Information Security Policy

Document Title: Information Security Policy			
Version No.	2.3	Policy Owner	ITACS
Superseded version	2.2	Author Role Title	Director of ITACS
Approval Date	22.5.17 – last updated September 2018	Approved by	VC
Effective Date	22.5.17	Review Date	September 2019

Information Security Policy

1. Purpose

The purpose of this Policy is to implement the necessary organisational measures to ensure as far as possible that the University's Information and Information Systems are secure.

A secondary aim of the policy is to raise awareness of Information Security issues to enable those using the University's Information Systems to promptly identify and act in the case of an Information Security breach.

This Policy informs the University's staff, students, and other individuals entitled to use University Information and University Information Systems, of the principles governing the collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of information.

It is the University's aim to ensure that:

- Information will be protected against unauthorised access or misuse;
- Confidentiality of information will be secured;
- Integrity of information will be maintained;
- Availability of information / Information Systems is maintained for service delivery;
- Business continuity planning processes will be maintained;
- Regulatory, contractual and legal requirements will be complied with;
- When information is no longer of use, it is disposed of in a suitable manner;
- All information security incidents and concerns including loss, theft or unauthorised access to information or Information Systems are promptly reported and investigated through the appropriate management channel.

Information for the purpose of this policy includes any information stored on:

- Electronic Information Systems (software, computers, and peripherals) whether deployed or accessed on or off campus;
- The University's computer network used either directly or indirectly;
- Hardware, software and data;
- Electronic recording devices (video, audio, CCTV systems); and
- Hard copy documents.

2. The Policy

The Information Security Policy will be reviewed annually to determine whether it still meets existing needs, and will be updated in accordance with changing demands. The UK Government's Cyberessentials scheme is used as a guide to determining policy in relation to the University's Information Systems.

2.1 Authorised users of Information Systems

All users of University Information Systems must be either formally authorised as a member of staff, or by enrolment as a student, or by such other process specifically authorised by the Vice Chancellor. Authorised users will be in possession of a unique personal user identity and password which must be used at all times when using the University's IT systems. The password associated with this identity must not be disclosed to any other person.

Authorised users must take care to protect University information. Confidential or Restricted information (as defined in the information classification scheme at appendix A) must not be downloaded to a non-University account, shared or otherwise processed without consideration of:

- Permission of the information owner
- The risks associated with loss of data falling into the wrong hands
- How the information will be secured during transport and at its destination.

2.2 Acceptable use of Information Systems

Use of the University's Information Systems by authorised users will be lawful, honest and decent and shall have regard to the rights and sensitivities of other people. The detail of acceptable use in specific areas may be found in the following list of subsidiary policies:

1. IT Acceptable Use Policy (http://url.tees.ac.uk/aup).
2. IT Hardware Asset Management Policy (http://url.tees.ac.uk/ham).
3. IT Software Asset Management Policy (http://url.tees.ac.uk/sam).
4. IT Remote Working Policy (http://url.tees.ac.uk/rwp).
5. Business Computing Standard (http://url.tees.ac.uk/bcs)

Any misuse of an information system, breach of Information Security, concern, loss or misappropriation of University data bearing assets must be reported either to a relevant system owner or to the Information Technology and Communications Services Department (IT Department).

Any incident relating to a potential loss of personal information must be reported to the Information Compliance Team in Legal & Governance Services without delay using the Personal Data Incident Form available here or by calling ext. 2563.

2.3 Information System Owners

Whereas the IT Department plays an important role in ensuring that information systems remain operational (availability), it does not typically 'own' those systems. Choices about who has access, how the system is used in a business sense and the accuracy of the information contained in the system lie with the system owner. Thus for any given Information System there are activities that lie with the IT Department as well as the System's Owner.

