Information Management and Security Policy

Organisation	Leeds Beckett University
Author(s)	Head of Information Governance
Developed in consultation with	University Secretary Records and Information Governance Manager
Owner	University Secretariat Office
Target audience	Staff
Sensitivity	Public
Approved by	Information Management Operations Group
Endorsed by	University Executive Team
Effective date	01-11-2020
Review Date	07-2023
Status	Published
External references	
Links to other internal policies / procedures	
Version reference	1.00
Version history and summary of changes	Supersedes the Information Security Policy

Contents

1.0 Introduction/Background

1.1 Information, in all its forms, is crucial to the effective functioning and good governance of our University. We are committed to efficient and effective information management and information security to ensure that all the information and information systems on which the University depends are adequately protected. Our University's information, paper and electronic systems, applications and the networks that support it are important institutional assets.

1.2 An asset could be a single significant document or a set of related data, documents or files; it can be shared or be confined to a specified purpose or an organisational business unit. It could be operating systems, infrastructure, business applications, off-the-shelf products, services, user developed applications, policies, business continuity plans, records and information. It could be stored on computers, printed out, written down, transmitted across networks and spoken in conversations.

1.3 Information security covers the policies and procedures in place to protect information and information systems from unauthorised access, use, disclosure, disruption, modification, or destruction. It is one of the fundamental components of the University's Information Governance Framework as it will ensure the University is able to protect the confidentiality, integrity and availability of information within the organisation.

1.4 All organisations are facing increased cyber security threats. Systems and networks may be the target of computer-based fraud, computer viruses, computer hackers or insiders and these threats are becoming more widespread, more ambitious and increasingly sophisticated and it is important that the University builds up its resilience against cyber security threats. This resilience includes the ability to a) manage and protect, b) identify and detect, c) respond and recover and d) govern and assure the security of the University's information.

2.0 Legal and regulatory framework

2.1 The University has a statutory duty to ensure to that the personal data and information it holds complies with the law and the regulations to which it is accountable. The General Data Protection Regulation 2016 (GDPR) and the Data Protection Act 2018 provides individuals with more control over the privacy of their personal information.

2.2 The security principle of the GDPR requires that personal data is processed securely by means of 'appropriate technical and organisational measures'. To do this the University must ensure risk analysis, organisational policies, and physical and technical measures are in place. The result of having these measures in place will ensure the 'confidentiality (security), integrity and availability' of information systems and the personal data processed within them.

2.3 The Information Commissioner's Office (ICO) has the power to fine organisations up to a maximum of 20 million euros (or equivalent in sterling) or 4% of worldwide in the preceding financial year, whichever is higher for breaches of the Data Protection Act and GDPR. Any loss or unauthorised disclosure of personal data by the University has the potential to damage our reputation and cause financial loss.

2.4 The University is also required to have effective arrangements for the management and quality assurance of data submitted to the Office for Students (OfS), Higher Education Statistics Agency (HESA and other funding bodies). This includes student, staff, financial and estates data.

2.5 The Freedom of Information Act 2000 also provides a general right of public access to all types of recorded information held by public authorities in order to promote a culture of openness and transparency. Section 46 Records Management code of practice information security and data protection are identified as key elements of effective compliance with this Act.

2.6 The Privacy and Electronic Communications Regulations (PECR) sit alongside the Data Protection Act and the GDPR. They give people specific privacy rights in relation to electronic communications.
There are specific rules on:

- marketing calls, emails, texts and faxes;
- cookies (and similar technologies);
- keeping communications services secure; and
- customer privacy as regards traffic and location data, itemised billing, line identification, and directory listings.

In addition, we are required to abide by all UK and EU legislation and subject to the terms of any contractual obligations relating to the management of information, including but not limited to the following:

- Computer Misuse Act 1990
- Copyright Designs and Patents Act 1988
- Counter-Terrorism and Security Act 2015
- Cyber Essentials Accreditation
- Data Protection Act 2018
- Equality Act 2010
- General Data Protection Regulation 2016
- Human Rights Act 1998
- Freedom of Information Act 2000
- Malicious Communications Act 1988
- Privacy and Electronic Communications Regulations 2003
- Regulation of Investigatory Powers Act 2000
- Terrorism Act 2006
- PCI DSS (Payment Card Industries Data Security Standard)

3.0 Policy Aims and approach

3.1 This Information Management and Security Policy supports the University's Information Governance Framework and sets out how the information we manage shall be appropriately secured to protect against the consequences of breaches of confidentiality (security), failures of integrity, or interruptions to the availability of that information and ensure compliance with Data Protection and GDPR requirements.

