Loughborough University

Information Security

Management of Information Security Incidents and Review of Policies

Version: 1.4
Approved February 2023
Review February 2027

Loughborough University

Management of Information Security Incidents, Data Breaches and Review of Policies

1. Purpose

The Information Governance Policy commits the University to investigating and monitoring all reported instances of actual or potential breaches of confidentiality and information security. The aim of investigation and monitoring is to minimise the risk of data loss to members of the University and the public, and, at the same time, manage any potential reputational damage to the University.

When handling information security incidents, the University will ensure that:

- Incidents are reported and investigated in a timely manner and by the appropriate staff member or staff members,
- Incidents are recorded, investigated, and reported to the appropriate sub-committee and committee,
- Incidents are handled in accordance with all appropriate legislation, and in particular the UK General Data Protection Regulation (GDPR), Data Protection Act 2018, and the Privacy and Electronic Communications Regulation (PECR),
- Incidents are reported to external bodies and affected individuals as and when it is appropriate to do so and in accordance with the relevant legislation,
- Investigations are undertaken in a fair and open manner.
- Incidents are reviewed to identify potential improvements to working practices and amendments to relevant policies.

As outlined in the Roles and Responsibilities for All Staff and Doctoral Researcher Policy and the IT Acceptable Use Policy, individuals are expected to report all potential and actual personal data breaches and security incidents to the appropriate staff member (see below, Section 3. Incident and Breach Handling) .

The Chief Operating Officer is the senior officer responsible for information governance and ensuring that all information security incidents are handled in a manner which ensures compliance with the relevant legislation.

2. Scope

This policy is relevant to all staff, doctoral researchers, students, external partners and the public.

3. Incident and Breach Handling

Once identified, all potential and actual data incidents must be reported immediately to the relevant Data Co-Ordinator and the Information Governance Manager using the

online personal data breach form. The Information Governance Manager can be approached for guidance.

All other information security incidents (phishing, compromised accounts, unusual activity, lost or stolen University devices), need to be reported via the IT Service Desk.

If a student identifies a personal data breach or security incident, they should immediately notify their school student support team, they may also submit an online data breach form. They should contact the IT Service Desk if they identify a potential security issue.

The person to whom the incident has been reported must take any necessary steps to contain and mitigate the incident and escalate appropriately,

Where appropriate, the Information Governance Manager and/or Information Security staff will engage with the relevant stakeholders and undertake an investigation of the incident to establish:

- The cause of the incident.
- The extent to which information may have been placed at risk.
- The potential damage that may have been caused to individuals and/or any reputational damage that may have been caused to the University as a result of the incident.

The Information Governance Manager will make a recommendation to the Academic Registrar and the University Data Protection Officer on whether the incident is categorised as high risk and requiring notification to the Information Commissioner's Office, within 72 hours of the University becoming aware of an incident. The University may also decide to contact other relevant authorities, for example the National Cyber Security Centre or the National Fraud and Cyber Crime Reporting Centre, where appropriate. An investigation and a decision on reporting an incident may run concurrently.

Following the investigation; the Information Governance Manager and Information Security staff will complete their documentation of the incident and make recommendations as to any further action that is required following the investigation. This should include:

-
- A recommendation on whether or not to inform data subjects of the incident and the corrective measures taken.
- A recommendation on any remedial action that should be taken to ensure that the circumstances are not repeated.

Following the review of an incident it may be necessary for further training to be undertaken by staff members from within those areas that are deemed to be at risk. Where there is evidence of wilful negligence or deliberate intent in the inappropriate release of information, it may be necessary to consider disciplinary action, as outlined in the Responsibilities of All Staff and Research Students Policy and the Acceptable Use Policy. Any such action would be taken in accordance with the procedures set out in the relevant Ordinances on discipline for staff and students.

www.lboro.ac.uk/governance/ordinances/35/current/ (staff)

www.lboro.ac.uk/governance/ordinances/17/current/ (students)

4. Monitoring of Information Security Incidents

All recorded information security incidents will be detailed for full consideration by the Information Governance Sub Committee (anonymised as far as possible). The Sub Committee will identify any recurring trends, incidents or areas of risk and will make recommendations for possible additions or amendments to the existing policies and/or training.

A report detailing all recorded information security incidents and recommendations for remedial actions will be submitted to the Infrastructure Committee periodically. An immediate report will be made should an incident of high concern arise. Any proposed changes to policies will be considered by the Infrastructure Committee and recommended to Senate and Council for approval.

5. Review of Information Security Policies

All Information Security policies, and the associated framework, will be reviewed on a regular basis by the Information Governance Sub-Committee, to ensure that they remain relevant, up to date and fit for purpose. Revisions to policies will be considered initially by the Infrastructure Committee as noted above.