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 firewalling).
• 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:
  o Impose restrictions on network traffic or use of network applications.
  o Refuse connection of devices to the network.
  o Remove networked devices or sub-sections of the network from service.
  o Manage network resource allocation (such as bandwidth).
• Ownership of network devices
  o 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.
  o 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.)
  o 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]:

6 / 7
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>Action Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>02</td>
<td>December</td>
<td>2009</td>
<td>(C. Nelson) First draft.</td>
</tr>
<tr>
<td>28</td>
<td>January</td>
<td>2010</td>
<td>(C. Nelson) Revised to reflect changes in policy documents.</td>
</tr>
<tr>
<td>26</td>
<td>February</td>
<td>2010</td>
<td>(C. Nelson) Revised to show status of individual policy documents.</td>
</tr>
<tr>
<td>26</td>
<td>July</td>
<td>2010</td>
<td>(C. Nelson) Reworded the outline of Business Continuity and Risk Management Policy (ISP-S2).</td>
</tr>
<tr>
<td>16</td>
<td>August</td>
<td>2010</td>
<td>(C. Nelson) ISP-S2 is renamed “Information Asset Protection Policy”.</td>
</tr>
<tr>
<td>02</td>
<td>November</td>
<td>2010</td>
<td>(C. Nelson) Updated approval status of documents.</td>
</tr>
<tr>
<td>18</td>
<td>May</td>
<td>2011</td>
<td>(C. Nelson) 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.
1. Introduction

1.1. The University relies on computer systems and, to a lesser extent, manual procedures for handling and processing the information supporting many of its activities. Information that the University manages shall be appropriately secured to protect against consequences of breaches of confidentiality, failures of integrity, interruption to availability and failure to comply with legal requirements. (The University must comply with relevant statutory or other overriding requirements affecting information security, whether or not they are explicitly stated within its policies.)

1.2. This is the top-level document, in a hierarchically structured set of documents, specifying information security policy for the University of Leicester (hereafter referred to as the University). This document includes:

- The purpose, scope, and structure of the security policy documentation.
- Responsibility for information security policy documentation.
- Developing and maintaining the policy document set.
- Implementing information security policies.
- Responsibilities for implementing information security policies.
- References to related documents.

2. Purpose of University information security policy documentation

2.1. Maintaining effective University information security policy documentation provides a sound basis for regulating how systems and procedures are designed, configured and operated. Regulation is necessary to ensure that information is adequately secured against adverse affects on availability, integrity, confidentiality or compliance.

2.2. University policy documentation should perform these functions:

- Present a comprehensive and coherent approach to information security at a strategic level.
- Reflect the intentions of the University e.g. by defining expected standards.
- Facilitate on-going development, scrutiny and revision of policies at strategic and tactical levels.
- Provide guidance or direction to users, administrators and developers of University information systems.
- Describe an ideal model, against which reality can be compared, to identify areas where policy is not being implemented well and policies that need to be revised.

3. Scope

3.1. The policies in this documentation set apply to all information systems:
- Owned by the University.
- Being used for University business.
- Connected to networks managed by the University.

3.2. The policies in this documentation set apply to all information:
- The University is handling whether or not it is owned by the University.
- Including software owned or licensed by the University.

3.3. The policies in this documentation set apply to all people:
- Managing or using any system identified in 3.1 above.
- Responsible to the University and handling information identified in 3.2 above.

4. Structure of the policy documentation set

4.1. The structure and content of this policy documentation set is based on an approach set out in the "UCISA Information Security Toolkit". The Toolkit is intended to help academic institutions to formulate and maintain policy documents, and is based on the control guidelines contained in the industry standard framework BS7799 (ISO27001).

4.2. This top-level document references a set of policy sub-documents all of which have equal standing, which state official University policy in various areas. These policy sub-documents will be referred to as "Strategic Policy" documents.

4.3. Each strategic policy document should only contain high-level descriptions of expectations and principles: they are to be deliberately free from practical details of policy implementation and regulations.

4.4. Where necessary, details expanding on how statements in the strategic policy documents are to be implemented should be described in "Policy Implementation" documents. These policy implementation documents are below the strategic policy documents in the documentation hierarchy.

4.5. Explicit regulations, typically in the form of simple dos and don'ts, shall be derived from either strategy or implementation level documents. These regulations will be grouped together in "University Regulations" documents according to whom they apply, rather than according to the area of information security they relate to. (These documents sit below the implementation documents in the hierarchy). This approach is intended to facilitate "delivery" of all relevant regulations to the correct target audience in a succinct form.

4.6. Statements in strategic, implementation and regulation documents must fully reference each other. This must be done to ensure that:
- Any available implementation details or regulations related to a strategic policy statement can easily be found.
- The strategic context of all implementation details can be identified.
- The implementation details (if there are any) and strategic context of every regulation can be traced.
4.7. Diagram summarising the policy documentation system structure:

5. Responsibility for information security policy documentation

5.1. The Information Communications Technology Committee (ICTC) has ultimate responsibility for approving updates and additions to the University information security policy documentation set. (This process will distinguish current official University policy documents from any other legacy or unofficial accounts of policy).

5.2. The policy documentation set will be reviewed at least annually; however, urgent requests for updates will be processed as quickly as possible.

5.3. Proposed changes and additions to the policy documentation may be submitted by any member of staff, via a Head of Department, ultimately for consideration by the ICTC.

5.4. Proposed updates to policy must be fully converted into proposed changes to the policy documentation. This must be done in such a way that implications for all related documents are fully taken into account. An update will only be considered approved when each resulting new or modified document has been approved.

6. Developing and maintaining the policy document set

6.1. The policy document set must be maintained as a whole to keep it internally self-consistent and also to maintain a uniform style.

6.2. Duplicated content and ambiguity should be removed.

6.3. The documentation set should be extended and revised over time to ensure that it remains comprehensive and current.

6.4. The documentation should be kept free from superfluous detail to make it easy to read and maintain.

6.5. To facilitate managing the documentation, the status, version history and approval history must be maintained for each document.

6.6. Document updates pending approval must be easily distinguishable e.g. by using different colour text.
7. Implementing information security policies

7.1. Measures will be taken by the University to implement information security policies including:

- Establishing a continuous "Plan-Do-Check-Act" cycle of activities which ensure that suitable practices are documented, reinforced and improved with time. (Documentary evidence of the processes and procedures involved will be required to demonstrate implementation of policy to external parties.)

- Ensuring that all individuals who use information systems, or otherwise handle information, understand the policies that are relevant to them and any consequences for non-compliance. In cases of policy violation deemed to be serious, wilful or repeated the University will not hesitate to take disciplinary action.

- Using physical security measures where deemed necessary.

- Applying technology where considered appropriate and feasible. For example, to control and log access to systems, data and functionality.

- Using various lawful forms of monitoring activities, data and network traffic to detect policy infringements.

- Taking into account relevant information security policy requirements when planning and undertaking activities involving IT-based information systems.

- Formal or informal risk assessment, to identify the probability and impact that various hazards could have on information systems.

- Monitoring effectiveness of its information security policy implementation. This may involve review independent from those charged with its implementation.

8. Responsibilities for implementing information security policies

8.1. It is the responsibility of the University to sufficiently resource and direct implementation of its information security policies.