4.0 Policy Structure

4.1 The Information Management and Security Policy sets out the University's Information Management and Security agenda in support of its Information Governance Framework that will deliver its commitment to this important agenda, which is essential to the whole University in its teaching, research, enterprise and administrative functions.

4.2 Elements of the structure and content of this policy is based on the approach set out in ISO 27001 (formally known as ISO/IEC 27001:2005) which is a specification for an information security management system (ISMS). An ISMS is a framework of policies and procedures that includes all legal, physical and technical controls involved in an organisation's information risk management processes that contributes to good information security practice.

4.3 This overarching Policy is underpinned by other policy commitments and procedures as set out in the University's Information Governance Framework and grouped under three main headings, namely:

- Business Continuity (section A)
- Information Management and Security, risk and compliance (section B)
- IT Information Security (section C)

which seek to clarify management actions as well as the individual and collective responsibilities of staff, students and partners to enable them to process information securely and in appropriate and informed ways in carrying out all their activities across the University.

4.4 This subsidiary information, policy and guidance shall be considered part of this Policy and shall have equal standing.

4.5 This Information Management and Security Policy forms part of the University's wider policy and procedural frameworks, including its General Regulations for students and the contractual terms and conditions for staff and other relevant parties. It is applicable to and will be communicated to staff, students and other relevant parties.

4.6 This policy shall be reviewed and updated regularly to ensure that it remains appropriate in the light of any relevant changes to the law, organisational policies or contractual obligations.

5.0 Scope of the Policy

5.1 The Information Management and Security Policy covers the protection of all forms of information to include its confidentiality (security), integrity and availability and applies to:

(a) all individuals with access to University information systems, including staff, students, visitors, contractors and other relevant parties.

(b) all systems and applications attached to the University computer or telephone networks and any systems supplied by the University.

(c) all information (data), personal and sensitive personal (special category) information processed by the University pursuant to its operational activities, regardless of whether it is processed electronically or in paper (hard copy) form, any communications sent to or from the University and any University information (data) held on systems external to the University's network.

(d) all external parties with access to University information systems, that provide services to the University in respect of information processing facilities and business activities.

(e) principal electronic and paper information assets including all the physical locations from which the University operates.

6.0 Responsibilities and/or Duties

6.1 This policy forms part of the University's information governance and risk management frameworks that are overseen by the Board of Governors through its Governance & Nominations and Audit Committees.

6.2 Under the University's Information Governance Framework the Board of Governors has ultimate responsibility for ensuring General Data Protection Regulation and Data Protection compliance which includes effective information management and information security measures.

6.3 A Strategic Information Management Group (SIMG) has responsibility for overseeing the approach, development and review of the Information Governance Framework across the University and reports to University Executive Team as necessary.

6.4 An Information Management Operations Group (IMOG) is the operational arm of SIMG and is responsible for co-ordinating the implementation of the University's Information Governance Framework which includes a Data Protection Policy. This Group reports to SIMG as a standing item of business at each of its meetings.

6.5 SIMG is chaired by the University's Secretary as Data Protection Officer and comprises members whom are 'senior information risk owners' and IMOG is chaired by the Head

of Information Governance and comprises managers from across the institution as 'information asset owners'.

6.6 Senior Information Risk Owners are accountable for the overall development of information management and information security, providing accountability and assurance to Governance & Nominations and Audit Committees on compliance with the Information Governance Framework and supporting policies.

6.7 Information Asset Owners responsible for information assets, business activities, information systems or individuals must ensure that information management and security policies and processes are disseminated appropriately and adhered to.

6.8 The Data Protection Officer is responsible for briefing the Board of Governors regarding data protection compliance and any issues arising from reported breaches of data protection or information security.

