Loughborough University

Information Security

Information Governance & Security Policy

Version 1.0:
Approved January 2022
Review July 2026

Information Governance & Security Policy

1. Introduction

1.1. Information is a vital asset to the University. It underpins the University's research, and innovation, education and student experience, and equity, diversity, and inclusion activities. It is fundamental to all other functions associated with its staff, students, funders, collaborators, and strategic partners as well as the efficient management of all its services and resources.

1.2. Good information governance practice is therefore of paramount importance, including the adoption of appropriate policies, procedures and structures which enable the secure, efficient and effective use of data whilst protecting the privacy of data subjects.

1.3. The University's information governance framework seeks to strike an appropriate balance between openness and confidentiality in the management and use of information. It applies equally to all information and data throughout its entire lifecycle, regardless of its source, content or composition. It extends to both physical and electronic formats, and is not restricted to data held in corporate systems; it also encapsulates data used or generated as part of education and student experience, or research activity, etc.

1.4. The University is committed to protecting the security of its information and information systems in order to ensure that the integrity of information is maintained, so that it is accurate, up to date and 'fit for purpose'; information is always available to those who have a legitimate need for it and there is no disruption to the business of the University; confidentiality is not breached, so that information is accessed only by those authorised to do so.

1.5. Cyber Security (sometimes known as IT Security) is a distinct subset of the information governance framework and covers the technology and procedures deployed to protect the university's data, systems and infrastructure from malicious or unauthorised misuse.

2. Scope

2.1. This policy provides a framework for the management of information security throughout the University and applies to:

2.1.1. All those with access to university information and information systems, including staff, doctoral researchers, students, partners and contractors;

2.1.2. Any systems attached to the University IT or telephone networks and any systems supplied by the University;

2.1.3. All information stored or processed by the University for its operational activities, regardless of whether it is stored or processed electronically or in hard copy form, including any communications sent to or from the University and any University information held on systems external to the University network;

2.1.4. All external and third parties that provide services to the University in respect of information processing facilities and business activities.

3. Information Governance and Information Security Policy Framework

3.1. This framework incorporates policies to ensure the University complies with relevant legislative requirements and professional standards and is made up of the following sub policies:

3.1.1. Information Governance and Security Policy (this policy) (relevant to all)

3.1.2. Information Categories and Controls Policy

3.1.3. Responsibilities of all Staff and Doctoral Researchers

3.1.4. IT Acceptable Use Policy

3.1.5. Information Services and Service Contractors Policy (relevant largely to IT professionals or others involved in procuring IT related services)

3.1.6. Information Sharing Policy (relevant to all)

3.1.7. Mobile and Remote Working Policy

3.1.8. Policy on the Management of User Access to Information (relevant to all)

3.1.9. IT Operations Policy (relevant to IT professionals)

3.1.10. Information Security Incident Handling and Review Policy (relevant to all)

3.2. The following policies are also relevant to all staff and students (taught and research):

3.2.1. Data Protection Policy

3.2.2. Freedom of Information Policy

3.2.3. Copyright Policy

3.2.4. Software Policy

4. Principles

4.1. General

4.1.1. There are 3 key interlinked strands to the University's information governance policy:

- Openness
- Legal compliance
- Information management and security

4.2. Openness

4.2.1. Non-confidential information on the University and all its activities should be available to the public through a variety of media. This may include through: open access publishing, the institutional repository, Freedom of Information Act compliance, etc.

4.2.2. In accordance with Data Protection legislation, individuals have the right to know how their personal data will be used, to be confident that the data held is accurate and to access their personal information on request.

4.2.3. The University has clear procedures and arrangements for liaison with the press, on-line and broadcasting media through its Marketing and Advancement function.

4.2.4. The University has clear procedures and arrangements for handling queries from our staff, students, funders, collaborators, strategic partners, suppliers and the public. The University supports the effective sharing of data where appropriate but pays due regard to confidentiality in relation to personal and commercially sensitive information.

4.3. Legal Compliance

4.3.1. The University aims to handle all identifiable personal and commercial information relating to its staff, students, funders, collaborators, and strategic partners and as processed in the course of its research activities in accordance with the requirements of relevant legislation.

4.3.2. Where significant risk has been identified, the University will undertake or commission regular and appropriate assessments and audits of its compliance with legal requirements.

4.3.3. The University has established and will maintain policies and procedures to ensure compliance with all relevant legislation, including for the protection of the privacy of individuals and for the controlled and appropriate sharing of information with other agencies.

4.3.4. Compliance activity and controls are prioritised where the greatest risks have been identified and the University's approach seeks to support the pursuit of academic excellence, innovation and operational effectiveness.

4.4. Information Management and Security

4.4.1. The University has established and implements policies, procedures and working practices (the rules) for the effective and secure management of its information assets including cyber security.

4.4.2. The University aims to know of all the information assets (including non-personal information) it holds, and the rules that apply to them. Those rules should be held in a single location and be accessible to anyone with an information governance or processing role.

4.4.3. Information is integral to all operational or academic activity and therefore its governance needs to be considered as part of all process optimisation or change activity.

4.4.4. Where significant risk has been identified, the University will undertake or commission regular and appropriate assessments and audits of its information management and cyber security arrangements.

4.4.5. A set of well-defined roles has been developed which set out accountability and responsibility for both the quality and the governance of each of the key information assets of the University. All information and, personal data in particular, will have clear “ownership” within the University (See Section 3 and Annex).