8.2. Responsibility for applying University information security policy to Departmental or Divisional information systems is delegated by the University to the Heads of Department or Division respectively. Heads are responsible for any further delegation of functions relating to policy enforcement.

8.3. Individuals must understand and agree to abide by University policies before being authorised for access to any information systems for which the University has responsibility.
9. References to strategic level policy sub-documents

<table>
<thead>
<tr>
<th>Name</th>
<th>ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information Asset Protection Policy</td>
<td>ISP-S2</td>
</tr>
<tr>
<td>Compliance Policy</td>
<td>ISP-S3</td>
</tr>
<tr>
<td>Outsourcing and Third Party Access Policy</td>
<td>ISP-S4</td>
</tr>
<tr>
<td>Personnel Policy</td>
<td>ISP-S5</td>
</tr>
<tr>
<td>Operations Policy for IT Service Providers</td>
<td>ISP-S6</td>
</tr>
<tr>
<td>Information Handling Policy</td>
<td>ISP-S7</td>
</tr>
<tr>
<td>User Management Policy</td>
<td>ISP-S8</td>
</tr>
<tr>
<td>Use of Computers Policy</td>
<td>ISP-S9</td>
</tr>
<tr>
<td>System Planning Policy</td>
<td>ISP-S10</td>
</tr>
<tr>
<td>System Management Policy</td>
<td>ISP-S11</td>
</tr>
<tr>
<td>Network Management Policy</td>
<td>ISP-S12</td>
</tr>
<tr>
<td>Software Management Policy</td>
<td>ISP-S13</td>
</tr>
<tr>
<td>Mobile Computing Policy</td>
<td>ISP-S14</td>
</tr>
<tr>
<td>Teleworking Policy</td>
<td>ISP-S15</td>
</tr>
<tr>
<td>Cryptography Policy</td>
<td>ISP-S16</td>
</tr>
<tr>
<td>ResNet Acceptable Use Policy</td>
<td>ISP-S17</td>
</tr>
</tbody>
</table>

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

Document history:

7 March 2007 (C. Nelson)  Began first draft.
24 May 2007 (C. Nelson)  Table of policy sub-documents added.
5 June 2007  Approved.
16 August 2010 (C. Nelson)  ISP-S2 is renamed “Information Asset Protection Policy”.
18 May 2011 (C. Nelson)  Revisions resulting from review within IT Services.

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.
1. Introduction

1.1. This information security policy document describes expectations and principles for protecting the security of University information assets. This is a sub-document of Information Security Policy (ISP-S1).

1.2. The term “information asset” is used below to refer to a useful or valuable:
   - Store of information in any format
   - Information processing system of any type
   - Facility used to transfer information

1.3. This document includes statements on:
   - University strategic risk management and business continuity planning
   - Departmental business continuity plans
   - Departmental local strategic risk registers
   - Operational level protection of information assets

2. University strategic risk management and business continuity planning

2.1. The University seeks to exercise effective control against the possibility that a specific event or set of circumstances will adversely affect the achievement of its strategic objectives in the medium and longer term. Implementing controls appropriately to protect security of the information assets, on which University business processes depend, is consistent with this aim. See also:

   - University of Leicester Risk Management Policy

2.2. The University has developed procedures for strategic risk management and business continuity planning that must be implemented across the University. Implementation of this strategic departmental risk management and business continuity planning is the responsibility of departmental and divisional heads. The overall project is administered by the Governance Section within the Division of Student and Academic Services.

2.3. These strategic risk management and business continuity planning processes have an important role to play in supporting information security, as outlined in the next two sections.

3. Departmental business continuity plans

3.1. At the departmental level, the University’s procedures require development of business continuity plans covering processes defined as “critical”.

3.2. Departmental information assets, such as computers or information stores, which need to be replaced or restored to service within 72 hours of failing or becoming
unavailable, would be considered to represent a “critical risk”. Inclusion of these in the departmental business continuity plan is required.

3.3. For further information refer to the University of Leicester business continuity planning procedures (contact the Governance Section).

4. Departmental local strategic risk registers

4.1. At the departmental level, the University requires local strategic risk registers to be established.

4.2. It is appropriate that significant information security risks, such as risks to important information assets, should be given visibility and monitored using this risk register.

4.3. Departmental local strategic risk registers should be maintained in accordance with the University of Leicester strategic risk management procedures (contact the Governance Section).

5. Operational level protection of information assets

5.1. Departmental senior management will generally be aware of any strategic level risks affecting the locally managed information assets on which their business processes depend. Where these risks are significant they will be recorded in the departmental risk register and monitored. Where an information asset represents a critical risk, it will also be featured in the departmental business continuity plan.

5.2. At the day-to-day level, operational managers and other staff must take an active role in identifying risks to University information assets within their areas and in protecting them where that can reasonably be expected.

5.3. This operational level protection of information assets should involve:
   - Recognition and assessment of risks, including new risks
   - Acceptance or assignment of responsibility for managing risks where practical
   - Upward reporting of significant risks which are not, or cannot, be managed
   - Upward reporting of new strategic risks, whether or not they are being managed
   - Undertaking, where appropriate, suitable prevention or remediation measures

5.4. Protecting information assets against damage or disruption must be undertaken with due consideration of:
   - The value and importance of the asset
   - The types and levels of risks to which the asset is exposed
   - The likely effectiveness of any protection measures
   - The cost of protection measures

5.5. A simple systematic approach can be helpful in assessing how well an IT or non-IT based information asset is protected from a range of common threats. Should such an approach be used and result in the identification of any significant risks to the work of the department, then those risks must be reported for potential inclusion in the departmental risk register. Information Assurance Services offers to provide further details about how to use the approach that is outlined in this document:
   - Managing Information Asset Security (ISP-I4)
Document history:

3 July 2009 (C. Nelson) Minor changes.
13 July 2009 (C. Nelson) Updated the information about business continuity.
18 August 2009 (C. Nelson) Reviewed and approved by Phil Simpkin, also minor changes made as suggested.
16 August 2010 (C. Nelson) ISP-I4 is renamed “Managing Information Asset Security”.
08 October 2010 (C. Nelson) Approved, with minor changes, by Neil Cox. Approved by Phil Simpkin.
02 November 2010 (C. Nelson) Approved by the Steering Group.
18 May 2011 (C. Nelson) Revisions resulting from review within IT Services.

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.
1. Introduction

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

1.2. This document includes statements on:
   - Compliance with legal requirements.
   - Compliance with other external regulatory requirements.
   - Compliance with the University's own information security standards.
   - Collection of evidence contained within information systems.
   - Records management.

2. Compliance with legal requirements

2.1. The University makes policy statements and provides explanatory information about legal compliance matters with the intention of helping its members to ensure their legal obligations are not breached through a lack of awareness. (University of Leicester information security policy documentation relating to the law is provided for informational purposes as distinct from being professional legal advice.)

2.2. It is ultimately the responsibility of each individual to ensure that they do not break the law. Students, staff and others managing or using any University information system or handling University information are not exempt from statutory obligations.

2.3. All those who have access to on-line services through the University's network are responsible for making themselves aware of the possible legal consequences attached to the use of those services.