6.9 One of the objectives of the Universities Information Governance Framework shall be to ensure that there is clear direction and visible management support, appropriate commitment and adequate resourcing for information management and security initiatives.

6.10 The responsibility for ensuring the protection of information systems and ensuring that specific information management and security processes are carried out shall lie with the Dean of each School and Director of each Service managing that information system.

6.11 However, achieving our Information Governance Framework objectives and commitments depends on staff, students and partners working within the University's policies, legislation, regulations and best practice guidelines. It is the responsibility of all individuals, with access to the University's information, to adhere to the requirements set out in this policy and all the University's relevant policies that maintain the 'confidentiality (security), integrity and availability' of information systems and the personal data processed within them.

7.0 Reporting breaches of data protection and information security

7.1 If any staff, students, partners or relevant parties become aware of a data protection or information security incident they should report it to their Dean or Director of Service and the Head of Information Governance using the Universities Report a data breach link .

7.2 The Head of Information Governance will consider the nature of the incident and actions required by the University. This may include reporting it to the Information Commissioner (ICO) to comply with requirements to report breaches that will impact on individuals and the security of their personal within 72 hours under data protection legislation. It may also include reporting to the Police or taking legal advice as necessary.

7.3 Financial and Legal Services should also be notified of any incidents where there may be insurance or legal implications to the University.

7.4 The University will establish and maintain appropriate contacts with other organisations, law enforcement authorities, regulatory bodies, and network and telecommunications operators in respect of its information management and security.

7.5 The implementation of the Information Management and Security Policy shall be reviewed independently of those charged with its implementation, predominantly through the University's programme of internal audit reviews and will be reported to the Board of Governors through its Audit Committee.

8.0 Definitions

8.1 All definitions relating to Records Management, Information Governance and Information Compliance are captured in our short guide titled Information Governance Definitions.

9.0 Dissemination

9.1 This policy will be made available to IAO's as part of their training and made available to all staff through the Guidance Index. The policy will be published on the University internet and disseminated though the Strategic Information Management Group, Information Management Operations Group and the Information Asset Owner's.

10.0 Monitoring and Compliance

10.1 This policy will be reviewed by the University Records and Information Governance Manager no less than every three years. Any amendments or additions will be submitted to the Information Management Operations Group for approval. The next review is scheduled for July 2023

SECTION A

Business Continuity Planning & Information Management and Security

Policy Statement

1. The Head of Regulatory Compliance and Assurance shall assess business continuity requirements and identify appropriate areas for further action through a periodic review of the University's business continuity arrangements.

2. Information risk assessments are carried out as part of the University's Information Governance Framework which enables the classification of information systems according to their level of criticality to the University.

3. Data Protection Impact Assessments (DPIAs) are included in formal system acquisition, changes, development and maintenance procedures where personal data will be processed in order to identify and mitigate any potential risks to privacy.

4. A business continuity plan will be developed for each information system or activity. The nature of the plan and the actions it contains will be commensurate with the criticality of the information system or activity to which it relates.

5. All business continuity plans will be periodically tested. The frequency of testing will be as defined for the appropriate criticality level and will include tests to verify whether management and staff are able to put the plan into operation.

6. All relevant staff will receive appropriate training to be able to carry out their roles with respect to business continuity plans.

7. Each business continuity plan will be reviewed, and if necessary updated. The frequency of reviews will be as defined for the appropriate criticality level.

Related policies:

Risk Management Policy
Crisis Management Plan (including Crisis Response and Business Recovery Plans)

SECTION B

Governance, Risk & Compliance & Information Management and Security

Policy Statement

1. It is the responsibility of all individuals, with access to the University's information, to adhere to the requirements set out in this policy and all the University's relevant policies that maintain the 'confidentiality (security), integrity and availability' of information systems and the personal data processed within them.

2. The Terms and Conditions of Employment set out all employees' responsibilities with respect to their use of paper and electronic information systems and the information held on them. Line managers must provide specific guidance on legal compliance to any member of staff whose duties require it.

3. The Student Contract set out all students' responsibilities with respect to their use of electronic devices including the accessing and use of paper and electronic information systems and data.