4.4.6. Staff, students, partners and suppliers of the University are given the necessary tools, knowledge and resources to manage information responsibly and effectively, including targeted training, functional and secure information systems and clear policies and guidelines. Staff, students, partners and suppliers have a clear individual responsibility to understand and apply policies and good practice to their handling of information.

4.4.7. Effective deployment of the University’s corporate systems plays a key role in the secure management of the majority of personal data held by the University, in particular, in relation to students and staff. The University has established and maintains incident reporting procedures and monitors and investigates all reported instances of actual or potential breaches of data privacy, confidentiality and security.

5. Responsibilities

5.1. It is the role of the University Council to approve the University’s policy in respect of Information Governance, taking into account general legal and higher education sector-specific requirements. Council is also ultimately responsible via the Chief Operating Officer for ensuring that sufficient resources are provided to support the requirements of the framework.

5.2. The Information Technology and Governance Committee, comprising representation from across the University, with support from the Information Governance Sub-Committee, is responsible for overseeing Information Governance policy and planning,

developing and maintaining policies, standards, procedures and guidance, coordinating Information Governance in the University and raising awareness of Information Governance.

5.3. Staff and students are expected to take ownership of, and seek to improve, the quality of information within their specified areas of activity. Professional Services have responsibility for end-to-end processes in their areas of activity and this responsibility includes ensuring effective information governance in relation to these processes. There is also an expectation that this policy and its supporting standards and guidelines are built into any local processes and procedures and that there is on-going compliance.

5.4. All staff, whether permanent, temporary or contracted, and contractors/suppliers are responsible for ensuring that they are aware of the requirements incumbent upon them in and for ensuring that they comply with these on a day to day basis.

Specific responsibilities of key staff will be found in Annex 1.

This policy document will be reviewed on a three-yearly basis by the Information Governance Sub-Committee of the Information Technology and Governance Committee.

Annex 1 Staff Responsibilities

1. Chief Operating Officer

The Chief Operating Officer (COO) is responsible to the Vice-Chancellor on a delegated basis for the general oversight and development of information governance policy. The COO has responsibility for ensuring policies and procedures are implemented and that mechanisms are established to monitor their effectiveness.

2. Deans of Schools and Heads of Professional Services

Deans of Schools and Heads of Professional Services have responsibility for the implementation of University information governance policies and procedures in their Schools and Services. The Dean or Head of Service should demonstrate visible commitment to good information governance by:

a) Ensuring that all staff undertake the general training in good information governance practice provided by the University.

b) Ensuring that staff undertake specialised information governance training relevant to their roles (e.g. research data management).

c) Ensuring that there are systems in the School or Service to maintain awareness of the information held and to ensure it is stored, used and shared only in accordance with University policies and procedures.

d) Providing sufficient resources for staff to be able to comply with University policies and procedures.

e) Bringing to the attention of the COO, any breach of statutory requirements which cannot be dealt with at School/Service level and/or may have implications for the University more widely.

f) Ensuring that staff co-operate fully with any information or information security audits authorised by the Information Technology and Governance Committee.

g) Ensuring students and staff are aware of the School or Service's procedures for secure handling of their personal data.

h) Ensuring that University information governance policies and procedures are followed in any dealings, formal or informal, with third party individuals and organisations.

3. Data Owners

The Data Owners have overall accountability for an area of institutional data (e.g., staff, students, research, finance) regardless of where that data is held. They are responsible for:

a) Setting the culture around data use and ensuring appropriate resources are in place to manage data governance risks and maximise the value of data.

b) Nominating Data Stewards to advise on applicable operational issues relating to data use within their area.

c) Identifying if any additional information governance training might be required to mitigate risks specific to their area.

4. Data Stewards

The Data Stewards has operational responsibility for specific information assets, appointed by a Data Owner, they are responsible for:

a) Implementing policies set in place by the Data Owner and/or relevant committees.

b) With expertise to understand the data and its processing in their area at a detailed level, act as the first point of liaison to resolve data issues where they are identified.

c) They are responsible for training and communications relating specifically to their area, as well as ensuring stakeholders are consulted on changes to structures or processes.

5. Information Governance Manager

The Information Governance Manager has strategic responsibility for building and embedding the information governance framework across the University. They are responsible for:

a) Developing institutional policy for the management and use of the University's information and data assets.

b) With expertise in information governance and legal compliance, offer guidance and training and matters relating to their areas of responsibility.

c) Ensuring the University has policies, processes and working practices in place to monitor the University's compliance with appropriate legal requirements.

d) They are responsible for training and communication relating to compliance with appropriate legal requirements and good practice relating to information governance and information security.

6. Data Co-ordinators

A designated member of staff in a School or Professional Service, they are responsible for maintaining a record of information processing activities specific to their area, and support the provision of good information management practices.

Annex 2 Key Definitions

By **Information** we mean any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphical, cartographical, narrative, or audiovisual.

By **Information Security** we mean the management of information to allow appropriate access and use for those who need it whilst preventing unauthorized access which might result in a breach of the University's legal responsibilities, the rights of individuals or might present a reputational risk to the institution. It includes arrangements to reduce the risk of copying, modification or deletion of information where this is not legitimate for the conduct of university activities.

The term "**the University**" in the Policy Framework should be interpreted in the widest sense and includes relevant activities, services and systems related to all Schools and Professional Services of the University as well as related to IT Services.

The risks to maintain good information security may be deliberate or accidental human acts or arise from technical or environmental factors.

Confidentiality - Confidentiality is the need to ensure that information is disclosed only to those who are authorised to view it.

Information Systems – Any system, service or infrastructure used to process information or the physical locations housing them. This includes critical business environments, business processes, business applications (including those under development), computer systems and networks.