Edge Hill University

Document Title	Information Security Policy
Document Owner	IT Services
Approved By	Information Strategy Group
Date Approved	June 2020
Date of Review	June 2021

Information Security Policy

1. Scope and Purpose

a. Information Security is the practice of ensuring that information is captured, stored, read, heard, modified, accessed and otherwise used and processed by only those who have the right to do so.

b. Information Security is often seen as a purely technical matter that requires specialist IT equipment and support. While there are many situations that do need this type of approach, the most effective first steps are based on user awareness, common sense and sound information governance practices. Assessing and understanding the risks for the University will help to establish the appropriate information management processes and procedures and, in turn, this should ensure appropriate incident management and recovery if security is compromised.

c. The range of potentially undesirable consequences associated with breaches of information security includes:

I. Information and/or systems being unavailable
II. Unauthorised access to data
III. Fraud
IV. Adverse publicity and/or reputational risk

d. Information security can be achieved through the following:

I. A pragmatic approach to policy and standards, resulting in an Information Security Policy which is supported by realistic and workable processes and procedures.
II. The rigour of security measures applicable to any information system, proportional to the assessed risk of the confidentiality, integrity or availability of its information becoming compromised.
III. A well-informed and well-trained workforce exercising an appropriate level of vigilance.

e. This Information Security Policy is applicable to, and will be communicated to University staff, students and all other relevant parties (ie anyone authorised to use or access University data, IT systems and infrastructure – including partners, contractors and other external agencies). The policy will be reviewed annually by the Information Strategy Group and will be tabled at the Risk Management Group and other relevant University groups and committees.

2. Information Security Policy

a. It is the policy of the University that information is governed, managed and secured appropriately in order to protect the University and its members from the consequences of potential breaches of confidentiality, failures of integrity or interruptions to the availability of that information.

b. This Information Security Policy provides the framework for information security across the University and shall be reviewed and updated to ensure it remains appropriate in the light of any relevant changes to the law, organisational policies or contractual obligations.

c. This Information Security Policy is applicable to, and will be communicated to University staff, students and other relevant parties. All users of University data, information and/or systems have a personal responsibility to manage and protect information under their possession.

d. The Information Strategy Group shall ensure that there is clear direction and visible management support for information security initiatives and, together with the Risk Management Group, shall ensure that appropriate business risks are assessed and monitored to identify the likelihood and impact of information related threats.

e. The responsibility for ensuring the protection of individual information systems, and that associated system-specific security processes are in place, shall reside with the Director, Dean or Head of Area and with the designated System Owner and Data Steward responsible for managing that information system.

3. Information Governance and Management Principles

a. The following principles form the basis for information governance and data management across the University as defined within the University's Record Management and Retention Policy:

Principle	Guidance
1.	The University, rather than any individual or business unit, owns all data
2.	Data should be defined consistently across all business areas of the University
3.	Every data source must have a designated Data Steward with overall responsibility for the accuracy, integrity and security of data. Additionally, the Data Steward will inform the Information Governance Office of significant change of purpose of any data source
4.	Wherever possible, data must be simple to enter, clearly defined and accurately document their subject, and be in a useful, useable format for both input and output
5.	Data should only be collected for a specific and documented purpose
6.	Data should be readily available to those with a legitimate business requirement
7.	Data should be recorded and managed over time in an auditable and traceable manner
8.	Data must be protected from unauthorised access and modification
9.	Retention periods identified in the Information Asset Register shall be adhered to
10.	Data purging and destruction shall be in line with University policies, without exception

4. Information Asset Registration and Classification

a. The Information Governance Office maintain the central University register of all Information Assets, and IT Services oversee the departmental entries of IT systems and processes as recorded in the IT Service Catalogue. Four information classifications have been proposed to support the capture, handling, retention and disposal of data assets, and these form the basis for the ongoing development of supplementary Information Classification guidance.

