Introduction

This information security policy document describes the expectations and principles relating to handling information. It is a sub-document of the Information Security Policy (ISP-S1).

This policy includes inventory, management and ownership of information; classification of information; disposal of information; removal of information; information on desks, screens and printers; stored data; backups; exchanges of information; information in application systems and handling payment card information.

Background

University staff and students and third parties associated with the University handling information/data on behalf of the University must comply with any “explicit agreements”, “legal compliance requirements” or “implicit expectations” when handling information.

The University endorses a culture of proactive risk management relating to information handling, to help reduce risks including: loss of data, unauthorised access, wasted resources, complaints and damage to reputation.

Policy outline

Departments should appropriately manage any security risks relating to handling all information for which it has responsibility.

Such Information may include data or information which is considered confidential, sensitive or has financial, reputational or research value, whether under Data Protection law or by virtue of the University’s Data Classification (as Highly Restricted or Restricted); personal data, including special category data, as defined by GDPR/Data Protection Act 2018; and information or data that is subject to a formal agreement with an external body that specifies secure handling requirements should be prioritised.

Information Asset Owners and Data Processors should:

- Identify information that must be protected and ensure that responsibility for doing so is assigned. This should be done systematically by departments, groups and individual members of staff as applicable.
- Ensure that those responsible for managing the security of information take into account confidentiality and value of the information they are managing when determining what security measures to use.
- Ensure that both the information owners and those responsible for handling that information, where different, have the same understanding of the security requirements, expectations and limitations.
- Ensure that those with responsibility for secure handling of information are offered training, guidance and support.
- Ensure that staff and students are generally aware of the need to take a responsible approach to handling information and provide them with guidance.
- Ensure that information is managed continuously until it is destroyed, or until that responsibility is transferred to another organisation.

Inventory, management and ownership of information

All Information Assets and Data Processing activities should be recorded on the University’s Information Asset Register which records all the Institutions Assets and Data Processing activities; supports the secure handling
Information Security Policy: Information Handling Policy

of information; compliance with GDPR/ Data Protection Act 2018; Information risk management and business continuity planning

Each department, office and group should review their Information Assets and Data Processing activities annually to keep the Information Asset Register up to date.

Each department, office, group and individual must ensure that they are aware of the items and classes of information they are responsible for handling.

The information asset list is a combination of specific information items, types of information, processes, computer systems, storage devices or locations where information is stored.

The information asset list should record useful information about each information asset identified including: Description or descriptive name. Location(s) of the information asset. Staff member with responsibility for handling the information or managing the information asset. The type(s) of information stored or processed. Origin or ownership of the information stored or processed. The importance of the information stored or processed. Any special or non-standard security measures required.

Information Assets should be reviewed and updated annually and new assets and data processing activities recorded when received.

A basic non-technical review of how the information involved is handled should be performed to minimise problems that may to a security incident.

**Information Asset Owners and Data Processors should:**

- Ensure that access rights to data (files, documents, web pages, etc.) are configured correctly.
- Ensure that files of personal and special category data (both physical and electronic) are stored securely and access is well controlled.
- Ensure that files of personal and special category data are retained in accordance with retention schedule requirements and are deleted when no longer in use.
- Ensure that physical hard copy documents are locked away out of sight when not in use.
- Ensure that security and access control records are maintained following staffing change events (such as a resignation or change in role of an individual).
- Ensure that data is owned and that ownership is transferred following staffing change events.

**Classification of information**

The University abides by its own Data Classification standards with 4 levels of data classification – Public, Unrestricted, Restricted and Highly Restricted: [https://www2.le.ac.uk/offices/ias/university-data-classification/university-data-classification-principles](https://www2.le.ac.uk/offices/ias/university-data-classification/university-data-classification-principles). Security standards such as ISO 27001 recommend that information should be classified and labelled according to its sensitivity. However; implementing a uniform information security classification system across the entire University is not practical. It is, however, recommended that confidential documents, folders, files, email messages etc. should be labelled accordingly. Whilst this in itself does not make the information secure it assists appropriate information handling. For example, it clearly indicates that such documents, or their contents, should not be distributed without due authorisation or consent from their owner.