In support of System Owners, the IT Department will ensure that centrally supported systems:

1. Are adequately protected from unauthorised access (hacking etc.).
2. Are physically secured against theft and damage.
3. Are built upon the principle of resilience reducing, wherever possible, single points of failure in their architecture.
4. Are recoverable should there be a failure of supporting infrastructure (Disaster Recovery). Recovery Point Objectives (RPOs) i.e. How often Information Systems are backed up and Recovery Time Objectives (RTOs) i.e. The time taken to restore a system, will be agreed between the system owner and the IT Department.
5. Are incorporated into external and internal network penetration testing schedules.
6. Are subject to secure disposal when data bearing elements are no longer required.
7. Electronic Access logs are only retained for a justifiable period to ensure compliance with the Data Protection, Investigatory Powers and Freedom of Information Acts.

Deans/Directors who are responsible for Information Systems 'Owners' are required to ensure that:

8. Procedures are in place to securely grant and revoke user access to systems.
9. Consideration is given to any necessary separation of duties within system roles. i.e. requestors are not also authorisers etc.
10. Data is maintained with a high degree of accuracy and security.
11. Compliance with contractual requirements is maintained (e.g. PDI-DSS).
12. A process exists to validate notifications from suppliers of feature and/or security updates that may need to be applied to Information Systems.
13. Adequate steps are taken to maintain Business Continuity should a supporting Information System become unavailable (See 4 above).
14. Any third parties entrusted with University data understand their responsibilities with respect to maintaining IT security and disposing of that data in a timely and secure manner.
15. Any suppliers given remote maintenance access to systems understand their responsibilities with respect to maintaining IT security.
16. In respect of points 14 and 15 above, wherever Personal Data is involved (as defined in the General Data Protection Regulation "GDPR") the third party security obligations must be documented in a legally binding contract. The University shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of the GDPR and ensure the protection of the rights of the data subject.

17. Systems are used for their intended purpose and that procedures are in place to rectify discovered or notified misuse.
18. Data entering or leaving the system is classified correctly such that appropriate levels of security can be applied.
19. Wherever Schools/Departments are considering building or procuring new IT systems which will store or access personal data; or where there will be a significant change to the way personal data is processed in an existing IT system (such as information being moved to the cloud) the Data Protection Officer must be contacted at the beginning of the project to determine whether a Privacy Impact Assessment is required. No new processing activity may be started prior to this determination, and must refer to any relevant contract.

2.4 User Privacy

Authorised users of Information Systems are not given rights of privacy in relation to their use of University Information Systems. Duly authorised officers of the University may access or monitor personal data contained in any University Information System (mailboxes, web access logs, file-store etc), this access is governed by the University's Privacy & Monitoring policy.

2.5 Information Classification

Not all information is equal. It is important to have a means to classify information such that it can be adequately protected. For example, personal and private information requires higher levels of protection than public information.

The information classification scheme is simple and offers two primary levels of categorisation: Information is either unprotected (public) or protected. Protected information is either confidential or highly confidential.

The scheme exists to:

- Safeguard information from accidental or deliberate compromise, which may lead to damage and/or be a criminal offence;
- Meet legal, ethical and statutory obligations;
- Look after the interests of all those who have dealings with the University and about whom it may hold information (including staff, students, alumni, collaborators, business partners, supporters);
- Ensure information security procedures are matched to classification;

It is not possible to mandate use of the scheme in a prescriptive manner as ultimately the judgement on Information Classification is a human one. However, guidance on application is given in appendix A.1.

System Owners should consider how the classification system could be applied to defined datasets within Information Systems. In so doing, a protocol for data handling methods could be devised for users of such systems.

2.6 Payment Card Data

As an organisation that processes card payments, the University is obliged to comply with the PCI-DSS (Payment Card Industry Data Security Standard). This standard aims to protect card data in order to reduce the risk of financial fraud. Organisations that fail to meet the compliance requirement risk being audited, fined and ultimately losing their ability to process card payments.

All staff that process card payments on behalf of the University must comply with PCI-DSS requirements by following Finance and Commercial Development's (FCD) Card Handling Procedures. This document is available in the FCD section of Unity (https://unity3.tees.ac.uk/departments/025/21/default.aspx).

2.7. Ownership

The Director, IT and Communications Services (IT Department) has direct responsibility for maintaining this policy and providing guidance and advice on its implementation.

Information System owners are responsible for the implementation of this Policy within their area, and are required to ensure adherence.

