# Policy Overview

<table>
<thead>
<tr>
<th>Title:</th>
<th>Information Security Policy Overview</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status:</td>
<td>Approved</td>
</tr>
</tbody>
</table>

## 1. Introduction

Information and information systems are vital to the business and operation of the University. Incidents involving loss of confidentiality, integrity or availability of information can be costly. Serious incidents, which may include failure to comply with information legislation, can also be damaging to the reputation of the University.

The objective of University Information Security Policy is to ensure that all information and information systems, on which the University depends, are adequately protected. Achieving this largely depends on staff and students working diligently in accordance with policy guidelines.

University Information Security Policy sets out requirements and recommendations, relating to how:

- Confidential information must be protected from unauthorised access.
- The integrity of information and information systems must be protected.
- Appropriate measures must be taken to manage risks to the availability of information.
- The University must ensure compliance with laws and the terms of contracts.

---

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

## 2. Policy Overview

The full policy is set out in a suite of documents. Staff members are urged to consult the policy documents. To provide an overview, the strategic policy document names are listed here with some of the key points:

### Information Security Policy (ISP-S1) [Approved]:

- The purpose, scope, and structure of the security policy documentation in detail.
- University committee responsibility for information security policy.
- University Information Security Policy applies to all staff and students.
- Heads of Department are responsible for applying the University Information Security Policy to their departmental information systems.

### Information Asset Protection Policy (ISP-S2) [Approved]:

- Implementing departmental business continuity planning and risk management is the responsibility of the Head of Department. The essential business continuity planning and risk management requirements are defined by the University Governance and Planning section.

### Compliance Policy (ISP-S3) [Approved]:

- It is the responsibility of each individual to ensure that they do not break the law.
- Staff must not cause a breach of the terms of contracts between the University and other organisations.
- Information is provided to help students and staff to avoid breaking UK information laws though lack of awareness.
Students, staff and others that may use any University information system, or handle University information, must be explicitly informed and confirm acceptance of University policy relating to institutional IT system usage monitoring and access to computer accounts.


Outsourcing and Third Party Access (ISP-S4) [Approved]:

- Outsourced IT arrangements, which are not the subject of a formal University contract, should not normally be used or depended upon for working with confidential information or for processing the personal data of third parties.
- Any access to University information systems provided to external organisations must be correctly risk-managed and where appropriate covered by a formal agreement.
- A risk assessment should be made and appropriate controls used (such as supervision), where external parties (such as contractors), are given physical access to areas where confidential information is stored or processed.

Personnel Policy (ISP-S5) [Approved]:

- Staff must agree to abide by the information security policies as a condition of using any University information systems or handling University data.
- Personnel management procedures must be implemented to help ensure that the recruitment, management and departure of staff do not harm information security.

Operations Policy (ISP-S6) [Approved]:

- Staff must keep the doors and windows of unattended offices locked. Outside normal building opening hours building entrances, office doors and windows must be kept locked when unattended.
- Where responsibility for managing physical access controls, such as door keys or access cards, is devolved to departments then it is the responsibility of the Head of Department to ensure that a proper system to manage them is in place.
- The procedures for the operation and administration of the University’s key information systems must be documented.
- Staff involved in administering, developing, testing and commissioning key systems, must follow appropriate change management procedures.
- Security incidents and software faults must be reported.

Information Handling Policy (ISP-S7) [Approved]:

- Groups and individuals belonging to the University must comply with any “explicit agreements”, “legal compliance requirements” or “implicit expectations” when handling information.
- Responsibility for managing information assets must be assigned.
- Appropriate information backup arrangements must be implemented.
- Individuals must be authorised by their Head of Department to remove confidential or valuable University information offsite or to insecure locations and appropriate security measures must be taken.
- Confidential paper documents must be disposed of by shredding.
- Electronic data must be securely deleted, e.g. when disposing of removable media or computing equipment containing hard drives. (Simple file deletion is often inadequate for ensuring that files cannot be recovered.)

