Information Security Policy

2022-2023

Edge Hill University

Contents

Summary
This Policy aims to provide clear information for our community on what constitutes best Information Security practice to ensure that University information is captured, stored, read, modified, accessed and processed in a compliant manner, for stated 'uses', and by those who have the right to do so. It seeks to define how our IT user community can reduce risk, maintain compliance and help to protect the University and its members from potential breaches, failures of data integrity or interruptions to the availability of information.

Glossary of Terms

Data Stewards

Designated staff members with responsibility for ensuring the data sets they oversee are managed within the guidelines of the Policy.

Multi Factor Authentication (MFA)

An IT security technology that requires two or more distinct mechanisms to validate a user's identity. MFA can prevent unauthorised access to IT applications and sensitive data, and helps defend against identity theft, cyberattacks and data breaches.

System Owners

Designated staff members with responsibility for ensuring the IT systems / applications they oversee are managed within the guidelines of the Policy.

Purpose

The purpose of this Policy is to define the IT security standards and best-practice approaches relating to people, processes and technology to ensure the continued availability, quality, integrity, confidentiality and security of University's information assets. It seeks to protect the University and those accessing our information assets from inappropriate, insecure or non-compliant actions.

This Policy applies to all members of staff including temporary and associate staff, researchers, students, partners, contractors, external agencies and all other relevant parties (i.e. anyone authorised to use or access University data, IT systems and/or services, from on or off campus). All users of University data, information and/or systems have a responsibility to read and adhere to this Policy, and to manage and protect information under their possession.

1. Policy

1.1 It is the policy of the University that information is governed and managed in a compliant manner, and secured appropriately, to protect the University and its members from the consequences of a potential data loss or breach.

1.3 Undesirable consequences associated with a potential data loss or breach include unauthorised access to data, failure of data integrity, information or systems being unavailable, fraud, adverse publicity and/or reputational risk.

1.4 Information security can be achieved through the following:

a. An established information governance framework and defined IT security practices which are supported by workable processes and procedures

b. A well-informed and well-trained user community exercising an appropriate level of vigilance

c. The application of and adherence to technical (application-specific) security measures relevant to each information system and/or process, proportional to the assessed risk

d. Regular assessment of risks, review of mitigating controls, and documented incident management and recovery procedures.

1.5 The Information Strategy Group will provide direction and support for information security initiatives and, together with the Risk Management Group, shall ensure that business risks are regularly assessed and monitored to identify the likelihood / impact of potential information related threats and, where appropriate, that relevant mitigating controls exist.

1.6 The responsibility for ensuring the management of individual data sets and 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.

2. Information Governance and Records Management Principles

2.1 The following principles and guidance form the basis for the information governance and data management framework, 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

3. Information Asset Registration and Classification

3.1 The Information Governance Office (Strategic Planning and Policy Unit) maintain the central University register of all Information Assets.

3.2 Four information classifications have been established to support the capture, handling, retention and disposal of data assets.

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

3.3 IT Services maintain a central register of all departmental submissions of IT applications, systems and services, as recorded in the IT Service Catalogue.

4. Business Continuity Planning

4.1 The University's Emergency Management Policy (EMP) and Procedure 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 an emergency event.

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

4.3 The University Risk Management Group monitors and maintains a Risk Register of business-critical risks, and a Board Assurance Framework report is reviewed regularly by the Governors Audit Committee.

4.4 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.

4.5 A Data Breach Policy is published with supporting procedures and guidance (see Section 18).

5. Compliance

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

5.2 The University has established policies and procedures defining our information governance, data and records management and information security standards. 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
- Payment Acceptance Strategy

5.3 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.

5.4 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 of Policy will be investigated and may be dealt with under the University's disciplinary procedures.

5.5 Further specific guidance and training is available to staff users of corporate information systems.

6. Outsourcing and Third-Party Access

6.1 External suppliers who are contracted to supply goods or services to the University should, where appropriate, be provided with copies of the University's Information Security Policy (IT Acceptable Use Policy and the Data Protection Policy) and will be required to agree to adhere to the relevant policies to ensure University information assets remain protected.

6.2 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, where appropriate, legal action may be pursued.

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

7. Human Resources

7.1 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.

7.2 Staff with line management responsibilities must ensure that their supervised staff members are aware of, trained and comply with, information governance and information security policies and guidance.