4. All members of the University will comply with the Information Management and Security Policy and, where appropriate, their compliance will be monitored.

5. Personal or confidential information will only be disclosed or shared where an employee has been authorised to do so.

6. The University will only process personal and sensitive personal (special category) data in accordance with the requirements of the data protection legislation. The University's Data Protection Policy sets out the principles and lawful basis for processing personal data.

7. Before any new information systems processing personal and sensitive personal data are introduced, a Data Protection Impact Assessment process will be carried out to ensure the University complies with its Data Protection and GDPR requirements, which will include an assessment of the legal and contractual requirements that may arise from the use of the system. These systems will be documented on the Service or School's Information Asset Register and a named Information Asset Owner, with responsibility for ensuring data protection compliance for that information, will be identified.

8. Before any new systems are introduced, a risk assessment will be required to be carried out to identify any legal obligations that may arise from the use of the system. These legal obligations will be documented and a named system controller, with responsibility for updating that information, will be identified.

9. Guidance is available to all electronic device users covering the key aspects of legislation governing the use of data and personal data, in so far as they relate to the use of information systems. Guidance is also available on the key aspects of computer misuse legislation.

10. The institution's policies forbid the use of information systems to send or publish derogatory remarks about people or organisations.

11. The University's records retention schedule defines the appropriate length of time for different types of information to be held. Information will not be destroyed prior to the expiry of the relevant retention period and will not be retained beyond that period. During the retention period appropriate technical systems should be maintained to ensure that the information can be accessed.

12. Where it is necessary to collect evidence from the information systems, it shall be collected and presented to conform to the relevant rules of evidence.

13. All of the organisation's information systems will be operated and administered in accordance with the University's Information Governance Framework and locally documented and approved procedures.

<u>Third Party Access & Information Management and Security</u>

14. All third parties who are given access to the University's information systems, whether suppliers, customers or otherwise, must agree to follow the University's information management and security policies and ensure they can comply with the University's requirements under information legislation. A summary of the information management and security policies and the third party's role in ensuring compliance should be provided to any such third party, prior to their being granted access.

15. The University must assess the risk to its information and, where deemed appropriate because of the confidentiality, sensitivity or value of the information being disclosed or made accessible, the University will require external suppliers of services to sign a data processing agreement to protect its information assets and the personal data that they contain.

16. Those responsible for agreeing maintenance and support contracts will ensure that the contracts being signed are in accord with the content and spirit of the University's information management and security policies and that Data Protection Impact Assessments have been undertaken and any identified risks are mitigated to ensure information legislation is complied with.

17. All contracts with external suppliers for the supply of services to the University must be monitored and reviewed to ensure that information management and security requirements are being satisfied. Contracts must include appropriated provisions to ensure the continued security of information and systems in the event that a contract is terminated or transferred to another supplier.

18. Any facilities management, outsourcing or similar company with which this University may do business must be able to demonstrate compliance with the University's information management and security policies and enter into binding service level agreements that specify the performance to be delivered and the remedies available in case of non-compliance.

Human Resource Policy & Information Management and Security

19. All employees must comply with the information management and security policies of the University in support of its Information Governance Framework.

20. Any information management and security incidents resulting from non-compliance should result in appropriate disciplinary action.

21. If, after investigation, a user is found to have violated the University's Information Management and Security Policy requirements and/or procedures, they may be disciplined in line with the University's formal disciplinary process.

22. The Terms and Conditions of Employment of the University include requirements to comply with information management and security policies and to protect the confidentiality of information, both during and after employment with the University.

23. All employees are required to sign a formal undertaking concerning the need to protect the confidentiality of information, both during and after their employment with the University.

24. Non-disclosure agreements must be used in all situations where the confidentiality, sensitivity or value of the information being disclosed is important.

25. All external suppliers who are contracted to supply services to the University must agree to follow the information management and security policies of the University.

26. All staff are to be provided with information management and security awareness tools to enhance awareness and educate them regarding the range of threats, the appropriate safeguards, and the need for reporting suspected problems.

27. An appropriate summary of the information management and security policies must be formally delivered to, and accepted by, all temporary staff, prior to their starting any work for the University.