2.4. Where a serious unlawful act involving the University is suspected, the Registrar must be informed.

2.5. Legislation imposes numerous obligations that apply to handling of University information and use of University information systems. The University must endeavour to comply with all relevant statutory requirements whether or not those requirements are explicitly stated within its internal policy documentation.

2.6. Items of legislation that are particularly relevant to individuals that use or are responsible for University information systems are summarised with further information about legal compliance measures, in policy sub-document:
   - Guide to Information Legislation (ISP-I5)

3. Compliance with the JANET Policies

3.1. "JANET" (Joint Academic NETwork) is the name given both to an electronic communications network and a collection of electronic communications networking
services and facilities that support the requirements of the UK higher and further education and research community. The University of Leicester uses JANET services and in doing so is required to comply with "JANET Acceptable Use Policy" and “JANET Security Policy”. These policies are available from the JANET website.

3.2. It is intended that University of Leicester information security policies support compliance with JANET Acceptable Use and Security Policies.

4. Payment Card Industry Data Security Standard (PCI DSS) compliance

4.1. 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)

5. Software Licence Management and Compliance

5.1. The University must endeavour to comply with software and data licensing agreements that it has entered into. It must be able to demonstrate a diligent approach to software licence management and be in a position, if necessary, to prove its claims with regard to software licences.

5.2. At the time that a software license agreement is being entered into the practicalities that compliance with that agreement would entail must be fully understood and considered. Where necessary an agreement must be explicitly negotiated with suppliers as to mutually acceptable compliance procedures or controls.

5.3. Software for official University business is obtained and deployed by departmental staff. It is ultimately the responsibility of Heads of Department to ensure that an appropriate departmental software licence management procedure is defined and in operation. It is the responsibility of staff that purchase or deploy software to be aware of and follow the correct departmental procedures.

5.4. By default the University applies principles expressed in the "CHEST (Combined Higher Education Software Team) Code of Conduct on the Use of Software and Datasets" (which may be found on the Eduserv website). Since the principles are generally relevant they are applied whether or not the software is provided through CHEST; however, they are superseded or supplemented by specific licensing terms for individual software products.

5.5. The specifics from each individual software product licence must be complied with and may supersede or supplement the principles in the CHEST code. All applications have externally defined licenses, including software provided under the "campus" and "select" schemes.

6. Compliance with the University's own information security standards

6.1. In addition to legal obligations and other external regulatory requirements, information security policy documents also set out some of the University’s own internally defined policies. The University must endeavour to ensure that is within its legal rights when operating its internal policies.

6.2. Members of the University should note that it is possible for an individual to breach Regulations, or to discredit or harm the University, without a criminal
offence having been committed. In cases deemed to be serious and wilful the University will not hesitate to take disciplinary action.

6.3. Before being authorised to access any University information systems or data Students, staff and others that may use any University information system, or handle University information, must:

- Be provided with an opportunity to review the information security policies.
- Be explicitly informed about the policies relating to institutional IT system usage monitoring and access to computer accounts.
- Confirm that they understand and consent to abide by the policies.

6.4. Policy sub-document:

- Institutional IT Usage Monitoring and Access (ISP-I6)

7. Collection of evidence contained within information systems

7.1. Where it is necessary to collect evidence from an information system to pursue or defend against a possible legal action, the evidence shall be collected and presented to conform to the relevant rules of evidence. Special consideration must be given to how the authenticity and accuracy of the information can be established therefore expert guidance should be sought before proceeding.

7.2. Where a suspected criminal offence, involving an information system, has been referred to the police, their instructions must be followed relating to identifying, seizing and preserving any digital evidence.

8. Records management

8.1. The University Records Management policy (which is scheduled to be written by August 2011) will refer to the minimum and maximum retention periods that apply to different categories of information held in documents and electronic records. The policy will take into account business and legal requirements and gives consideration to how stored information should be safeguarded whilst remaining accessible to those with authorisation. (Appendix 6 of the University of Leicester document "Data Protection Code of Practice (A guide to the Data Protection Act 1998)" currently gives some guidance about retention periods relating to personal data.)

8.2. The recommended approach to records management is contained in the University of Leicester document "Records Management Code of Practice (A guide to Records Management)".

---

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

---

Document history:

15 October 2007 (C. Nelson) Began first draft.

28 August 2008 (C. Nelson) Refer to JANET AUP v10 and JANET Security Policy.

5 December 2008 (C. Nelson) Revised following feedback from the Steering Group.

13 February 2009 (C. Nelson) 2.4 / 2.5 merged and modified.

3 July 2009 (C. Nelson) Minor changes.

26 January 2010 (C. Nelson) Simplified statement 2.4 to avoid confusion about incident reporting as identified in “Security of Research Data” audit report of January 2010.


18 May 2011 (C. Nelson) Revisions resulting from review within IT Services.

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.
1. Introduction

1.1. This information security policy document sets out principles and expectations about maintaining the security of University IT facilities that are accessed, or provided by third parties. It is a sub-document of Information Security Policy (ISP-S1).

1.2. Definitions:
- Third parties – external organisations, or individuals other than the University’s own staff or students.
- 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.

1.3. This document includes statements on:
- Formally provided, and informally available, IT facilities and services
- Managing outsourcing and third party access risks
- Contractual issues
- Third party support, maintenance and development
- Guest access by third parties
- Physical access by external parties to sensitive areas

2. Formally provided, and informally available, IT facilities and services

2.1. Formally provided University IT facilities and services are those:
- Either provided directly by University departments and managed by University staff
- Or provided to the University by third parties and subject either to formal bilateral agreement or clear understandings setting out standards and expectations which cover information security.

2.2. Informally available IT facilities (informal outsourcing):
- Staff and students are able to access and use a range of IT facilities on the Internet which are provided by third parties with which the University does not have any formal agreement or established understanding. Users signing up to use these facilities are typically required to accept the terms and conditions of a unilateral agreement entirely determined by the provider.
- Examples of informal IT outsourcing include:
- Using Google Docs for University business (*with no formal bilateral agreement*).
- Using MSN Hotmail or Google Mail for University business (*with no formal bilateral agreement*).
- Forwarding University business email from a University email account to MSN Hotmail or Google Mail (*with no formal bilateral agreement*).

- In the absence of any control by or accountability to the University, a number of possible security risks are associated with entrusting information to these facilities. The potential risks include a lack of knowledge and control over:
  - Who may have access to user data
  - How user data is used
  - Where user data is stored
  - How securely user data is stored
  - How reliable and available the facility will be in the short term
  - How viable the facility will be in the long term
  - How the facility may change in terms of user interface or nature of service
  - Whether user data will be recovered in the event of a disaster
  - How much support will be provided in the event of a problem

- Use of informally outsourced IT arrangements to process personal data may range from being inadvisable to breaching aspects of the Data Protection Act.

- Given the risks above, such facilities must not be used, or depended upon, for working with confidential University information or for processing the personal data of third parties.

- Staff who demonstrate informally outsourced IT facilities must not promote or approve their use for handling confidential information (and preferably should also warn against such use).

- Staff must not configure their University email accounts to automatically forward incoming email to services that are not operated by the University, unless such an arrangement has been formally approved by the Director of IT Services and is subject to an appropriate bilateral contract.