User Management Policy (ISP-S8) [Approved]:

- Staff and Students must agree to abide by the information security policies as a condition of using any University information systems or handling University data.
Access to University IT resources must be authorised and a record maintained of such authorisations.

All University IT resource users must be identifiable.

Computer user’s access to computer resources must be controlled and revised by system managers when circumstances change to ensure that security risks are minimised whilst allowing the Universities business interests to be carried out without undue hindrance.

Use of Computers Policy (ISP-S9) [Approved]:

Any device connected to a network, managed or provided by the University, and deemed by IT Services not to meet currently required hardware, software and configuration standards or connected without authorisation is liable to physical or logical disconnection from the network without notice.

It is unacceptable to use University IT facilities for any of the following:
  o Any illegal activity.
  o Creation or transmission, or causing the transmission, of any offensive, obscene or indecent images, data or other material, or any data capable of being resolved into obscene or indecent images or material.
  o Creation or transmission of material with the intent to cause annoyance, inconvenience or needlessly anxiety.
  o Creation or transmission of material with the intent to defraud.
  o Creation or transmission of defamatory material.
  o Creation or transmission of material such that this infringes the copyright of another person.
  o Creation or transmission of unsolicited bulk or marketing material to users of networked facilities or services, save where that material is embedded within, or is otherwise part of, a service to which the user or their User Organisation has chosen to subscribe.
  o Deliberate unauthorised access to networked facilities or services.
  o Using communal or “open access” computing facilities for recreational or other non-University work when there are others waiting to use the resource (this may include simultaneously using more than one end user device).
  o Deliberate activities having, with reasonable likelihood, any of the following characteristics:
    ▪ Wasting staff effort or networked resources, including time on end systems and the effort of staff involved in the support of those systems.
    ▪ Corrupting or destroying other users’ data.
    ▪ Violating the privacy of other users.
    ▪ Disrupting the work of other users.
    ▪ Denying service to other users (for example, by deliberate or reckless overloading of access links or of switching equipment).
    ▪ Continuing to use an item of networking software or hardware after IT Services has formally requested that use cease or be suspended.
    ▪ Misuse of networked resources, such as the introduction of "viruses" or other harmful software.

Where a computer account is provided for exclusive use by an individual:
  o The account holder should be instructed not to reveal the password or otherwise permit anyone else to use the account.
  o The account must not be used by anyone except the account holder.

Cases of unacceptable use of IT facilities may be investigated by authorised staff. The findings will be reported as appropriate to the relevant Head of Department or the Registrar.

University IT system managers must wherever technically possible enforce appropriate password related policies.

University business must not be exposed to undue and unnecessary risk as a result of inadequate computer data backup arrangements. The information owner or custodian is responsible for checking, or seeking assurance, that the backup arrangements for the computer facility or service being used are suitable.
Computer system managers are responsible for ensuring that backup arrangements published, or agreed with users of the system, are reliably implemented and that users are informed promptly should there be any problems with, or changes to, the backup arrangements.

**System Planning Policy (ISP-S10) [Approved]:**

- Planning and deployment of information systems and upgrades must incorporate assessment and adequate mitigation of the associated information security risks.
- Computer systems must be planned to ensure that adequate physical security, processing power, storage and network capacity are available for current and projected needs, all with appropriate levels or resilience and fault tolerance. Arrangements for correct maintenance of equipment must be established.

**System Management Policy (ISP-S11) [Approved]:**

- System management policy applies to all staff that use administrator privileges on any University multi-user computer or software application service.
- System managers have a key role to play in ensuring confidentiality, integrity and availability of University information and information systems. They are responsible for endeavouring to ensure correct and secure operation of computers in accordance with both University level policies and any relevant departmental policies.
- Computer system managers are required to be aware of University information security policies in general. System Management Policy (ISP-S11) and the other policy documents that it refers to are of particular relevance for system managers.