Confidential	Available only to specified and relevant individuals, with appropriate authorisation. A breach of confidentiality could result in unacceptable damage with very serious and lasting consequences to the University or one of its activities
Restricted	Available only to specified and/or relevant individuals, with appropriate authorisation. A breach of confidentiality could cause serious damage resulting in the compromise of activity within the University in the short to medium term. This includes both personnel data and research data
Internal	Available to any authenticated member of the University. Typically, if this level of information was leaked outside of the University, it could be deemed inappropriate or ill-timed
Public	Available to any member of the public without restriction. However, this information should not be placed into the public domain without reason

5. Business Continuity Planning

a. The University's Emergency Management Plan (EMP) is overseen by the Facilities Management Department, with contributions from all relevant areas of the University, and is reviewed annually. The EMP focuses on the University's response to an emergency and outlines how the University will liaise with internal and external agencies to coordinate actions in response to the requirements of the event. In addition, a specific Data Breach Policy exists with supporting procedures and guidance.

b. Specific departmental Business Continuity Plans (BCPs) are maintained and regularly reviewed by the individual departments and faculties where there is a greater understanding of, and responsibility for, managing the risks associated with their local operations, systems and business activities.

c. The University Risk Management Group monitors and maintains a Risk Register of business-critical risks, and this is reviewed regularly by the Governors Audit Committee.

d. The software source code for each corporate business information system (Student Records, Finance, Payroll and Human Resources) is held under Escrow with the National Computer Centre.

6. Compliance

a. The University will only store, process, retain and disclose personal information in accordance with the requirements of the General Data Protection Regulation (GDPR) 2018 and the University's Data Protection Registration.

b. The University has established policies and procedures to avoid breaches of any criminal and civil law, statutory, regulatory or contractual obligations and of relevant information governance, data and records management and information security requirements. These include:

- Data Protection Policy
- Data Quality Policy
- Data Breach Policy
- Privacy Policy
- GDPR Training Policy
- Records Management & Retention Policy
- IT Acceptable Use Policy
- Information Security Policy
- Password Policy
- Payment Acceptance Strategy & Policy

Each of these policies are supported by procedural documents, guidance and/or supplementary information. Any substantive changes to these policies will be communicated to all staff and other relevant parties.

c. All users of the University's information systems are informed of their responsibilities under the IT Acceptable Use Policy (AUP) and the Information Security Policy. Any suspected breach will be investigated and may be dealt with under the University's disciplinary procedures.

d. Further specific guidance is available to staff users of corporate information systems.

7. Outsourcing and Third-Party Access

a. External suppliers who are contracted to supply goods or services to the University should, where appropriate, be informed of the University's Information Security Policy and Data Protection Policy, and will be required to agree to adhere to the policy, and to protect its information assets.

b. Failure of a contractor, external agency or other third-party to comply with the Information Security Policy of the University may lead to immediate cancellation of the contract and, in certain circumstances, legal action may be pursued.

d. Any third party used for external disposal of the University's obsolete information-bearing equipment or hardcopy material must be able to demonstrate compliance with the University's Information Security Policy.

8. Human Resources

a. All members of the University must comply with the Information Security Policy of the University. Any information security incidents resulting from non-compliance may result in disciplinary action.

b. Staff with line management responsibilities must ensure that their supervised staff members are aware of, trained and comply with, information governance and information security best practice.

c. The University will provide information governance and security training, advice and guidance to all staff to ensure that their use is both efficient and does not compromise information security.

d. Network access privileges for staff will normally start on their first day of employment with the University (on completion, and approval, of the relevant Staff User Registration Form), and be terminated on their last day of employment. Access may be ceased / extended on application by a PVC / Dean / Director to the Deputy Vice-Chancellor, who will refer the matter to the Director of IT Services where appropriate.

9. Operations

a. Areas and offices where sensitive information is processed shall be given an appropriate level of physical security and access control to prevent unauthorised access, damage and interference.

b. Software errors, malfunctions and faults should be reported, logged and monitored via established procedures to ensure timely corrective action is taken.

c. To ensure the correct and secure operation of information processing facilities, changes to operational procedures are controlled and, where appropriate, have management approval.

d. Development and testing facilities for business-critical corporate information systems must be separated from 'live' operational instances, and the migration of software from development to operational status is subject to agreed change control procedures.

e. User acceptance criteria for corporate information systems upgrades and new versions are required, and suitable tests of the systems carried out, prior to migration to 'live' operational status.