### 3. Managing outsourcing and third party access risks

3.1. Staff of sufficient seniority must be involved in, and take responsibility for, ensuring that risks are identified and managed where University IT systems are to be accessed, or provided, by third party individuals or organisations. The purpose is to protect the interests of the University, its members and to ensure legal compliance.

3.2. A risk assessment must be used to help decide whether a formal agreement with the third party is needed and if so what it should include. (See also “contractual issues” below.)

3.3. The risk assessment, which in some cases may conclude that an activity cannot safely proceed, must include:
General analysis of the proposed arrangement in terms of any new or increased information security risks. In particular, consideration of what University information will become accessible to the third party organisation. In doing so potential legal compliance risks are to be identified, e.g. relating to Data Protection legislation.

Determination of whether the third party is already subject to an agreement with the University e.g. is providing a service that has been purchased subject to standard University terms and conditions.

An assessment of the potential impact on University business that could result from the third party suffering or causing a problem i.e. understand potential risk impact in terms of scope and severity.

An assessment of how trustworthy and competent the third party is in relation to undertaking the proposed arrangement or activity.

4. Contractual issues

4.1. Where it is determined that a formal agreement is to be made with a third party in relation to accessing or providing University IT facilities, the following issues must be addressed:

- The third party must agree to follow University information security policies. The information security policies, or a summary, must be formally provided to any such third party prior to their being granted access.
- Where relevant, third parties should be asked to provide a copy of their information security policies. Enquiries should be made in writing relating to any concerns arising.
- All orders/contracts for the provision of services should be issued on the basis that the University’s standard terms and conditions of contract shall apply. These include standard clauses on confidentiality and data protection. Where an agreement is being negotiated separately then these two standard clauses should be included in that agreement. Where this is not possible then advice should be sought from Information Assurance Services prior to any agreement being concluded.
- Any specific arrangements that may be required by the University in relation to assuring information security must be negotiated and included in the agreement. For example, any specific responsibilities, security controls, monitoring or reporting that may be required.
- The potential effects of termination of the agreement, or its transfer/assignment to another organisation, must be considered and controlled if possible. Matters relating to ongoing security of University information in the event of contract termination should be taken into account. If there is to be a handover of a service between two third parties, there should not be a period when neither or both parties may be considered to have responsibility for, or control of, the service.
- Where appropriate binding service level agreements should be negotiated that specify the performance to be delivered and the remedies in case of non-compliance.
- It is highly advisable to agree the details of liability clauses up front.
5. Guest access by third parties

5.1. Where third parties are involved in providing support and maintenance of University IT facilities it may be necessary for them to access systems using the highest levels of privilege. It is essential in that:

- Such privileged access by third parties to, or via, the University network is in all cases approved by and where necessary facilitated by IT Services.
- A member of University staff is responsible for managing the access provided in terms of scope, level and duration. It is also recommended that third party access is monitored or logged.
- Privileged remote access arrangements must only be permitted via secure encrypted network protocols. See also Cryptography Policy (ISP-S16).
- The third party has provided the University with the code of practice that their staff and agents must follow in handling customer’s information. The code of practice provided by the third party has been reviewed, is acceptable and the University has assurance in writing that the code will be followed. It is preferable that this forms part of the agreement with the third party for provision of the service.

5.2. Where third parties are to be involved in the provision of bespoke University information systems or software it is essential that:

- The third party can provide credible assurances of security quality controls or standards in relation to their applications development process.
- Use of the application as an element of the University’s production systems is not permitted if it is known to have serious security vulnerability. See also Software Management Policy (ISP-S13).

5.3. Changes, by a third party organisation to a University information system, must be subject to the same change management procedure that would apply if those changes were being made by University staff.

6. Third party support, maintenance and development

6.1. University members must not permit information security safeguards and policies to be bypassed, or allow inappropriate levels of access to University information or IT facilities to other members or any third parties such as guests, customers, collaborators, suppliers, consultants or contractors. See also Use of Computers Policy (ISP-S9).

6.2. Any access to University information systems provided to third parties must follow established recognised procedures. For example procedures are currently available for providing guests and conference delegates with temporary central service user accounts or wireless Internet access. See also User Management Policy (ISP-S8).

7. Physical access by external parties to sensitive areas

7.1. A risk assessment must be made and appropriate controls established before external parties, such as contractors, are given access to normally secure areas where confidential information is stored or processed. This is likely to apply particularly to computer machine rooms and certain offices. The potential risks include:

- Disclosure or theft of confidential information
- Theft or tampering with equipment
- Accidental damage to equipment
Misuse of facilities

The outcome of the risk assessment may be to deny access, simply grant access or provide access whilst taking steps to manage the risks. For example, access may need to be supervised, or it may be that sensitive information or equipment is first removed or given additional protection. See also Building Security (ISP-I1).

<table>
<thead>
<tr>
<th>Date</th>
<th>Action Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>24 April 2009</td>
<td>Began first draft.</td>
</tr>
<tr>
<td>15 July 2009</td>
<td>Minor changes advised by the Steering Group.</td>
</tr>
<tr>
<td>08 October 2009</td>
<td>Added a statement about staff auto forwarding email outside the University.</td>
</tr>
<tr>
<td>02 July 2010</td>
<td>Revised wording to better distinguish what is required from what is recommended best practice, as advised by the Steering Group.</td>
</tr>
<tr>
<td>17 August 2010</td>
<td>Approved by Richard Thomas following a change to the “contractual issues” section.</td>
</tr>
<tr>
<td>02 November 2010</td>
<td>Approved by the Steering Group.</td>
</tr>
<tr>
<td>18 May 2011</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.
1. Introduction

1.1. This information security policy document contains high-level descriptions of personnel processes that must be implemented to ensure that employees are both able and required to protect the University's information security. It is a sub-document of Information Security Policy (ISP-S1).

1.2. This document includes statements on:

- Recruitment, references and screening
- Employment contract terms
- Information security education and training
- Staff termination, suspension or change of employing department
- IT usage monitoring and access
- Disciplinary process
- External parties

2. Recruitment, references and screening

2.1. For roles involving handling of confidential information or access to sensitive information systems, Human Resources may use a pre-employment screening process to help ensure that staff selected are suited to the demands of the job.

3. Employment contract terms

3.1. Staff are to sign a formal undertaking that includes:

- Awareness that in cases of University policy violation deemed to be serious, wilful or repeated the University may take disciplinary action.
- A confidentiality or non-disclosure agreement to protect University information both during and after their employment with the University.
- Agreement to comply with the University Information Security policies.
- Agreement to undertake mandatory training courses in information compliance and security as and when required by the University.
- Understanding that, except in special circumstances, those staff granted University email addresses will be contactable via those addresses. (The University requires and so assumes that staff will regularly monitor email sent to their central service email address ensuring receipt of communications relating to University business.)

4. Information security education and training
4.1. The University is committed to providing staff with sufficient training to ensure that they are able to perform their specific information security responsibilities. Training requirements to support information security are to be reviewed during the staff appraisal process.

4.2. Information system users are to be provided with sufficient instruction or training to ensure they do not compromise security through lack of awareness or skill.

5. Staff termination, suspension or change of employing department

5.1. Upon termination, suspension or change of employing department, Human Resources will revise the staff records system accordingly. (This is intended to trigger appropriate account management processes on centrally managed IT systems.)

