Loughborough University

Information Security

Information Governance Policy

Approved
June 2016

www.lboro.ac.uk

Information Governance Policy

1. Summary

Information is a vital asset to the University. It underpins the University's Research, Teaching and Enterprise. It is fundamental to all other activities associated with its staff, students, funders, collaborators, and strategic partners as well as the efficient management of all its services and resources. It plays a key part in governance, planning and performance management.

It is therefore of paramount importance to ensure that information is efficiently managed, and that appropriate policies, procedures and management accountability and structures provide a robust governance framework for information management.

2. Principles

The University recognises the need for an appropriate balance between openness and confidentiality in the management and use of information. The University fully supports the principles of good corporate governance and recognises its public accountability, but equally places importance on the confidentiality of, and the security arrangements to safeguard, both personal and commercially sensitive information that is held by the institution. The University also recognises the need to share information and data with other organisations and other agencies in a controlled manner consistent with the interests of our staff, students, funders, collaborators and strategic partners and, in some circumstances and where appropriate, with the public.

The University believes that accurate, timely and relevant information is essential to deliver the highest quality in all its activities.

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

- Openness
- Legal compliance
- Information security

2.1. Openness

- 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.
- The University adopts a general policy of openness in terms of allowing individuals access to their personal information. Personal information will be maintained and released to the individuals concerned on request in accordance with the provisions of the Data Protection Act.
- The University has clear procedures and arrangements for liaison with the press, on-line and broadcasting media through its Marketing and Advancement function.

- The University will have clear procedures and arrangements for handling queries from our staff, students, funders, collaborators, strategic partners, suppliers and the public.
- The University will support the effective sharing of data where appropriate.

2.2. Legal Compliance

- The University regards 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 as confidential, except where relevant legislation requires otherwise.
- The University will undertake or commission regular and appropriate assessments and audits of its compliance with legal requirements.
- The University has established and will maintain policies to ensure compliance with all relevant legislation.
- The University has established and will maintain policies for the controlled and appropriate sharing of information with other agencies, taking account of relevant legislation.

2.3. Information Security

- The University will establish and maintain policies for the effective and secure management of its information assets and resources.
- The University will undertake or commission regular and appropriate assessments and audits of its information and IT security arrangements.
- The University will promote effective confidentiality and security practice to all its staff, students, partners and suppliers through policies, procedures and/or training as appropriate.
- The University, through the Information Governance Sub-Committee of the Information Technology and Governance Committee will establish and maintain incident reporting procedures and will monitor and investigate all reported instances of actual or potential breaches of confidentiality and information security.

3. Responsibilities

It is the role of the University Council to approve the University's policy in respect of Information Governance, taking into account legal and Higher Education Sector requirements. Council is also ultimately responsible via the Chief Operating Officer for ensuring that sufficient resources are provided to support the requirements of the policy.

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.

Staff and students are expected to take ownership of, and seek to improve, the quality of information within their specified areas of activity. There is also an expectation that this policy and its supporting standards and guidelines are built into local processes and procedures and that there is on-going compliance.

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 an annual 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.