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: Business Operations Manager
- 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.
- All our policies are subject to equality impact assessments*. We are always keen to hear from anyone who wishes to contribute to these impact assessments. Please contact: Business Operations Manager

*Equality Impact Assessments are carried out to see whether the policy has, or is likely to have, a negative impact on grounds of: age, disability, gender reassignment, pregnancy and maternity, race, religion or belief, sex or sexual orientation

Approved by:	Version:	Issue Date:	Review Date:	Contact Person:
CMT, Audit	**v.6.1**	**May 2020**	**May 2023**	**Business Operations Manager**

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 encompasses all data, stored electronically, or on paper.

Any data stored on College owned equipment, or produced by persons in the employ of the College as part of their duties is considered to be owned by the College and therefore subject to this policy.

Every person handling data or using College systems, whether a member of staff or a student, should be accountable for their actions and have a duty of care to ensure due diligence is afforded to data security.

3. Legislation

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

- General Data Protection Regulation
- Data Protection Act 1998
- 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 Business Operations Manager 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 School or Head of Service 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 three 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 indentifable personal data, for example, internal staff briefings, team meeting minutes..

5.3. Confidental

Any information relating to an indentifiable 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 Confidental 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 the Data Protection Act (1988) as personal sensitive data, specifically data relating to racial or ethnic origin, political opinions, religious beliefs, membership of trade union organisations, physical or mental health, sexual life, offences or alleged offences.

6. Actions to Implement and Develop Policy

6.1. Data Confidentiality

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

6.2. 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.

6.3. 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 (floppy disks, USB devices, CD-ROM's etc…) 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.

6.4. IT Systems

6.4.1. 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.

6.4.2. Backups

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

6.4.3. 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.

6.4.4. 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.

6.5. Electronic Storage Systems

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

- central servers
- departmental servers (i.e. outreach centers)
- personal computers
- portable electronic devices, including:
    - laptops
    - Tablet PCs/iPads
    - Mobile phones
    - MP3 players
- removable media, including:
    - floppy/ZIP disks
    - optical media (CD/DVD)
    - 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.

6.6. 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 Business Operations Manager, or their nominated deputy, in regard to appropriate encryption and protection measures.

6.7. Electronic Communications Systems

6.7.1. 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 Systems Manager IT on behalf of the Business Operations Manager.

6.7.2. 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:

- Sensitive data is appropriately encrypted, or trasnmistted vai approved file transfer systems
- Extremely sensitive data is not transmitted without first consulting the Business Operations Manager, or their nominated deputy, in regard to appropriate encryption and protection measures.

6.8. 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.

6.9. 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 encrypted 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 surrended 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