5.2. Upon termination, all employees, contractors and third parties must return all information assets and equipment held which belongs to the University.

6. IT usage monitoring and access

6.1. The Director of Human Resources may request that legally compliant monitoring of staff e-mail be undertaken for legitimate University purposes. Policy and procedure relating to how the University may monitor usage of its IT systems (including University Mobile Phones) and the circumstances in which it may access user information on its systems and networks that is normally private is given in:

- Institutional IT Usage Monitoring and Access (ISP-I6)

7. Disciplinary process

7.1. Employees who, after an investigation, have been found to have breached security or violated policy in a serious, wilful or repeated way, may be subject to disciplinary action.

7.2. Unless the police are involved from the outset, when different procedures may apply, IT Services will coordinate investigation of any suspected improper use of University IT facilities. Human Resources will coordinate any resultant disciplinary action.

7.3. Where there are reasonable grounds for suspecting misuse of a computer account, that account may be suspended by the system manager, in consultation with Human Resources, pending further investigation.

8. External parties

8.1. Precautions, in the form of formal agreements, should be taken to protect the information security interests of the University where external organisations or individuals are:

- Employed to work on University information systems.
- Provided with or given access to confidential information.

8.2. The necessary precautions relating to external parties are described in:

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

---

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

---
Document history:

07 December 2009 (C. Nelson) Began first draft.

06 July 2010 (C. Nelson) As advised by the Steering Group:
- Removed a proposal to incorporate specific responsibilities for information security into job descriptions.
- Removed “when on leave or” from “Understanding that, except when on leave or in special circumstances, staff will be contactable via their central IT service email address.”
- Removed “in particular validity of references should be checked.”

30 September 2010 (C. Nelson) Revisions prompted by input from HR including:
- Provide for optional use of staff security screening by HR.
- Only require those staff with central IT service email addresses to be contactable via those addresses.
- Withdrawal of access rights may be requested by HR to departments managing information services.
- Added reference to IT usage monitoring and access.

05 October 2010 (C. Nelson) Reworked section 5 to clarify that HR are not expected to know details of staff accounts or their permissions on IT systems across the University.

06 October 2010 (C. Nelson) Changes by Alun Reynolds incorporated.

02 November 2010 (C. Nelson) Approved by the Steering Group.

18 May 2011 (C. Nelson) Revisions resulting from review within IT Services.

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.
1. Introduction

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

1.2. This document includes statements on:

- Physical security
- Insurance
- Critical information assets
- Operational procedures, controls and responsibilities
- Reporting Information Security Incidents
- Reporting Software Faults

2. Physical security

2.1. Physical threats to information security include:

- Environmental threats - temperature, humidity, fires, floods, storms
- Supply system threats - disruption to energy supply, communications
- Manmade threats - unauthorised access, tampering, theft, wilful damage, accidents

2.2. The physical security of University information systems must be managed appropriately, taking into account their importance to the business operations of the University and the types and quantities of information they hold.

2.3. Physical security arrangements must be considered when new information systems are being planned and arrangements must be reviewed if circumstances change.

2.4. An assessment of the physical threats and vulnerabilities affecting important information systems must be undertaken. Where necessary specialist advice should be obtained to support this assessment. The cost of possible countermeasures to physical security threats must be taken into consideration. Countermeasures should be implemented where deemed appropriate, effective and justified.

2.5. Taking into account any countermeasures to be implemented, a decision must be made by management about how to handle any physical risks that may remain. The options are: consider further countermeasures, accept the residual risk or transfer the risk.

2.6. See also:

- Managing Information Asset Security (ISP-I4)
2.7. New building security measures and changes to existing measures must be agreed and operated with collaboration between the department responsible for the information system and Estates (Estates and Facilities Management Division).

2.8. When building or maintenance work is to take place, the risks that the work may present to any information systems must be assessed and managed. Risks must be managed with collaboration between the department responsible for the information system and Estates.

2.9. See also:
   - Building Security (ISP-I1)

3. Insurance

3.1. The risk of loss or destruction of University owned computers or data should be offset by appropriate levels of insurance cover. (Clearly whilst this can help to offset the cost of replacing lost computer hardware, it will not help to recover lost information that has not been backed up securely elsewhere.)

3.2. The University property insurance policy does not cover laptops and smartphones. (In particular, note that University smartphones managed by IT Services are not supplied with any insurance cover.)

3.3. Estates Insurance Services Office offer advice about insurance and can arrange specific insurance for items not covered by the University property insurance policy. For example cover for University mobile computing hardware, including laptops and smartphones, can be arranged.

3.4. To activate cover for other computer and peripheral devices that are not taken offsite, such as desktop PCs and printers, departments must ensure that the items are on the departmental insurance schedule. The schedule is to be revised and returned to Estates Insurance Services Office annually.

3.5. Estates Insurance Services Office must also be specifically notified of each additional high value item or where there are significant changes in computing hardware. A web form for doing this is available on the University Insurance Website:
   - http://www.le.ac.uk/estates/customer_care__office_support/insurance/computer/index.html

4. Critical information assets

4.1. At the departmental level, University Governance and Planning requires development of business continuity plans covering business processes defined as “critical”. Departmental information assets, such as computers or information stores, which need to be replaced or restored to service within 72 hours of failing or becoming unavailable, would be considered to represent a “critical risk”. Inclusion of these in the departmental business continuity plan is required. For further information refer to the University of Leicester business continuity planning procedures (contact University Governance and Planning).

5. Operational procedures, controls and responsibilities

5.1. The procedures for the operation and administration of the University’s key information systems must be documented, and those procedures and documents regularly reviewed and maintained.

5.2. Staff involved in administering, developing, testing and commissioning systems, must follow appropriate change management procedures.
5.3. When reviewing key systems and procedures, explicit consideration should be given to whether segregating duties and areas of responsibility would help to reduce the risk of information security incidents and be feasible.

6. Reporting Information Security Incidents

6.1. Procedures will be established and widely communicated for reporting security incidents and suspected security weaknesses in the University’s business operations and information processing systems. Mechanisms shall be in place to monitor and learn from those incidents.

6.2. See policy sub-document:
   - Reporting Information Security Incidents (ISP-I3)

7. Reporting Software Faults

7.1. Procedures will be established for reporting software malfunctions and faults in the University’s information processing systems. Faults and malfunctions shall be logged and monitored and timely corrective action taken.