28. The Casual Worker Agreement includes requirements to comply with data protection policies (including IT security policies) and to protect the confidentiality of information, both during and after engagement with the University. Training will be provided on commencement of engagement to ensure that casual and temporary workers are able to effectively carry out their roles.

29. Periodic training for those predominantly responsible for information management and security on a day-to-day basis is to be prioritised to educate and train in the latest threats and information security techniques.

30. All new staff are to receive mandatory information security awareness training, including Data Protection training, as part of induction.

31. Where staff change jobs, their information management and security needs must be reassessed and any new training provided as a priority.

32. Training in information security threats and safeguards for technical staff is mandatory, with the extent of technical training to reflect the job holder's individual responsibility for configuring and maintaining information security safeguards.

33. Where IT staff change jobs, their information management and security needs must be reassessed and any new training provided as a priority.

34. Upon notification of staff resignations, the school or service staff manager must consider whether the member of staff's continued system access rights constitute an unacceptable risk to the University and, if so, revoke all access rights.

35. 35. Departing staff are to be treated sensitively, in taking into account the termination of their access privileges.

36. Departing staff must return all information assets, equipment and devices belonging to the University, unless agreed otherwise with the designated owner responsible for the information asset.

Related documentation, policies and procedures:

- Accuracy of Published Information Procedures
- Code of Practice on the Freedom of Speech and Expression
- Code of Good Practice and Regulations relating to Misconduct in Academic Research
- Data Protection Policy
- Data Retention Schedule
- Information Classification Procedure
- Intellectual Property Policy (subject to approval)
- Policy, Regulations, and Procedures Relating to Professional Suitability or Professional Misconduct
- Records Management Policy
- Research Ethics Policy and Procedures
- Student Code of Discipline
- Student Contract
- Social Media Policy
- Terms and Conditions of Employment
- Whistleblowing (Public Interest Disclosure) Complaints Procedure

SECTION C

Principle IT Security

Policy Summary

This policy sets out the University's definition of, commitment to and requirements for IT security. It specifies regulations to be implemented to secure the Information Technology (IT) that the University manages and to protect against the consequences of breaches of security and confidentiality, failures of integrity and interruption to availability. It will refer to more specific policy documents covering these specific needs.

This policy provides management direction and support for IT Security across the University. It has been ratified by the University Executive Team of the University and forms part of its Information Management and Security policies and procedures that supports the University's Information Governance Framework. It is applicable to, and will be communicated to, staff, students and other relevant parties. This document includes:

- Legal requirements that the University must abide by, including the statutory duty, under the Counter Terrorism and Security Act 2015, termed "PREVENT" to aid the process of preventing people being drawn into terrorism.
- The purpose, scope and structure of the IT Security policy documentation.
- Responsibility for IT Security Policy documentation.
- Responsibilities for implementing IT Security policies.

Measures that will be taken by the University to implement information technology and security policies include:

1. Ensuring that all individuals who use information technology systems, or otherwise handle information, understand the policies that are relevant to them and any consequences for noncompliance.

2. Using physical security measures when deemed necessary.

3. Applying technology where considered appropriate and feasible. For example, to control and log access to systems, data and functionality.

4. Using various lawful forms of monitoring activities, data and network traffic to detect policy infringements.

5. Taking into account relevant information management and security policy requirements when planning and undertaking activities involving IT-based information technology systems.

6. Formal or informal risk assessment, to identify the probability and impact that various hazards could have on information technology systems.

7. Monitoring effectiveness of its information security policy implementation. This may involve review independent from those charged with its implementation.

8. The Director of IMTS is responsible for the implementation and management of Information Technology Security Policies at the University.

9. It is the responsibility of the University to sufficiently resource and direct implementation of these policies.

10. Individuals must understand and agree to abide by University IT policies and Regulations before being authorised for access to any information technology systems for which the University has responsibility.

Related IT Security Policies:

- IT Security Policy Overview
- Bring Your Own Device Policy
- Computer Protection Policy
- Cryptography Policy
- Information Handling Policy
- Mobile Computing Policy
- Network Management Policy
- Software Management Policy
- System Planning and Management Policy
- User Management Policy
- Use of Computers Policy
- Wireless Communications Policy
- Password Policy