10. Information Handling

a. The University encourages a clear desk and screen policy, and screens on which University information is processed or viewed should be sited in such a way that they cannot be viewed by unauthorised persons.

b. All users of University information systems must manage the creation, storage, amendment, copying and deletion or destruction of data in a manner which safeguards and protects the confidentiality, quality, integrity and availability of such data – as defined by the Records Management and Retention Policy.

c. The removal or transfer of information assets, other than those deemed to be 'Public', should be authorised by the appropriate Data Steward, System Owner and/or line manager. In addition, all information held on laptops, tablets or other mobile devices and storage media must be encrypted using University prescribed software.

d. Information assets, other than those deemed to be 'Public', may only be transferred across networks, transmitted by post or other similar means, or copied to other media, when the confidentiality and integrity of the data can reasonably be assured.

e. Where held, paper-based / hard copies of information must be protected and handled according to the records management, distribution and authorisation levels specified for those documents.

f. The archiving of information assets and documents must take place with due consideration for legal and regulatory matters, align with the University Records Management and Retention Policy and be documented in a relevant Retention Schedule.

g. Backup of the University's information assets and the ability to recover them is an important priority. System owners, administrators and Data Stewards must ensure that appropriate backup, recovery and business continuity procedures are in place to meet the needs of the business, typically in liaison with IT Services.

h. Appropriate measures should be taken when permanently disposing of information assets, be it paper-based or electronic, including the disposal of IT equipment or storage media containing data.

i. All users must be aware of the risks of breaching confidentiality associated with the printing, photocopying or other duplication of University information.

11. Payment Acceptance Strategy and Cardholder Information

a. The University has an established PCI Steering Group which oversees the management of all payment processing (and cardholder information) across the University.

b. The Payment Acceptance Strategy (PAS) affirms that all payments processed using payment cards must comply with the Payment Card Industry Data Security Standard (PCI-DSS) and provides the overarching framework to ensure the efficient, inclusive and compliant delivery of University payment services. The PAS is applicable to all staff involved in processing payments on behalf of the University, all payment processes across the University and all systems and processes which link, directly and indirectly to payment processes.

c. The PAS shall be reviewed annually by the PCI Steering Group and will be submitted for annual approval by the Information Strategy Group.

12. User Management

a. Established procedures for the registration and de-registration of individual user accounts, and for managing access to University information systems, ensure that user permissions and access rights match their agreed account authorisations.

b. Users shall have a unique identifier (user ID) for their personal and sole use for access to University information services. The user ID must not be used by anyone else and associated passwords shall not be shared with any other person for any reason as defined within the University's IT Acceptable Use Policy.

c. System password management criteria and access control standards are established to minimise information security risks and yet allow the University's business activities to be carried out without undue hindrance.

d. User access to University information systems must be authorised by the relevant line manager and System Owner (or designate), including the appropriate access rights or privileges granted. User access rights must be adjusted appropriately, and in a timely manner, whenever there is a change in business need, change in staff role, and/or when staff leave the University.

13. Use of Computers

a. The University's IT Acceptable Use Policy (AUP) defines the appropriate use of University computers. The AUP is applicable to, and will be communicated to staff, students and other relevant parties.

b. All University IT equipment, mobile devices and storage media must be safeguarded appropriately - especially when left unattended.

c. University systems and central filestores should be used for the storage of digital information, where it will be protected by a regular automated backup service. The local storage of information on the hard drive of PCs and laptops, or on USB devices, is discouraged and should be reduced wherever possible.

d. All University information stored on a laptop or mobile device must be encrypted. It is the responsibility of the user to ensure this takes place, and that information is backed up appropriately.

e. Utmost care should be taken when transporting data on removable devices or media and all ***non-*** public information must be encrypted and should only be accessed from equipment in secure locations. Secure File Transfer (SFTP) is recommended wherever possible.

f. Email should only be used to communicate information where appropriate measures have been taken to ensure authenticity and confidentiality, that it is correctly addressed, and that the recipients are authorised to receive it.

g. Users are not permitted to load unapproved software on to the University's PCs, workstations, laptops or other IT devices (as stated within the University's IT Acceptable Use Policy).