7.2. See policy sub-document:
   - Reporting Software Faults (ISP-I2)

---

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

---

Document history:

<table>
<thead>
<tr>
<th>Date</th>
<th>Month</th>
<th>Year</th>
<th>Author</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>23 March</td>
<td></td>
<td>2007</td>
<td>(C. Nelson)</td>
<td>Began first draft.</td>
</tr>
<tr>
<td>3</td>
<td>July</td>
<td>2009</td>
<td>(C. Nelson)</td>
<td>Minor change.</td>
</tr>
<tr>
<td>16 July</td>
<td></td>
<td>2009</td>
<td>(C. Nelson)</td>
<td>Title changed as agreed by the Steering Committee and a minor addition suggested by Prof. Hillman.</td>
</tr>
<tr>
<td>06 July</td>
<td></td>
<td>2010</td>
<td>(C. Nelson)</td>
<td>As advised by the Steering Group, removed “for which it is necessary to accept some residual risk” from “It is recommended that key systems, for which it is necessary to accept some residual risk, are given consideration in a business continuity plan.”</td>
</tr>
<tr>
<td>16 August</td>
<td></td>
<td>2010</td>
<td>(C. Nelson)</td>
<td>ISP-I4 is renamed “Managing Information Asset Security”.</td>
</tr>
<tr>
<td>Date</td>
<td>Author</td>
<td>Details</td>
<td></td>
<td></td>
</tr>
<tr>
<td>---------------</td>
<td>--------------</td>
<td>-------------------------------------------------------------------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>22 September</td>
<td>(C. Nelson)</td>
<td>Liz Gordon recommended stressing that University mobile phones provided through IT Services are not automatically insured.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>13 October</td>
<td>(C. Nelson)</td>
<td>Incorporated changes to the section about insurance as recommended by David Masters.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>02 November</td>
<td>(C. Nelson)</td>
<td>Approved by the Steering Group.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>18 May</td>
<td>(C. Nelson)</td>
<td>Revisions resulting from review within IT Services.</td>
<td></td>
<td></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.
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
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 Officer 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)

<table>
<thead>
<tr>
<th>Document history:</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>13 March 2009</strong> (C. Nelson) Began first draft.</td>
</tr>
<tr>
<td><strong>22 April 2009</strong> (C. Nelson) 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><strong>3 July 2009</strong> (C. Nelson) Minor change.</td>
</tr>
<tr>
<td><strong>21 July 2009</strong> (C. Nelson) Changes recommended by the Steering Group and other minor changes.</td>
</tr>
<tr>
<td><strong>26 Feb 2010</strong> (C. Nelson) 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><strong>16 August 2010</strong> (C. Nelson) ISP-I4 is renamed “Managing Information Asset Security”.</td>
</tr>
</tbody>
</table>

Failure to comply with University Policy may lead to disciplinary action.
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.
1. Introduction

1.1. This information security policy document contains high-level descriptions of expectations and principles relating to how computer and application user accounts and privileges should be managed. This is a sub-document of Information Security Policy (ISP-S1).

1.1. User accounts and privileges must be managed correctly to ensure authorised user access to information systems is possible whilst preventing unauthorised access.

1.2. This document includes statements on:

- Scope
- Authorisation to manage user accounts and privileges
- Eligibility for accounts to use University IT facilities
- Management of user accounts and privileges
- Password management

2. Scope

2.1. Login accounts and privileges must be managed in accordance with this policy for all computer systems and software applications used for University business or connected to University networks.

3. Authorisation to manage user accounts and privileges

3.1. Management of accounts and privileges on University computers and applications is to be restricted to authorised and suitably trained members of staff. Authorisation may be given, through line management, by the head of the department responsible for the management of the computer or application concerned.

3.2. Connection of privately owned computers to the wired network is only permitted in special circumstances with approval beforehand by both the Head of Department and a Network Authoriser. A condition of connecting a device to the wired network is that IT Services will be permitted to inspect its configuration. Where connection is permitted the designated system administrator of the device is responsible for ensuring that configuration and usage is in accordance with University Information Security Policy. This includes the management and usage of all login accounts and privileges on the device.

3.3. Specific staff are authorised to control login accounts and permissions for systems that IT Services manages. IT Services may delegate specific limited responsibilities for managing accounts and permissions to staff in other departments.

3.4. See also:

- Network Management Policy (ISP-S12)

4. Eligibility for accounts to use University IT facilities
4.1. Use of login accounts and privileges on University IT facilities, including permission to use University networks, may be authorised only for:

- Current University staff and students
- Students awaiting graduation
- Emeritus staff and those holding recognised honorary positions
- Those working closely with University staff on approved research or administrative projects.
- Staff in other organisations with which the University has a relevant formal agreement, e.g. for provision of computer system support.
- Visitors to the University, who may be granted temporary wireless access to the network by a member of staff with a CFS account

5. Management of user accounts and privileges

5.1. Those with responsibility for creating user accounts on University IT facilities must ensure that accounts are only created for individuals who are eligible to have an account and whose identity has been validated.

5.2. Before being provided with accounts, all users must be informed that compliance with University information security policy is a condition of using any University information system or handling University data.

5.3. Access to University IT resources must be authorised and a record maintained of such authorisations. For any computer, application or network account, it must be possible to determine:

- The identity of the person responsible for the account i.e. the user, or primary user in the case of shared accounts.
- The identity of the person responsible for managing the account and configuring its privileges. (This would typically be the administrator of the system, application or service to which the account provides access.)

5.4. Provision of privileged access to other organisations must be authorised by management and is subject to special controls. For further details see:

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

5.5. Computer user’s access to computer resources must be controlled and revised by system managers when circumstances change. This is to ensure that security risks are minimised and to allow University business to be carried out without undue hindrance. Specifically:

- Users’ access rights must be adjusted in a timely manner to provide only that access which is authorised and necessary. This should take place whenever there is a change in business need, staff change their role, or staff or students leave the University.
- The purpose and membership of all privileged groups and roles should be periodically reviewed.
- A periodic general review of login accounts should lead to removal of access to those accounts which are no longer eligible or required.
5.6. Management of user privileges should wherever possible be based on group membership or role assignment, rather than by individual account. Except for systems or applications with a simple and self-documenting access control model, the purpose of each user group or role should be clearly defined and documented.

5.7. “Privileged accounts” are those with special computer system privileges that are needed by system administrators and which ordinary users do not need to use. System administrators must:

- Not provide ordinary users with privileges which could jeopardise the security of any other system users or their data.
- Not use privileged accounts themselves except when undertaking specific system administration tasks that require such privileges, i.e. they must use a normal account at other times.

5.8. See also “Accounts” section in:

- Use of Computers Policy (ISP-S9)

6. Password management

6.1. Once access to a system or application is authorised, the user is to be informed of their temporary password in a secure way. This temporary password must be changed immediately; this should be enforced automatically by the system where possible.

6.2. See also “Passwords” section in:

- Use of Computers Policy (ISP-S9)

---

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

---

**Document history:**

<table>
<thead>
<tr>
<th>Date</th>
<th>Action</th>
<th>Author</th>
</tr>
</thead>
<tbody>
<tr>
<td>01 September 2008</td>
<td>Began first draft.</td>
<td></td>
</tr>
<tr>
<td>07 July 2010</td>
<td>On advice from Steering Group, added “Students awaiting graduation” to those eligible to use University IT facilities.</td>
<td>C. Nelson</td>
</tr>
<tr>
<td>18 May 2011</td>
<td>Revisions resulting from review within IT Services.</td>
<td>C. Nelson</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.
1. Introduction

1.1. This information security policy document contains high-level description of the responsibilities and required behaviour of users of University IT systems, including University networks. It is a sub-document of Information Security Policy (ISP-S1).

1.2. This document includes statements on:

- Departmental policies and procedures
- Connecting devices to University networks
- Use of University IT facilities for private work
- Unacceptable use of University IT facilities
- Accounts
- Passwords
- Unattended user equipment
- Protecting against unknown or malicious code
- Use of email facilities
- Backups

2. Departmental policies and procedures

2.1. Where necessary Heads of Department may specify and implement policies relating to use of IT systems for which they have responsibility, provided that any such policies are consistent with University wide policy and do not have a negative impact elsewhere. Such policies may, for example, include specific rules relating to use of software, managing provision of network services, user behaviour etc.

