Information Security Policy

Document Title: Information Security Policy			
Version No.	3.0	Policy Owner	University Secretary and Head of Legal & Governance Services.
Superseded version	2.3	Author Role Title	Head of Information Governance, LGS
Approval Date	18.05.2021	Approved by	UET
Effective Date	**18.05.2021**	Review Date	June 2022

1. Introduction

Information is a vital asset which the University needs to function. In an increasingly interconnected environment where information is exposed to a wide variety threats, it is crucial to implement safeguards to ensure the security, availability, confidentiality and integrity of the University's information and information systems and to ensure the University's uses appropriate technical and organisational measures to enable compliance with data protection legislation and other information standards.

2. Purpose of Policy/Document

This Policy defines the principles governing the collection, use and disposal of information. Its purpose is to:

- protect University information and systems from unauthorised access, theft, loss, damage or misuse;
- provide assurance that information is managed securely and in a consistent way across the institution;
- ensure the availability and integrity of information and systems for service delivery;
- support effective business continuity and planning;
- ensure compliance with legal, regulatory and contractual requirements; and
- support the University to meet its strategic aims.

3. Scope

This Policy applies to all users of University information and information systems, including staff, students, authorised third parties and the University's subsidiary companies. It covers information of all types, including personal and none-personal data, in all formats whether electronic or hard copy and any hardware or software used to process it, including the University computer network.

4. Policy Statement

4.1 Access Permissions

Access to information and information systems shall be restricted to users who have an authorised business need as determined by the relevant IAO, Line Manager or upon completion of enrolment in the case of students. There will be procedures in place to periodically review and

revoke access permissions, in particular, to ensure the withdrawal of permissions where user roles change and on termination of employment or study.

4.2 Assets, Classification & Handling

All information will be organised into groups known as Information Assets which will be classified, documented in an Information Asset Register and handled as described in the Information Classification Policy and Information Handling Guidelines. The application of security controls will be based on classification level, ensuring that those assets posing greatest risk are handled with greater security.

4.3 Business Continuity

Information systems and their contents will be recoverable in the event of failings of supporting infrastructure in accordance with the University's Disaster Recovery plans.

4.4 Disposal

Information and information systems will be subject to secure disposal as per the timeframes defined within the Record Retention Schedule and in a manner that takes into account the damage that may be caused by loss, theft or unauthorised access to the information. Only ITDS are permitted to dispose of IT Hardware.

4.5 Documented Operating Procedures

Will be maintained for all information systems to ensure proper use for their intended purpose and consideration will be given to any necessary separation of duties within system roles. i.e. requestors are not also authorisers etc.

4.6 Hardware Management

All IT hardware will be registered and asset marked by ITDS and managed in line with the IT Hardware Asset Management Policy.

4.7 Incident Management

Any event or action which may compromise the confidentiality, integrity or availability of systems or data, either accidentally or deliberately, and has caused or has the potential to cause damage to the University's information assets and/or reputation will be reported in line with the University's Data Breach Management Policy.

4.8 Monitoring System Access & Use

The University reserves the right to monitor activity where it suspects there has been a breach of Policy, to ensure compliance with legislative requirements, to prevent or detect crime or support the apprehension of

offenders. Such monitoring will be undertaken by authorised persons in line with the IT Privacy and Monitoring Policy.

4.9 Network Security

Intrusion prevention and detection systems and a programme of penetration testing will be deployed by ITDS to protect information and systems from unauthorised access and to ensure timely identification and response to network threats and vulnerabilities.

4.10 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 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).

4.11 Physical Controls

Information and information systems will be physically secured from unauthorised access, theft and damage. Access will be restricted to any area which processes personal data and Managers will provide information on the potential security risks and the measures used to control them to staff with authorisation to enter such areas.

4.12 Portable and Removable Devices

Such as USB's and external hard drives should be used only where necessary and may not be used for permanent storage of information. If used, the information they hold must be protected in accordance with the Information Handling Guidelines.

