Loughborough University

Information Security

Responsibilities of All Staff and Doctoral Researchers

Version 2:
Approved January 2022
Review January 2025

Responsibilities of All Staff and Doctoral Researchers

1. Purpose

This policy outlines the responsibilities of all staff and doctoral researchers in relation to information security and provides links and direction to other, relevant Information Security Policies.

2. Scope

This policy is relevant to all staff and doctoral researchers. The responsibilities of taught students have been incorporated into the Loughborough University IT Acceptable Use Policy.

The University's Introduction to Information Security Policy provides a brief overview of the approach and some useful definitions.

This policy should be read in conjunction with the Loughborough University IT Acceptable Use Policy

www.lboro.ac.uk/services/it/staff/help/policies/aup/

and in accordance with the University Data Protection policy,

www.lboro.ac.uk/admin/ar/policy/dpact/ludpp/

Freedom of Information Policy

www.lboro.ac.uk/admin/ar/policy/foi/

and Copyright Policies.

copyright.lboro.ac.uk/copyright/policy/copyright-policy/

Individuals with third party access to University information may also find this policy helpful.

3. Roles and Responsibilities

3.1 Safe, fair, and lawful use of IT facilities

The University Acceptable Use Policy (AUP) clearly states what can or cannot be done with the University's computing resources. You must read and comply with the AUP and any other information security policies the University has approved.

FIND OUT MORE: University Acceptable Use Policy

3.2 Responsibility for Information governance

Responsibility for information governance is overseen by University Council and delegated to individuals via the Information Technology and Governance Committee and the Information Governance Sub-Committee.

Deans of Schools and Heads of Professional Services are responsible for implementation of the University's information governance polices under their control, and they should demonstrate a visible commitment to good information governance.

FIND OUT MORE: Information Governance Policy

3.3 Using confidential or highly confidential data

When processing data and information you are required to consider the sensitivity, confidentiality or level of risk associated with its use and put appropriate organisational or technical control measures in place. If further clarification of appropriate control measures is needed these can be sought from the 'Data Owner'. Such measures are particularly important if you are using confidential or highly confidential information or data. This applies to personal or sensitive personal data about individuals.

FIND OUT MORE: Data Protection Policy

Information Categories and Controls Policy

3.4 Storage of physical and electronic information and data assets

Care must be given to ensuring that physical and electronic information and data assets are stored appropriately. Electronic confidential information must be stored in a secure environment (e.g., Office 365 one drive, encrypted laptop). Hardcopy confidential information must be stored in a lockable facility and kept locked when not in use.

FIND OUT MORE: Information Categories and Controls Policy

3.5 Access to confidential information and data

Access to confidential information and data must be strictly managed and controlled in order to protect individual's privacy, information confidentiality, the integrity of data and its availability.

FIND OUT MORE: Policy on the Management of User Access to Information

3.6 Third party data storage agreements

If you are entering into a data storage agreement with a third party or an external organisation, you are responsible for ensuring the integrity and security of the University's data, information, and systems are upheld.

FIND OUT MORE: Information Service and Service Contractors Policy

3.7 Information and data sharing

If you need to share information or data either within the University, or externally. You must put in place appropriate measures to share in a safe and secure way, based on the sensitivity, confidentiality, or risk associated with the information or data involved. The Data Owner can provide advice on risks associated with the category of data or information they are responsible for, and how it should be accessed or stored.

FIND OUT MORE: Information Sharing Policy

Information Sharing – Quick Guide

Information Sharing Flowchart

3.8 Managing access to information requests

Individuals hold the right to ask for information about the activities of the University, or for information the university holds about them by making a Freedom of Information (FOI) request, or a subject access request (SAR). If you receive either an FOI or SAR request, you need to bring this to the attention of your line manager, and, or contact the University Freedom of Information and data protection team respectively, who will be able to oversee the request and manage any reputational or commercial risks associated with it. By law the University is required to meet strict timelines for responding to such requests.

FIND OUT MORE: Freedom of Information Guidance

Subject Access Requests

3.9 Compliance with copyright policy

Copyright provides an author/creator of a work with legal protection. It is important to understand how copyright applies in learning, teaching and research, as you are required to ensure compliance with university copyright policy.

FIND OUT MORE: Copyright Policy

Copyright guidance

3.10 Mobile and remote working

When working away from a secure environment on one of the University campuses, you must take appropriate action to protect the integrity and security of the information, data, and systems you are working on. Particular care is required when handling confidential information in these circumstances.

FIND OUT MORE: Mobile and Remote Working Policy

3.11 Access to externally hosted software

You must ensure that your actions do not represent a risk to the effective operation, security and integrity of the University IT systems and environment and consult with IT Services if access to non-University maintained software is required.

FIND OUT MORE: Software Policy

3.12 Reporting a personal data breach or information security incident

If you become aware of a possible data breach or have a concern that information is not being handled in accordance with the University's information security policies; you must report it as soon as possible either to your Data Co-ordinator or using the personal data breach form available on the 'Current Students and Staff' homepage.

FIND OUT MORE: Management of Information Security Incident and Review of Policies

Report a data breach

3.13 Failure to comply with information security policies

Failure to comply with Loughborough University, information security policies may be treated as misconduct and could be subject to disciplinary action as per University Ordinance XVII (students) and Ordinance XXXV (staff).

FIND OUT MORE: Ordinance XVII (Students)

Ordinance XXXV (Staff)