3. Connecting devices to University networks

3.1. IT Services is responsible for managing, either directly or through an agent, connections to University networks that have connectivity with the Internet. (IT Services may delegate responsibility for authorising connection to its networks to trusted staff in other departments.)

3.2. Minimum required hardware, software and configuration standards for securing devices attached to University networks are determined by IT Services and set out in policy. (IT Services may also publish other more specific requirements.)

REQUIRED HARDWARE, SOFTWARE AND CONFIGURATION STANDARDS

For details refer to: "Hardware and software requirements" in
- Network Management Policy (ISP-S12)
3.3. Devices must not be connected to a network, managed or provided by the University, unless the device meets current required hardware, software and configuration standards (see above) and its connection is authorised.

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

3.5. It is the responsibility of the department operating any devices that have fallen below required standards (see above) to take prompt remedial action.

4. Use of University IT facilities for private work

4.1. University IT facilities are provided principally for official academic and administrative purposes. Occasional personal use is, however, permitted so long as:

- It is not in breach of any University policies.
- It is not excessive, in volume, frequency or time.
- It does not disrupt or restrict usage by other users.

4.2. Staff wishing to embark on any significant use of University IT facilities for work which is not part of their official University duties, such as consultancy or private work, must only do so after notifying their Head of Department and in accordance with guidelines issued by Personnel Services.

5. Unacceptable use of University IT facilities

5.1. 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. (In cases of policy violation deemed to be serious, wilful or repeated the University will not hesitate to take disciplinary action.)

5.2. The list of unacceptable uses of IT facilities below is applicable to all University IT systems. It is consistent with JANET acceptable use policy and legal compliance requirements. See also Compliance Policy (ISP-S3).

5.3. It is unacceptable to use University IT facilities for any of the following:

- Any illegal activity.
- 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.
- Creation or transmission of material with the intent to cause annoyance, inconvenience or needless anxiety.
- Creation or transmission of material with the intent to defraud.
- Creation or transmission of defamatory material.
- Creation or transmission of material such that this infringes the copyright of another person.
- 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.
Deliberate unauthorised access to networked facilities or services.

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).

Deliberate activities having, with reasonable likelihood, any of the following characteristics:

i. Wasting staff effort or networked resources, including time on end systems and the effort of staff involved in the support of those systems.

ii. Corrupting or destroying other users' data.

iii. Violating the privacy of other users.

iv. Disrupting the work of other users.

v. Denying service to other users (for example, by deliberate or reckless overloading of access links or of switching equipment).

vi. Continuing to use an item of networking software or hardware after IT Services has formally requested that use cease or be suspended.

vii. Misuse of networked resources, such as the introduction of "viruses" or other harmful software.

5.4. Where a network managed or provided by the University is being used to access another network, any breach of the acceptable use policy of that network will be regarded as unacceptable use.

5.5. Without prior explicit approval, the University's computing services must not be used for placing or distributing advertisements other than those promoting the activities or trading operations of the University or the Student’s Union. Where a proposed promotion may feature direct marketing, on behalf of a third party organisation, Information Assurance Services should be consulted. (All advertisements should be 'legal, decent, honest and truthful' and comply with the British Code of Advertising, Sales Promotion and Direct Marketing issued by the Advertising Standards Authority.)

5.6. University members must not permit information security safeguards and policies to be bypassed, or allow inappropriate levels of access to University information or IT facilities to other members or any third parties such as guests, customers, collaborators, suppliers, consultants or contractors. See also:

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

6. Accounts

6.1. Where a computer account is provided for exclusive use by an individual:

- The account holder should be instructed not to reveal the password or otherwise permit anyone else to use the account.

- The account must not be used by anyone except the account holder.

6.2. Where use of a shared account is necessary to facilitate a specific activity:

- The purpose of the shared account must be clearly understood and the account must be used only for the purpose specified.
• Usage of, and access to, the shared account must be carefully managed. Every shared account must have an “owner” responsible for managing access to the account and supervising its use.

• The owner of a shared account must maintain a current record of which individuals have access.

• When an individual having access to a shared account leaves, or no longer requires access to the account, then the account owner must change the password and securely inform those continuing to require access.

6.3. “Privileged accounts” are those granting special computer system privileges that ordinary users do not need to use. (In addition to special accounts such as e.g. “root” under UNIX or “administrator” under Windows, privileged accounts can be ordinary user accounts that have extra permissions resulting from being added to user groups such as “power users” or “administrators”.)

• These accounts should only be used to undertake specific system administration tasks and should not be used for routine work, where a normal account has sufficient privileges.

• Wherever possible local system administration tasks on departmental user devices should be undertaken by professional departmental or central computing staff in accordance with University and departmental policies. In particular use of privileged accounts should be controlled and periodically reviewed to implement the principle of least privilege.

• Where a privileged account potentially permits access to information belonging to others, effective line management control over who has access to it and the way it is used must be maintained. (This applies to any system that holds or provides access to data belonging to more than one user.)

• Where a computer user also acts as the local system administrator, and so uses a privileged account on their local system, they are required to manage and use the system in accordance with all University and departmental policies.

6.4. Wherever possible both centrally and departmentally provided computing accounts should be managed such that:

• Preferably, computing activities undertaken using a particular account can be associated with a specific individual.

• Alternatively, an identified individual takes active responsibility for the management and activities of users of a particular computing facility or account.

6.5. Students are not permitted to log into more than one University provided computer simultaneously unless special arrangements have been made. (This may otherwise be considered unfair use of resources by an individual or an indication that an account is being shared in breach of University policy.)

7. **Passwords**

7.1. University IT system managers must wherever technically possible enforce appropriate password related policies. Specific recommendations about configuring password strength, account lockout, password expiry and other password access control parameters on University computer accounts are given in policy implementation document:
7.2. Using mechanisms that allow automatic login into a computer account (including email accounts) without being challenged to provide a password each time can put security of that account at risk. It is strongly recommended that mechanisms that fill in passwords automatically are not used. However where they are used, it is strongly recommended that there is an additional layer of access control. For example, using a pin number to help protect access to a Smartphone, especially if it is configured for automatic connection to an email account.

7.3. Users of University IT systems must take all reasonable precautions to ensure that their passwords (or other security “secrets”) are not disclosed.

7.4. University IT users should be advised about scams intended to make them reveal passwords and how to avoid being caught out.

7.5. Where a computer account user suspects that security of their personal computer account may have been compromised they must:
   - Immediately change the password (if possible).
   - Immediately report the incident - see Reporting Information Security Incidents (ISP-I3).

8. Unattended user equipment

8.1. Computers and other equipment such as smartphones, used to log into University IT accounts, must never be left unattended if they are logged in and unlocked. (Users of such equipment should be advised to log them out or lock them before leaving them unattended.)

   1.1. Except in very special circumstances such equipment must be capable of automatically locking after a timeout period when left unattended. This automatic locking must be enabled and be effective in ensuring that unauthorised access to accounts that are already logged in, or which can be logged into using stored credentials, is prevented. The timeout period should normally be no longer than 20 minutes.

