1. Introduction

1.1. This information security policy document contains high-level descriptions of expectations and principles relating to handling information. It is a sub-document of Information Security Policy (ISP-S1).

1.2. It is recognised that having a policy of endeavouring to adequately protect University information in all its forms is challenging. However, to have and pursue such a policy is the only responsible option. Advice on implementing secure management of electronic data is offered by IT Services. Estates can be consulted regarding physical security arrangements.

1.3. Definitions:

- Confidential information - information which if improperly disclosed or lost could cause harm or distress. This includes personal data, as defined by the Data Protection Act, and other valuable or sensitive information not in the public domain.

1.4. This document includes statements on:

- 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
- Handling payment card information

2. Background

2.1. Groups and individuals belonging to the University must comply with any “explicit agreements”, “legal compliance requirements” or “implicit expectations” when handling information.

2.2. In addition to needing to meet legal compliance requirements, it is beneficial to the University to achieve and maintain good standards of information handling. 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.

3. Policy outline
3.1. Secure handling of the following types of information is a priority:

- Information which is considered confidential or valuable for any reason by its owner or the University.
- Personal data as defined by the Data Protection Act.
- Information or data that is subject to a formal agreement with an external body that specifies secure handling requirements.

3.2. The University intends that the security risks, relating to handling all information for which it has responsibility, are to be appropriately managed. Pursuing this policy requires that University staff and management:

- 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 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 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. (The interpretation of “responsible approach” here depends on circumstances such as the type of information being handled and reasonable expectations.)
- Ensure that information is managed continuously until it is destroyed, or until that responsibility is transferred to another organisation.

4. Inventory, management and ownership of information

4.1. Maintaining and reviewing an information inventory supports:

- Secure handling of information
- Compliance with the Data Protection Act
- Information risk management
- Business continuity planning

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

4.3. It is recommended that each department, office and group establishes and maintains, for example by annual review, a list of important information assets held. This list should cover not only their own information but also information held that belongs to others.

4.4. An information asset list can be any combination of specific information items, types of information, processes, computer systems, storage devices or locations where information is stored. The most suitable approach should be determined locally; however, enumerating every document held is unlikely to be necessary or practical.
4.5. 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.

4.6. Periodically reviewing and updating the list of important information assets is recommended. Performing at least a basic non-technical review of how the information involved is handled may help to identify one of these common problems that can lead to a security incident:

- Expectations differing between the information owner(s) and staff responsible for handling the information. Examples:
  - The information owner incorrectly assumes their data is being regularly backed up.
  - The information owner incorrectly thinks someone else is looking after the security configuration of the system where it is stored.
  - Staff handling documents do not realise they should be locked away out of sight when not in use.
- No current member of staff is taking responsibility for the asset or information held. Examples:
  - The security of an operational computer system is no longer being adequately maintained as a result of a staff change.
  - Computer storage media or documents are abandoned.
- The handling requirements appropriate for the information in question are unknown therefore suitability of the measures in place is in doubt. Example:
  - A file of sensitive personal information is found stored in an insecure area.
- Scope of access to confidential data is not being controlled appropriately. Example:
  - Access to files or web pages has not been checked since being accidentally misconfigured.
- The information is not in a location with adequately managed physical security. Example:
  - Access to the room is insufficiently well controlled or supervised.
- Continuing to store the information has become an unnecessary risk.
  - Personal data stored unnecessarily.
5. **Classification of information**

5.1. 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.

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

6. **Disposal of information**

6.1. Sensitive paper documents must be disposed of by shredding. (The University uses the services of a company providing secure on-site shredding.)

6.2. Electronic data must be securely deleted, e.g. when disposing of removable media or computing equipment containing hard drives. Either a suitably effective in-house procedure may be used, or another organisation may undertake the work provided that they are subject to a contractual agreement stipulating secure data handling and deletion. (Note that simple file deletion is often inadequate for ensuring that files cannot be recovered. Staff needing to ensure that confidential data has been deleted are advised to seek assistance from their departmental Computer Officer or IT Services.)

6.3. Policy relating to secure disposal of information also features in:

   - Software Management Policy (ISP-S13)
   - Mobile Computing Policy (ISP-S14)

7. **Removal of information**

7.1. 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.)

7.2. 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.)

7.3. Specific policy relating to taking personal information out of secure University locations on mobile computing devices is given in:

   - Mobile Computing Policy (ISP-S14)
   - Cryptography Policy (ISP-S16)

8. **Information on desks, screens and printers**

8.1. 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.

8.2. 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.