14. System Planning

a. The implementation of new or upgraded software must be carefully planned and managed. Change control procedures shall be used for new University information systems, or additional enhancements to existing systems, jointly authorised by the System Owner, the PVC / Dean / Director(s) responsible for the information system, and by the Director of IT Services (or nominated designates).

b. The implementation of new or upgraded software must be carefully planned and managed, to ensure that the information security risks associated with such changes are mitigated using a combination of procedural and technical controls.

c. Equipment supporting business systems shall be planned to ensure that adequate processing power, storage and network capacity are available for current and projected needs, all with appropriate levels of resilience and fault tolerance and are given adequate protection from unauthorised access, environmental hazards and electrical power failures.

15. System Management

a. The University's information systems must be managed by suitably trained and qualified staff to oversee their day-to-day running and to preserve security and integrity in collaboration with nominated System Owners and Data Stewards.

b. Access controls for all information systems must be set at appropriate levels, and access to operating system commands and application system functions is restricted to those authorised to perform systems administration or management functions.

c. Default system passwords must be changed or disabled at initial installation / implementation.

d. Systems must be up to date and patched in a timely (and planned) manner to preserve security and integrity of said system.

e. Capacity demands of systems supporting business processes must be monitored and projections of future capacity requirements made to enable adequate processing power, storage and network capacity to be made available.

f. System clocks must be regularly synchronised between the University's various processing platforms.

g. Security, operational and error logs must be maintained and reviewed by qualified staff.

16. Network Management

a. The University's network is managed by suitably authorised and qualified staff to oversee its day-to-day running and to preserve its security and integrity.

b. The network should be designed and configured to deliver high performance and reliability to meet the business needs whilst providing a high degree of access control and privilege restrictions.

c. Networks and communication systems must be adequately configured, updated and maintained to safeguarded against both physical attack and unauthorised intrusion. All moves, changes and other reconfigurations of network infrastructure will only be carried by staff authorised IT Services staff.

d. Access to the resources on the network will be controlled to prevent unauthorised access and access control procedures must provide adequate safeguards through robust identification and authentication techniques. Remote network access will be subject to similarly robust authentication.

17. Software Management

a. The University's information systems and business applications will be managed by suitably trained and qualified staff to oversee their day to day running and to preserve security and integrity in collaboration with nominated System Owners and Data Stewards.

b. Default system passwords must be changed or disabled at initial installation / implementation.

c. Software applications must be up to date and patched in a timely (and planned) manner to preserve security and integrity of said software.

d. Change control procedures will be used for changes or upgrades to University information systems and these must be authorised by the System Owner (or designate). All application software upgrades must be tested and approved changes are applied to the live environment.

e. The procurement or implementation of new, or upgraded, software must be approved, planned and managed in line with established policies and procedures, and any software development for or by the University should follow the established approval processes.

f. Modifications to vendor supplied software and the development of interfacing software shall only be undertaken in a planned, authorised and controlled manner by suitably trained and qualified staff.

18. Mobile Computing and Teleworking

a. Persons who undertake part or all of their work from a location outside the University, and/or those accessing information systems remotely, must be authorised to do so by the appropriate authorities within the University – typically the HoD / PVC-Dean / Director, the System Owner and the IT ServiceDesk.

b. Users of mobile computing equipment, and those working from an off-campus location, must comply with guidelines on the use of such equipment advising them on how to use these in ways that conform to the University's Information Security Policy and Information Handling guidance, IT AUP and other good practices.

c. All authorised users of the University Remote Desktop Service must do so using Multi-Factor Authentication.