Distribution of confidential or classified information must be controlled in accordance with authorisation.
Disposal of information

Sensitive paper documents must be disposed of by shredding using the confidential waste disposal service\(^1\).

Electronic data must be securely deleted when disposing of removable media or computing equipment containing hard drives. The central contract for IT equipment disposal must be used to ensure that this takes place\(^2\). Simple file deletion alone is inadequate for ensuring that files cannot be recovered and must not be relied on in and of itself.

Further information is available in the Software Management Policy (ISP-S13) and Mobile Computing Policy (ISP-S14).

Removal of information

Individuals must be authorised, by the Head of Department, to remove confidential or valuable University information offsite or to insecure locations. (It should be determined locally whether or not repeated authorisation is required by those undertaking a specific routine activity.)

Whether information should be removed, and if so whether any particular security measures are required, should be determined by assessing the risks that the removal may introduce. (Advice about Data Protection and general information security is offered by Information Assurance Services.)

Specific policy relating to taking personal information out of secure University locations on mobile computing devices is given in the Mobile Computing Policy (ISP-S14) and the Cryptography Policy (ISP-S16).

Information on desks, screens and printers

Staff responsible for handling confidential paper documents should take appropriate measures to avoid their unauthorised disclosure. Suitable procedures must be decided and employed based on the nature of the documents and assessment of the risks involved. This may involve locking the documents away when they are unattended. While confidential documents are being printed or copied, devices and documents must be either physically secure or else remain attended.

The possibility that confidential information displayed on computer screens may be viewed by those without authorisation must be avoided. This must be considered especially when siting devices on which confidential information is regularly displayed.

For further details about physical security in buildings see Building Security (ISP-I1).

Stored data

There are many types of data store, including filing cabinets and desks; files, books and documents; computers with internal disk drives; external disk drives including storage arrays; media such as DVDs and CDs; and flash drives.

The security of each University data store must be managed by a member of staff. Security management includes assessing and keeping under review risk levels associated with the data store. Where judged necessary and feasible risk mitigation measures should be implemented. Mitigation measures include storing information elsewhere that is more secure; improving the physical security of the location; backing up the data to another location; encrypting the data. These measures should be proportionate to the value of the

---

\(^1\) https://uniofleicester.sharepoint.com/sites/staff/waste-recycling/directory/SitePages/Home.aspx#title2

\(^2\) https://uniofleicester.sharepoint.com/sites/staff/waste-recycling/directory/SitePages/Home.aspx#title4?Mode%3DEdit&web=1

\(^3\) Page Information Security Policy: Information Handling Policy ISP-S7 April 2019
data – measured by the extent to which loss, corruption or disclosure of the data held could cause a significant negative impact on University business or reputation.

For further details see Managing Information Asset Security (ISP-I4)

**Backups**

Whilst “backups” are mostly associated with electronic information, this policy applies equally to information in other formats.

The member of staff with day-to-day responsibility for managing an information asset is by default responsible for ensuring that any necessary backup procedures are in place, adequate and tested. This may be the information owner or the manager of a system that stores or processes the information.

**Information Asset Owners and Data Processors should:**

- Make backups of information, such as data and software, where the possibility of losing the live, working or master copy of the information is unacceptable; or where not having backups is potentially more costly than making them; or where there is any doubt, backups should be taken. This should take into account the type and frequency of the backup, which should be appropriate to the medium.
- Ensure that the backed up data is stored appropriately and in resilient disk storage systems or secure locations.
- Clearly establish who is taking responsibility for backup arrangements, especially where data is used across teams.
- Ensure that staff or data processors responsible for archiving or making backups are aware of any University data retention policy relating to the type of data being handled.
- Ensuring that all owners of information held in the asset are aware of the backup arrangements. Where appropriate there should be liaison between the person responsible for managing backups and data owners with the aim of ensuring that the arrangements are suitable.
- Ensure that when potentially inadequate backup arrangements are identified owners are notified and actions taken.
- Ensure that backup media is securely disposed of, when no longer required, in a way that ensures that information will not be disclosed to unauthorised persons.
- Periodically test the recoverability of backed up data to ensure that the recovery procedure does not accidentally destroy more recent files.

