- Keep their equipment password protected.
- Store equipment in a safe and clean space when not in use.
- Follow all data encryption, protection standards and settings.
- Refrain from downloading suspicious, unauthorised, or illegal software.
- Ensure applications and devices are logged out when not in use.
- Ensure college data and information cannot accessed by unauthorised users.

Staff and students can access the College network using their own device. Where a user connects to the College network, using their own device (referred to a “Bring your Own device” (BYOD)), this device may need to be tested by the college to ensure compliance with this policy. When connecting a BYOD device to the College network, the system will check details such as make, model, windows version, etc before the device is approved to connect. No personal data is collected during this process.

e) Creating strong passwords

College network passwords contain a minimum of 8 characters, and they expire after 180 days. All network users should create complex passwords, a combination of at least eight upper- and lowercase letters, numbers, and special characters. Employees are encouraged not to sequentially change their password on expiry. The whole password should be changed on expiration.

f) Cyber Security Awareness

The College employ security practices that effectively safeguard colleagues, students and customers, our IT infrastructure, and the College reputation. Staff are required to engage in cyber security awareness training exercises and ensure students are introduced to the College online safety hub which can be accessed via: https://intra.newdur.ac.uk/studentIntra/s_ict_online_safety.html

9. Security Monitoring

Assurance of the effectiveness of security mitigation is achieved through several activities. These activities also inform security monitoring processes in terms of information and event monitoring. Assurance activities carried out are as follows:

a) Phishing Vulnerability Assessment

The College engaged with an external ISO27001 registered suppliers to carry out phishing campaigns to identify risk to phishing attacks. The assessment highlights strengths and weaknesses and provided recommendations for ongoing prevention and protection.

b) External Security Assessment

The College engage with external security suppliers to carry out vulnerability assessments. The key objectives of a security assessment are to assess IP address ranges and web applications to identify vulnerabilities based upon ease of exploitation, level of effort to remedy, and severity.

c) Cyber Essentials Plus

The College are currently certified for Cyber Essentials Plus. This is a government-backed scheme that helps organisations protect themselves against the growing threat of cyber-attacks. The certification provides a clear statement of the basic controls the College has in place. Cyber Essentials Plus is the highest level of

certification offered under the Cyber Essentials scheme. It is a rigorous test of the College cyber security systems where vulnerability tests are carried out to make sure that the College is protected against basic hacking and phishing attacks.

d) Internal Audit

The internal audit plan includes audits relating to web browsers and filtering, and remote working and ransomware. Both audits include investigations and monitoring of information and network security.

e) External/Internal Monitoring

The implementation of additional security risk mitigation tools has provided facilities to allow the College to monitor internet traffic and activities across our network. Monitoring rules have been set to alert when unusual activity is detected such as impossible travel, which tracks a users' sign in time and location and alerts if it is impossible to achieve.

The College continue to monitor the cyber environment for threats and vulnerabilities and will take protective action to implement preventative measures to mitigate security risks.

10. Evaluation and Review

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

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.