**Network Management Policy (ISP-S12) [Approved]:**

- Devices must not be permitted to continue exposing a serious network security vulnerability to the campus network or Internet if there is no imminent prospect of that vulnerability being removed (whether that be by source code level support, an active program of security patching or firewiring).
- All computer systems providing important University services must be fully supported. That support may be provided by an external supplier or local service provider; however, it must include ongoing remediation of any security vulnerability discovered.
- All network devices should be maintained so as to be up to date with security patches for both the operating system and any software applications installed.
- Where applicable, network devices should have current and automatically updated anti-virus software installed.
- Where applicable, network devices should have correctly configured firewall software installed. As a default all ports should be closed unless specifically opened. Services exposed to the network and the scope of exposure for each service should be the minimum possible.
- Where there is a risk to the network security, quality of service for network users, or in order to enforce University policy, IT Services is authorised to:
  - Impose restrictions on network traffic or use of network applications.
  - Refuse connection of devices to the network.
  - Remove networked devices or sub-sections of the network from service.
  - Manage network resource allocation (such as bandwidth).
- Ownership of network devices
  - Devices owned by the University or its recognised partner organisations, such as the Student’s Union and University Hospitals, may be connected to the wired network.
  - Privately owned devices may only be connected to the wired network in special circumstances approved by the Head of Department. (In such cases approval to connect the device must also be obtained from a Network Authority or Authoriser in the usual way - see below.)
  - Privately or University owned laptops/PCs may be connected to the wireless network.
- Administration of network devices
Every networked device must be associated with an identifiable and contactable person responsible for its administration. Devices for which the administrator cannot be identified or contacted are liable to be removed from the network.

Users of privately owned network devices are, and will be assumed by IT Services to be, responsible for ensuring that their devices are configured, actively maintained and used in accordance with University policies.

**Authorisation to connect a network device**

- Approval must be obtained from a Network Authority or Authoriser before connecting a device to the wired network. The request for connection may only be made by a member of staff. (The unauthorised connection of laptops, PCs or other devices to the University wired computer network is forbidden for security reasons.)
- CFS service users and approved visitors are authorised to access the wireless network service.
- Visitors to the University may be granted temporary wireless access to the network by a member of staff with a CFS account.

**Controlling access to and from other networks**

- IT Services is responsible for controlling the network gateway between the University of Leicester networks and the Internet.
- Exposure of network services to incoming connections from the Internet is not permitted without prior agreement from IT Services.

Software Management Policy (ISP-S13) [Approved]:

- Software is to be patched as soon as possible to remove security vulnerabilities.
- Use of software which tests or attempts to break University system or network security is prohibited unless the Director of IT Services has been notified and given authorisation.
- Software found on University systems which incorporates malware of any type is liable to automated or manual removal or deactivation.
- Software that is not licence compliant must be brought into compliance promptly or uninstalled.
- Software that is known to be causing a serious security problem, which cannot be adequately mitigated, should be removed from service.
- Operating systems and application software must not be abandoned or otherwise left unmaintained for extended periods.
- The Director of IT Services has responsibility for IT at the University and on behalf of the University is permitted to regulate or prohibit use of particular software or types of software for the overall benefit of the University.
- Heads of Department may implement additional specific local policies relating to IT management, which may include further restrictions affecting software.

Mobile Computing Policy (ISP-S14) [Approved]:

- Individuals must be authorised by the Head of Department to remove or send confidential information outside a secure University location. Depending on the specific nature and quantity of the data it may also be necessary to encrypt it.
- The University does not require staff or students to store or access confidential information using computing devices that it does not own or manage. Should the University require one of its members to use a mobile computing device to store or access confidential data, then a suitably configured University owned device must be provided.
- Staff and students are strongly advised not to store or access any confidential information from computing devices which are not owned or managed by the University.
- Staff and students should not permit others to use a University owned mobile computing device, for which they have current responsibility, especially where doing so may put any confidential information at risk of loss or disclosure.
- Where a mobile computing device is to be used to handle data provided to the University by an external body or vice versa, it must be capable of meeting any specific security requirements demanded by that external body.
• Departmental procedures must ensure that data is removed as appropriate before mobile computing equipment is reassigned to another person.
• Data must be securely deleted when disposing of mobile computing equipment.
• Normally, advice and support for approved devices and software may be requested from departmental computing staff or IT Services.
• Unencrypted confidential information must not be transmitted via a network where traffic may be subject to snooping or interception. Unless there is reason to believe otherwise assume this is the case for any network. Where it is uncertain that encrypted network protocols are in use from source to destination then encryption of data files before sending them is recommended.