2.8. Breach

Individuals in breach of this policy are subject to disciplinary procedures (staff or student) at the instigation of the Dean/Director (or above) with responsibility for the relevant Information System, which may result in disciplinary action being taken or criminal prosecution.

The University will use all available means to safeguard its Information Systems and to protect the University from any adverse impact on its operations, infrastructure or reputation.

Appendix A: Information Classification Scheme

A.1 Information Classification Scheme

The information classification scheme is in two parts. The first is guidance on classification and the second on data handling relating to classification. The high-level concept behind classification is described below.

INFORMATION		
Unprotected	**Protected**	
Public	Confidential	Highly Confidential

- Disclosure of information which would be highly damaging to the University either to its reputation or financially warrants a **Highly Confidential** classification.

- Disclosure of information which would be damaging or a have a negative impact on the University would be classified as **Confidential**.

- There are no special security considerations for unprotected information.

A.1.1 Classification serves the sole purpose of indicating the protections that must be applied to an information dataset. E.g. we can mandate that information deemed highly confidential is not sent in plain cover through the internal post.

The following may help in classifying Information:

a) Personal Information will generally fall into the Protected Category. Things such as internal telephone numbers, post titles and names are not personal information for the purpose of this scheme and would not be regarded as protected information.

   Personal information that would be classed as protected information would be such things as Home address, Personal phone numbers etc and warrant a confidential classification. Bank account details, Credit Card numbers, Passwords or Medical records would most safely be classified as Highly Confidential. A dataset that contains a mix of classifications must always be handled according to the most sensitive.

b) There is also a consideration of volume. Disclosing a single individual's personal information (say home address) by accident or breach of security (hacking) may call into question the University's reputation as a safe pair of hands. However, losing a memory stick containing the home address of all staff would be far more serious. Thus you may wish to consider the

classification of data based on volume. This is an important consideration when transmitting information, particularly outside the University.

c) The value of intellectual property may also be a factor in classification for research data both in situ and in transit.

d) Information Classification may vary over time. I.e. Timed press releases or other embargoed information may begin with a relevant protected classification but change to unprotected on release. Where classification may vary, it is best to treat it with the most sensitive classification from the outset.

A.1.2 Information Handling.

These general guidelines apply to the handling of protected information:

a. Storage: Information should always be stored on University provided facilities. If that storage is electronic then a location requiring authentication (not open access) must be used. E.g. U or S drives, SharePoint meeting or collaboration sites. University information should not be stored on unmanaged third party systems (Dropbox) or home computers. Memory sticks should only be used if encrypted. The University operates a clean desk policy and paper documents should not be left on desks.

   Additional requirements for Highly Confidential Information:

   - The use of memory sticks or other removable media (encrypted or otherwise) should be considered as a last resort only. The goal should be to keep such information safe within the organisation wherever possible.
   - Only portable computing devices (laptops etc) featuring 'whole device' encryption are to be used.

b. Dissemination & Access: Information can be shared via SharePoint (Unity) to specific groups using authentication (group membership – meeting sites etc). Generally, such circulation (including paper) should be on a need-to-know basis. Information can be accessed remotely using University managed devices. Paper documents may be circulated using the internal post system.

   Additional requirements for Highly Confidential Information:

   - The Information owner should conduct regular reviews of access to the information.
   - All remote access must be via encrypted channels.
   - Paper documents must be delivered by hand internally, marked confidential.

c. Exchange & Collaboration: Information can be emailed without encryption. Paper documents should be dispatched under plain cover.

Recipients must clearly understand the sensitivity of the information they will receive and the University's expectation upon them to care and dispose of it.

Additional requirements for Highly Confidential Information:

- Information should be encrypted prior to exchange.
- The exchange must utilise University provided facilities.
- Both the nature and the volume of the information should be considered prior to selecting a method of exchange.

d. Disposal: Deletion of information on any University provided equipment is necessary. Paper documents should be disposed of in confidential waste bins. Please ensure that any University device that is no longer required is disposed of in line with the Finance Asset Management procedures.

   Where home IT equipment has been used for University purposes, it should be disposed of as above, by special arrangement with the IT Department's Information Assurance Team.