4.13 Software

All software must be deployed in line with the requirements of the IT Software Asset Management Policy, by or with the authorization of ITDS. Procedures will be implemented to ensure the timely validation and deployment of feature and security updates.

4.14 Storage & Transmission

Information may only be stored or transmitted via facilities that are provided by and/or managed by ITDS and which ensure sufficient protection of the information. This protection will be determined by the

classification of the information as per the Information Classification Policy and Information Handling Guidelines.

4.15 System Acquisition and Development

Information security requirements will be defined within the business requirements for all new information systems or changes to existing systems. System developments will be controlled with the use of formal change control procedures implemented by ITDS to reduce the risk of accidental or deliberate development of vulnerabilities. The acquisition and/or development of systems should be carried out with the involvement of the IG Team at the earliest possible stage to ensure privacy by design and the proper management of associated risks.

4.16 System Logging

Event, error and operational audit logs will be properly reviewed and managed by qualified staff. System clocks must be regularly synchronised between the University's various processing platforms.

4.17 System Testing

Prior to acceptance, all new or upgraded systems or hardware will be tested to ensure compliance with this Policy.

4.18 Third Party Access

Third parties may be provided with access to relevant information and systems where there is a valid business need. This must be sponsored by the Information Asset Owner who will be responsible for ongoing monitoring of access requirements.

Third party access protocols will be documented and maintained and will include a requirement to ensure third party users understand their obligation to comply with this Policy.

Where a third party will be processing Personal Data on behalf of the University, the University will:

- document roles and responsibilities in a legally binding contract; and
- choose a Processor providing sufficient guarantees to implement appropriate technical and organisational measures to ensure the protection of University Personal Data.

4.19 Training & Awareness

Mandatory Information Security training will be undertaken by all staff every 2 years. An ongoing programme of awareness will be delivered by the IG Team, taking into account current risks and concerns highlighted by staff, or in the management of breaches.

4.20 Web Servers

Web servers will be deployed and administered by suitably qualified and authorised individuals and will be monitored to maintain high levels of security and to control the publication of University information, including personal data.

5. Roles & Responsibilities

Everyone with access to University information and systems has some responsibility for information security.

5.1 The **Board of Governors** is ultimately responsible for ensuring that the University meets its legal obligations in relation to Information Security;

5.2 The **Audit Committee** is responsible for routinely monitoring information security risks;

5.3 Overall responsibility for this Policy lies with the **University's Senior Information Risk Owner (SIRO)** who will be a member of the University Executive Team;

5.4 The **Head of Information Governance and Data Protection Officer (DPO)** and the **Information Governance Team** is responsible for operational management of information security risks, the development and maintenance of this policy and the provision of advice to ensure compliance with Legislative and Regulatory requirements;

5.5 The **Director of ITDS and the Information Assurance Team** are responsible for ensuring that effective IT security systems, controls and training programs are operationally implemented commensurate to risk, fit for purpose and available across the University and for implementing the technical controls detailed within this Policy;

5.6 The **Information Governance Project Board** is responsible for approving this policy and the **Information Governance Project Team** is responsible for raising awareness of this and associated Policies;

5.7 **Deans & Directors** have responsibility for ensuring compliance with this Policy within their business areas. Choices about who has access, how the system is used and the accuracy of the information therein lie with the Information Asset Owner;

5.8 **Information Asset Administrators** are accountable to their Deans & Directors and will have day to day responsibility for monitoring compliance with this Policy within their business area;

5.9 **All staff, students and authorised third parties** are responsible for information security and therefore must understand and comply with this Policy and associated guidance.

6. Policy Enforcement

Failure to comply with this Policy may result in action being taken under staff or student disciplinary proceedings.

7. Related Documents

This Policy is a key component of the University's overarching Information Governance Framework. It should be read alongside the following documents:

- Data Protection Policy & Procedure
- Information Classification Policy
- Information Handling Guidelines
- IT Acceptable Use Policy
- Remote Working Policy

8. Exceptions

Exceptions to this policy should be directed by a Manager to the Information Governance Team for risk assessment. The request and decision will be centrally documented.