INFORMATION SECURITY POLICY

This policy is available on-line at: www.tynecoast.ac.uk

- We will consider any request for this policy to be made available in an alternative format or language. Please contact: Executive Director of Digital and Projects
- We review our policies regularly to update them and to ensure that they are accessible and fair to all. We welcome suggestions for improving the accessibility or fairness of this policy.

Approved by:	Version:	Issue Date:	Review Date:	Contact Person:
Exec Group, Audit	v.8	February 2026	February 2029	Executive Director of Digital and Projects

Equal Opportunities: **Impact Assessed**

Review:

POLICY NUMBER 17

Information Security Policy

1. Policy Statement

Data plays an essential part in both the teaching and administrative services of Tyne Coast College. Ensuring the security of this data and the systems on which it is hosted is necessary to fulfill our obligations to the providers of this data and to protect the data and systems from accidental or deliberate damage, loss or corruption.

2. Scope

For the purposes of this policy, the term data refers to all information—whether stored electronically or on paper—regardless of location, platform, or storage method. This includes data held in cloud or Software-as-a-Service (SaaS) environments, on-premises systems, endpoints, mobile or IoT devices, AI-powered tools and assistants, and any third-party platforms or services.

Any data stored on, processed by, or transmitted through College-owned systems, cloud services procured by the College, or third-party processors acting on behalf of the College (including Managed Service Providers), as well as any data created by College staff or students in the course of their duties or studies, is considered College-owned and is therefore subject to this policy.

Every individual handling data or using College systems—whether a member of staff, student, contractor, or third-party partner—must be accountable for their actions and exercise due care to ensure the security and integrity of all data at all times.

3. Legislation

Access and use of data must be made in compliance with all appropriate legislation, which includes but is not limited to:

- UK General Data Protection Regulation
- Data Protection Act 2018 (as amended)
- Data (Use and Access) Act 2025
- Privacy and Electronic Communications Regulations 2003
- The Computer Misuse Act 1990
- Copyright Designs and Patents Act 1988
- Malicious Communications Act 1988
- Criminal Justice and Public Order Act 1994

4. Responsibilities

4.1. The Executive Director of Digital and Projects is responsible for information security management, including ensuring all staff are aware of the policy,

have received appropriate training and that suitable systems and process are in place.

4.2. All staff have a responsibility to give full and active support to the policy

4.3. All staff are expected to observe the Information Security Policy and associated procedures, both on College premises and outside the College.

4.4. Each significant category of data is the responsibility of a designated officer of the College. This person is responsible for the security of that data and determines the standards of confidentiality and requirements for access that apply. Unless specified otherwise this will be assumed to be the relevant Head of Department whose department operates the system in question.

4.5. The data owner for each system, or their nominated representative, determines who should have access to the data on that system.

4.6. The security and operation of central IT systems is the responsibility of the IT Services department. It is IT Services responsibility to ensure that all data systems meet the access requirements defined by the appropriate data owner.

4.7. It is the responsibility of any person signing a contract, or otherwise granting access to data, by a 3rd party to ensure that the 3rd party has adequate data safe guards in place. Data security safe guards providing equivalent protection to those outlined in this document are considered the minimum acceptable standard.

5. Classification of Data

For the purposes of this policy four top-level classifications of data exist

5.1. Public

Data which is already in the public domain, or is intended for circulation to learners, for example, press releases, website content, course notes etc…

5.2. Internal

Data which is widely available to College employees and does not contain identifiable personal data, for example, internal staff briefings, team meeting minutes..

5.3. Confidential

Any information relating to an identifiable person (i.e. name & address, person code, passport number etc…)

Data which may reasonably be expected to be considered personally confidential, or commercially confidential. For example, data or materials pertaining to existing or planned courses which may be of interest to a competing organization.

5.4. Highly Confidential Data

Data that if lost or stolen would be likely to cause damage or distress to one or more individuals.

Data, which if used inappropriately may have a significant impact upon the College or an individual. In particular, employee or learner bank account details or any other data which it is believed could be used for illegal purposes.

Any data identified by UK legislation as sensitive data (e.g. racial or ethnic origin, political opinions, religious beliefs, etc…)

6. Actions to Implement and Develop Policy

6.1. Data Confidentiality

All personal data is maintained for the purpose defined within the Data Register. The designated Data Protection Officer is responsible for maintaining the Data Register, dealing with subject access requests, maintaining awareness of data protection legislation and offering advice on compliance.

6.2. Data Privacy Impact Assessments

Data Privacy Impact Assessments (DPIA) are required where processing is likely to result in a high risk to the rights and freedoms of individuals.

6.3. Data Access & Disposal

Access to data is restricted to those who need such access to carry out the duties for which they are employed. Each member of staff who has been granted access is personally responsible for ensuring compliance with this policy, the relevant legislation and the confidentially of the data to which they have been granted access.

When no longer required data must be securely disposed of – shredded for paper records, or securely erased for electronic records. IT services are responsible for the correct disposal of data which is stored on centrally operated servers.

Data retention periods are documented in the Archive Policy and data register.

6.4. Physical Security

All reasonable measures must be taken to prevent physical access by unauthorized persons to College data.

Computer workstations which are used to access sensitive data should be logged off or locked when not in use. Electronic devices such as laptops or tablet PC's, and computer media that contain sensitive data should not be left unattended when offsite.

Paper copies of data should be stored securely when not in use, examples include, in a locked office, in a locked filling cabinet. Where paper copies of sensitive data are required to be taken offsite they should not be left unattended.