7.3 All employees 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.

7.4 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.

8. Operations

8.1 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.

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

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

8.4 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.

8.5 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.

9. Information Handling

9.1 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.

9.2 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.

9.3 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.

9.4 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. All information held on laptops, tablets or other mobile devices and storage media must be encrypted using University prescribed software.

9.5 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.

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

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

9.8 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.

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

10. Payment Acceptance Strategy and Cardholder Information

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

10.2 The Card Payment Data Security Policy requires that all card payments should align with the Payment Card Industry Data Security Standard (PCI-DSS). The Policy provides the overarching framework to ensure the efficient and compliant provision of University payment services, are 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.

11. User Management

11.1 Established procedures for the registration, approval 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.

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

11.3 Central password management criteria and access control standards are defined and, where available, Multi Factor Authentication (MFA) must be used.

11.4 Privileged Access Management (PAM) has been introduced across the technical IT infrastructure to establish additional control (and protection) of elevated "privileged" access to specific user accounts, processes, and/or systems.

11.5 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.

12. Use of Computers

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

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

12.3 University systems and central file stores 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.

12.4 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, where required, that information is backed up appropriately.

12.5 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.

12.6 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.

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

13. System Planning

13.1 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).

13.2 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.

13.3 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.

14. System Management

14.1 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.

14.2 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.

14.3 Default system passwords must be changed or disabled at initial installation / implementation. Where available, Multi Factor Authentication must be used.

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

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

14.6 System clocks must be regularly synchronised to ensure continuity.

14.7 Security, operational and error logs must be maintained and reviewed by authorised staff.

15. Network Management

15.1 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.

15.2 The network should be designed and configured to deliver high performance to meet University needs, and to provide the required degree of access control and privilege restrictions.

15.3 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 must only be carried by staff authorised staff.

15.4 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 techniques including Multi Factor Authentication.

15.5 Penetration Testing will be completed by an approved scanning vendor on an annual basis and must follow an industry-accepted approach. The focus and defined scope will be informed by current and relevant cyber threat intelligence from trusted sources (eg Jisc, NCSC, etc), and will take account of any significant IT-related developments and/or changes. The (vulnerability) findings from penetration tests will be prioritised based on their CVSS score, with resulting actions, mitigations and remediations planned and implemented to agreed timescales.

16. Software Management

16.1 The University's information systems / business applications will be managed by suitably trained and authorised staff, typically System Owners and Data Stewards, to oversee their day to day running, security and integrity.

16.2 Default system passwords must be changed or disabled at initial installation / implementation. Multi Factor Authentication must be used where available.

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

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

16.5 The procurement or implementation of new, or upgraded, software must be approved, planned and managed in line with established policies and procedures. Any bespoke software development for or by the University should also follow the established approval processes and change control procedures.

16.6 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 authorised staff.

17. Mobile Computing and Teleworking

17.1 Persons who undertake part or all 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 PVC-Dean / Director / HoD and the System Owner, typically in liaison with the IT Service Desk.

17.2 Users of portable / 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, the IT Acceptable Use Policy and other relevant Information Governance policies and procedures.

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

18. Data Breaches and Cyber / IT Security Incident Reporting

18.1 All users of University systems must immediately report any incident (or suspected breach) involving personal data to the Information Governance Office (dataprotection@edgehill.ac.uk) as documented at *https://go.edgehill.ac.uk/display/compliance/Data+Security+Breaches*

18.2 Any cyber or IT security incident, suspected incident, near miss and/or email of concern, should be reported to the IT Service Desk (itservicedesk@edgehill.ac.uk). Further details available on the IT Services Wiki *https://go.edgehill.ac.uk/display/itservices/Important+reminder%3A+Online+security*

Key to Relevant Documents

Relevant University documents and UK legislation which relate to and/or govern the provision and use of IT facilities include:

Edge Hill University

- Information Strategy
- Records Management & retention Policy
- Data Protection Policy
- Data Quality Policy
- Privacy Policy
- Data Security Breach Policy
- GDPR Training Policy
- Card Payment Data Security Policy
- IT Acceptable Use Policy

Endmatter

Title	Information Security Policy
Policy Owner	Director of IT Services
Approved by	Information Strategy Group
Date of Approval	1st November 2022
Date for Review	June 2023