8.3. Further details about physical security in buildings:
- Building Security (ISP-I1)

9. Stored data

9.1. Data stores are valuable if loss, corruption or disclosure of the data held could cause a significant negative impact on University business or reputation. 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
- Flash drives

9.2. The security of each valuable 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. Typical mitigation measures include:
- Store information elsewhere that is more secure
- Improve physical security of the location
- Backup the data to another location
- Encrypt the data

9.3. This document has additional advice about assessing and managing risks to information assets:
- Managing Information Asset Security (ISP-I4)

10. Backups

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

10.2. University business must not be exposed to undue and unnecessary risk as a result of inadequate backup arrangements. Depending on the type of data involved and how frequently it changes:
- Have arrangement to ensure regular backup
- Run sufficiently frequent backups
- Store backup data remote from the original data
- Periodically test recovery from backups
• Store backup data on resilient disk storage systems

10.3. Backups of information, such as data and software, must be made where the possibility of losing the live, working or master copy of the information is unacceptable. In other cases where not having backups is potentially more costly than making them, or where there is any doubt, backups should be taken.

10.4. 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.

10.5. Where aspects of administering an information asset, e.g. a computer system, are shared between different individuals or groups it must be clearly established who is taking responsibility for backup arrangements.

10.6. Staff responsible for archiving or making backups should make themselves aware of any University data retention policy relating to the type of data being handled.

10.7. The staff member responsible for an information asset is also responsible for 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.

10.8. Staff identifying potentially inadequate backup arrangements, for information which the University has responsibility, must inform their line manager.

10.9. Backup media must be securely disposed of, when no longer required, in a way that ensures that information will not be disclosed to unauthorised persons.

10.10. The type and frequency of data backup should be appropriate.

10.11. Recoverability of backed up data should be periodically tested (ensuring that the recovery procedure does not accidentally destroy more recent files).

11. Exchanges of information

11.1. 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. For further details refer also to:

• Data Protection Code of Practice (University of Leicester publication)
• Freedom of Information Code of Practice (University of Leicester publication)

11.2. The Data Protection Act requires that personal data is securely handled and imposes special conditions relating to transfer of personal data abroad. Advice is available from Data Protection staff in Information Assurance Services. For further details refer also to:

• Data Protection Code of Practice (University of Leicester publication)

11.3. 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 head of the department involved to ensure that the agreement is drawn up, signed and filed within the department.
Advice about drafting formal agreements is offered by the Purchasing Office and Information Assurance Services. See also:

- **Outsourcing and Third Party Access Policy (ISP-S4)**

11.4. Non-disclosure agreements with other organisations must only be made with due regard for provisions of the Freedom of Information Act. Advice about how to do this is offered by the Purchasing Office and Information Assurance Services.

11.5. 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.

11.6. The limited security of email should always be taken into account when undertaking critical business activities. 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.)

11.7. 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.)

11.8. Physical digital media in transit must be protected by security measures appropriate to the risks involved. For further information refer to:

- **Mobile Computing Policy (ISP-S14)**
- **Cryptography Policy (ISP-S16)**

11.9. 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 related information see:

- **Compliance Policy (ISP-S3)**
- **Guide to Information Legislation (ISP-I5)**

11.10. 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 see also:

- **Use of Computers Policy (ISP-S9)**

11.11. 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.

**12. Information in application systems**
12.1. 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.

13. Handling payment card information

13.1. 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 done 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. Refer to policy sub-document:

- Payment Card Security (ISP-I10)

---

**Failure to comply with University Policy may lead to disciplinary action.**

---

**Document history:**

<table>
<thead>
<tr>
<th>Date</th>
<th>Action Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>13 March 2009</td>
<td>Began first draft.</td>
</tr>
<tr>
<td>22 April 2009</td>
<td>In relation to “network transactions”, revised the text to say “should where possible” rather than “must” as suggested by D. Garton. In relation to “email exchanges”, “must” was also changed to “should”.</td>
</tr>
<tr>
<td>3 July 2009</td>
<td>Minor change.</td>
</tr>
<tr>
<td>21 July 2009</td>
<td>Changes recommended by the Steering Group and other minor changes.</td>
</tr>
<tr>
<td>26 Feb 2010</td>
<td>Added a paragraph to the introduction. Statements on use of encryption and digital signing of email and other electronic transactions reworded.</td>
</tr>
<tr>
<td>16 August 2010</td>
<td>ISP-I4 is renamed “Managing Information Asset Security”.</td>
</tr>
</tbody>
</table>
The official version of this document will be maintained on-line. Before referring to any printed copies please ensure that they are up-to-date.