Paper copies of sensitive data should be destroyed when no longer required; this should be achieved by shredding or incineration.

6.5. IT Systems

6.5.1. Access Controls

Electronic access to data is controlled by means of a user's network username and password. Control of network accounts is the responsibility of IT Services. IT services must be notified when staff leave and will be responsible for removing their network accounts. Any files left by that staff member on the College servers will be archived for future retrieval.

Requests for network accounts will only be actioned on production of suitable documentation.

- Suitable documentation for staff is considered to be an appropriate communication from HR.
- Suitable student documentation is considered to be a current student ID card verified by EBS Agent, or written notification from MIS.

6.5.2. Multi-Factor Authentication (MFA)

Passwords alone are no longer considered adequate protection. MFA is required for all remote access to college systems.

6.5.3. Backups

Backups of central servers will be carried out in line with the IT Services Backup Procedures.

6.5.4. Privacy

The privacy of users' files will be respected, but the College reserves the right to examine systems, folders, files and their contents, to ensure compliance with the law and with College policies and regulations.

6.5.5. Software Assets

To ensure that the use of all software and licensed products within the College complies with the relevant acts for the protection of software, the College will carry out checks from time to time to ensure that only authorised products are being used. Unauthorised copying of software or use of unauthorised products by staff or students are grounds for disciplinary and where appropriate legal proceedings.

6.6. Electronic Storage Systems

Potential data storage locations include, but are not limited to:

- Cloud services (as designated & managed by IT Services)
- central servers
- personal computers
- portable electronic devices, including:
    - laptops
    - Tablet PCs/iPads
    - Mobile phones
- removable media, including:
    - flash memory devices (USB sticks, SD cards, Compact Flash cards, etc…)
    - removable hard disks (inc external USB drives)

Data stored on central and departmental servers is the responsibility of IT Services. They will be responsible, on behalf of the relevant data owner, for the security of the data on these systems.

Data should not be stored on the internal hard disks of college workstations without the permission of IT Services.

Full disk encryption must be enabled on laptops that are assigned to staff for use off campus.

6.7. Portable Storage Devices

Data stored on portable electronic devices must be suitably encrypted. Where staff have been issued with a portable storage device by the College they must make use of this device in preference to any personally owned devices.

No data belonging to the College should be stored on privately owned portable data storage devices.

It is the responsibility of the person saving or copying data onto an authorized portable storage device to ensure that adequate backups of the data exist to guard against loss of the portable storage device.

Extremely sensitive data should not be copied onto portable storage devices without first consulting the Director of IT, or their nominated deputy, in regard to appropriate encryption and protection measures.

6.8. Electronic Communications Systems

6.8.1. Internal Systems

Responsibility for the security of data transmitted on the College LAN (both wired and wireless) and inter-site WAN connections is the responsibility of the IT Systems Manager on behalf of the Director of IT.

6.8.2. External Systems (including internet and e-mail)

Data transmitted over the public internet, or other external networks, is particularly vulnerable to loss or theft. Therefore it is the responsibility of the individual undertaking the transmission to ensure that personal data is appropriately encrypted, and only transmitted via approved transfer methods.

6.9. Remote Access

Responsibility for ensuring that this and other relevant polices are complied with when accessing College systems remotely lies with the individual undertaking the access.

6.10. Contingency

The IT Services backup policy defines requirements for backup and restoration for all central servers.

6.10 Encryption

Only IT Services staff are permitted to encrypt files or other data that is stored on central or departmental servers.

The encryption keys or passwords to any data which is owed by the college, as defined by section 2 of this policy, must be surrendered upon receipt of a written instruction from a senior manager of the college. Failure to comply with this instruction may result in disciplinary action.

7. Compliance

Failure to comply with the guidance provided in this policy may result in disciplinary action being taken against the individuals involved under the College's disciplinary procedure. In certain cases this may amount to gross misconduct which will lead to summary dismissal.

In the case of contracted 3rd parties who are required to process College data, termination of contract and legal action may result from a failure to ensure that sufficient data security safe guards are in place. Data security safe guards providing

equivalent protection to those outlined in this document are considered the minimum accepted standard.

8. Monitoring & Evaluation

Any identified breaches of the policy will be dealt with in accordance with the "Information Security Incident Response Procedure". Both the Data Security Policy and Information Security Incident Response Procedure will be reviewed and evaluated following the closure of any serious incidents that may occur.

9. Related Policies

- Acceptable Use of Information and Communication Technology
- Information Security Incident Response Procedure
- Harassment Policy
- Data Protection Policy
- Joint Academic Network (JANET) Acceptable Use Policy available from: http://www.ja.net/documents/policy_documents.html

Equality, Diversity Inclusion and Belonging

We as a college community are focused on ensuring that those minority groups within society who are more likely to experience discrimination and are protected by the Equality Act 2010 do not experience unfair discrimination, harassment or victimisation while working at, studying at or visiting Tyne Coast College.

The Information Security Policy has been written and complies with the following **Protected Characteristics** (please tick all that apply):

Age	X
Disability	X
Gender reassignment	X
Marriage or Civil Partnership (in employment only)	X
Pregnancy and Maternity	X
Race	X
Religion or Belief	X
Sex	X
Sexual Orientation	X

Full description of **Protected Characteristics** can be found in the Equality, Diversity, Inclusion and Belonging Policy

Name of Person responsible for Policy	Craig Scott
Signed	
Date Reviewed	21/01/26