Teleworking Policy (ISP-S15) [Approved]:

• Teleworkers are likely to require greater access to data and systems than mobile workers so represent a greater security risk.
• Staff who will be doing part or all of their work using dedicated equipment in a fixed location outside the University must be authorised to do so.
• The location, equipment used and procedures for maintenance and backup of teleworking systems must be approved and must not present a significant risk to information security.

Cryptography Policy (ISP-S16) [Approved]:

• Loss, theft, or unauthorised disclosure of certain information could be detrimental to the University, its staff or students. Such information includes that defined as personal data by the Data Protection Act 1998. Where the University is handling digital personal data that cannot be sufficiently secured by physical controls, the data must be encrypted.
• Data which must be handled securely, using encryption where pertinent, includes:
  o Any personal data classed as “sensitive” by the Data Protection Act.
  o Any data, that is not in the public domain, about a significant number of identifiable individuals.
  o Personal data in any quantity where its protection is justified because of the nature of the individuals, source of the information, or extent of the information.
• Data as described above must be encrypted:
  o Where it is stored on a computing device or any computer storage medium which may be exposed to a significant risk of being lost or stolen. Any such device when outside a secure University location is considered to be at significant risk, including home computers.
  o Where it is to be transmitted via a computer network using a mechanism that does not itself incorporate encryption. Depending on the specific technology being used this could refer to: sending data by email either within or outside the University, transferring files offsite, remotely accessing files or Web pages. The risk is that unencrypted data in transit may be intercepted.
  o Where the data is being sent using a postal service such that the data media could be lost, stolen or intercepted and read whilst in transit.
• Where data being handled by the University is subject to an agreement with an external organisation specifying use of encryption, the agreed handling procedures, encryption technologies and standards must be used.
• Where personal data is to be encrypted and no overriding requirements (from an external body) apply, the recommended minimum University encryption standards (or better) must be applied. For further details refer to the “Cryptography implementation” section.
• Individuals must be authorised by the Head of Department before taking or sending confidential information out of a secure University location.
• University Web transactions that involve the transfer of sensitive data or funds must use encryption, for example, Hypertext Transfer Protocol over Secure Socket Layer or Transport Security Layer (HTTPS).

ResNet Acceptable Use Policy (ISP-S17) [Approved]:
University students using the halls of residence networks are required to comply with the terms and conditions of the network service provider.

**Document history:**

<table>
<thead>
<tr>
<th>Date</th>
<th>Month</th>
<th>Year</th>
<th>(C. Nelson)</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>02 December</td>
<td>2009</td>
<td></td>
<td>First draft.</td>
<td></td>
</tr>
<tr>
<td>28 January</td>
<td>2010</td>
<td></td>
<td></td>
<td>Revised to reflect changes in policy documents.</td>
</tr>
<tr>
<td>26 February</td>
<td>2010</td>
<td></td>
<td></td>
<td>Revised to show status of individual policy documents.</td>
</tr>
<tr>
<td>26 July</td>
<td>2010</td>
<td></td>
<td></td>
<td>Reworded the outline of Business Continuity and Risk Management Policy (ISP-S2).</td>
</tr>
<tr>
<td>16 August</td>
<td>2010</td>
<td></td>
<td></td>
<td>ISP-S2 is renamed “Information Asset Protection Policy”.</td>
</tr>
<tr>
<td>02 November</td>
<td>2010</td>
<td></td>
<td></td>
<td>Updated approval status of documents.</td>
</tr>
<tr>
<td>18 May</td>
<td>2011</td>
<td></td>
<td></td>
<td>Revisions resulting from review within IT Services.</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.