**Exchanges of information**

The Data Protection Act 2018 requires that personal data is securely handled and imposes special conditions relating to transfer of personal data abroad. For further details see the Data Protection Code of Practice (University of Leicester publication) and the Freedom of Information Code of Practice (University of Leicester publication).

Any request for information about the University or about living individuals, which a member of staff would not normally handle as part of their job, should be referred to Information Assurance Services.

Exchanges of significant amounts of personal data or other confidential information with other organisations should be covered by suitable formal agreements. The security specification of the agreement should reflect any legal compliance requirements and the sensitivity of the information involved. It is the responsibility of the
Advice about drafting formal agreements for the exchange or transfer of data or information should be obtained from Procurement, Information Assurance Services and/or Legal Services. For further information see **Outsourcing and Third Party Access Policy (ISP-S4)**.

Non-disclosure agreements with other organisations must only be made with due regard for provisions of the Freedom of Information Act. Advice should be obtained from the Procurement, Information Assurance Services and Legal Services.

Where confidential information must be sent via the University internal post system it should be in a sealed and taped envelope and marked “personal and confidential” and “for addressee only”. For particularly sensitive information delivery by hand should be considered.

The limited security of email should always be taken into account when undertaking critical business activities. University email is not generally encrypted, although University devices and therefore access to University email accounts are. Important negotiations, agreements and transactions should be carried out, or supported by, traditional hand signed paper documentation. (This will be reviewed if facilities become available that support email that is encrypted, digitally signed and verified by a trusted Certificate Authority.)

Network transactions or connections between University computer systems and systems operated by other organisations should as far as possible utilise technology that assures confidentiality, authentication, nonrepudiation and integrity. (An assessment of the risk to the University should be undertaken when deciding whether to undertake electronic transactions that cannot be fully secured.)

Physical digital media in transit must be protected by security measures appropriate to the risks involved. For further information see **Mobile Computing Policy (ISP-S14)** and **Cryptography Policy (ISP-S16)**.

Information that may be associated with the University must not be distributed, published or otherwise made available unless it is legally compliant, appropriate and approved by management. (Inappropriate content includes material which is obscene, violent, illegal, damaging to the University or otherwise in breach of University policy.) For further information see **Compliance Policy (ISP-S3)** and **Guide to Information Legislation (ISP-I5)**.

Unsolicited email, faxes and other electronic messages should not be replied to, forwarded or acted upon until and unless the sender’s identity and authenticity of the message have been verified. For further policy relating to protecting against malicious code and inappropriate material sent via email and other forms of electronic messaging. For further information see **Use of Computers Policy (ISP-S9)**.

Members of the University must not disclose, modify, copy or disseminate to others any privileged information which may become available to them. Where they have been given access to information in error, they should advise the owner that the information may be inadequately protected or incorrectly distributed.

**Information in application systems**

Where information is being processed by an application system, quality controls should be used to help ensure its accuracy and integrity. Where applicable the following measures should be implemented:
• Ensure that a member of staff with responsibility and knowledge for ensuring secure operation of the application is nominated.
• Ensure correct levels of access to inputs, outputs and to administrative functions of the application system.
• Generate and review regularly transaction and processing reports to help identify integrity problems.
• Validate input and output data. For application systems, where the consequences of doing otherwise could be serious, input and output data should be validated to at least ensure it is of the correct type and within a reasonable range.

Handling payment card information
As a merchant processing payment card data the University is required to comply with the Payment Card Industry Data Security Standard (PCI DSS), a worldwide information security standard defined by the Payment Card Industry Security Standards Council. Enforcement of compliance is provided by the organisation’s card provider. Organisations that fail to meet the compliance requirement risk losing their ability to process credit card payments and being audited and/or fined. Further information is available in Payment Card Security (ISP-I10).