   1.2. Computers in the process of being logged out, or shut down, should not be left unattended until it is certain that they have definitely logged out. (This is in case the log out process fails and a logged in account is left unattended).

9. Protecting against unknown or malicious code

9.1. Accidental or deliberate running or installation of malicious code (malware) on computers presents a significant information security risk. The need to restore integrity of systems infected with such code also has an impact on their availability for use and consumes computer support staff effort.

9.2. An appropriate combination of proactive measures should be used to help manage the risk of malicious code being run on University systems. The measures should be promoted and supported by management and implemented by computer system administrators and users. Some combination of the following measures is recommended:
   - Deploying antivirus software developed by a reputable supplier, which should be kept fully up to date and used to scan all files: downloaded from the internet, received as attachments to email (or other forms of messaging) and all removable media when inserted. (Applicability of this varies between operating systems).
• Advising computer users to avoid running software or opening files obtained from untrusted sources and to be particularly cautious of accessing files attached to unsolicited email and stored on untrusted media. (This should be issued in conjunction with the advice about when it is appropriate to use privileged accounts.)

• Managing support of computers such that privilege to install software is restricted to staff, typically experienced computer support staff, who would be more aware of the problems that can result from installing code from untrustworthy sources.

• Implement departmental or Network Organisation level policy requiring staff to obtain approval from the Network Authority before installing items of non-standard software on University computer equipment. (The approval procedure should include a basic assessment of whether use of the software is justified and assurance that any software licensing requirements are met.)

9.3. See also:

• Software Management Policy (ISP-S13)

10. Use of email facilities

10.1. University email services are provided for official academic and administrative purposes, occasional personal use is permitted so long as such use is not excessive, in volume, frequency or time and does not disrupt or restrict usage by other legitimate users.

10.2. Staff must not configure their University email accounts to automatically forward incoming email to services that are not operated by the University, unless such an arrangement has been formally approved by the Director of IT Services and is subject to an appropriate bilateral contract. Also refer to:

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

10.3. Users of University email services should be advised that whilst privacy of their email messages is respected there are circumstances in which the content of their messages may be disclosed. This may be in response to a Data Subject Access Request made under the Data Protection Act. In addition there is provision for officers of the University to access the contents of University email. Also refer to:

• Institutional IT Usage Monitoring and Access (ISP-I6)

10.4. The University encourages the use of Out of Office functionality on email systems to inform colleagues and trusted third parties of your absence from the Office. For your personal security, telling unknown or un-trusted 3rd parties about your whereabouts is best avoided. It is strongly recommended that wherever possible you restrict sending Out of Office Replies to "people inside your organisation" and only to "Contacts" outside of your organisation. Detailed advice on how to do this is available on the IT Services website.

10.5. University email systems may not be used for any of the following:

• Unapproved transmission of commercial material (see also section 5 above).

• Spamming, i.e. sending unsolicited and unauthorised messages to a large number of people; this includes misuse of mailing lists. (Mass emailing to members of the University may be undertaken for purposes approved by the Registrar.)
• Messages requesting recipient to re-forward thereby setting up a chain action (chain mail).
• Messages likely to cause offence.
• Messages purporting to come from someone other than the actual sender (spoofing).
• Material advocating criminal activity or which may bring the University into disrepute.
• Material which violates copyright restrictions.
• Material which is defamatory or libellous.
• Material which could be used to breach computer security or facilitate unauthorised access.
• Material likely to prejudice the course of justice.
• Personal data about a third party in contravention of the Data Protection Act.

10.6. Other policy documents referring to use of email include:
• Information Handling Policy (ISP-S7)
• Mobile Computing Policy (ISP-S14)
• Cryptography Policy (ISP-S16)
• Guide to Information Legislation (ISP-I5)

11. Backups

11.1. 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.

11.2. 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.

11.3. For further details also refer to the Backups section in:
• Information Handling Policy (ISP-S7).

---

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

Document history:

27 August 2008 (C. Nelson) Began first draft.
24 September 2009 (C. nelson) Revised policy relating to shared accounts.
09 October 2009 (C. Nelson) Added a statement about email out-of-office replies.
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.
1. Introduction

1.1. This information security policy document sets out principles for how University information systems are to be specified and designed to meet security requirements and manage risks. It is a sub-document of Information Security Policy (ISP-S1).

1.2. This document includes statements on:
   - Scope
   - Specification or design
   - Authorisation and assessment
   - Equipment planning
   - System access
   - Implementation
   - Documentation

2. Scope

2.1. This system planning policy relates to information systems that are used to provide services that are important to the business of the University.

2.2. This policy does not apply to deployment of additional instances of an existing tested and approved solution such as the standard CFS desktop client.

2.3. In relation to IT systems, this policy refers to both hardware and software.

2.4. The principles covered in this policy also apply when planning for use of information systems or services provided by other organisations. See also:
   - Outsourcing and Third Party Access Policy (ISP-S4)

3. Specification or design

3.1. During specification or design of significant new information systems, or major upgrades to existing systems, information security risks should be identified and assessed. Those risk mitigation measures considered essential should then be incorporated into the specification or design.

3.2. General advice is offered by IT Services.

3.3. When planning highly sensitive, critical or specialised systems it is recommended that specialist security advice should be sought.

4. Authorisation and assessment

4.1. Projects to deliver new information systems, or significant upgrades to existing systems, should include authorisation and assessment phases:
• Before progressing from the specification or design phase into development or installation.
• As part of acceptance testing before progressing into live service.

4.2. This authorisation and assessment should include:
• Business approval – management approves the purpose and use of the system and ensures that the system is consistent with departmental strategy and any broader strategy (for systems that will provide a service beyond the department).
• Information security approval – the new system complies with relevant policies and does not adversely affect the security of existing information infrastructure.
• Technical approval – the system is approved from a technical perspective by the relevant technical managers.

4.3. Payment card processing systems must not be planned, commissioned, used or modified without consultation with and approval by the Finance Office. Refer to policy sub-document:
• Payment Card Security (ISP-I10)

5. Equipment planning

5.1. Computer systems shall be planned to ensure that adequate processing power, storage and network capacity are available for current and projected needs, all with appropriate levels of resilience and fault tolerance. Equipment shall be correctly maintained.

5.2. Computer systems shall be given adequate protection from unauthorised access, environmental hazards and failures of electrical power and other utilities. See also:
• Operations Policy for IT Service Providers (ISP-S6)

6. System access

6.1. Access controls for all information and information systems are to be set at appropriate levels in accordance with the value and sensitivity of the information assets being protected.

6.2. Access to operating system commands and application system functions is to be restricted to those persons who are authorised to perform systems administration or management functions. Where appropriate, use of such commands should be logged and monitored.

6.3. See also
• User Management Policy (ISP-S8)

7. Implementation

7.1. Following testing and approval new or upgraded systems shall be implemented and operated in accordance with University information security policies.

8. Documentation

8.1. Documentation of the planning process should include evidence that information security needs have been assessed and addressed. Findings of risk assessments and decisions taken in light of those assessments should be documented.

9. Related policy documents
9.1. From planning to providing a live service, project and system managers should be familiar with information security policy generally and in particular these documents:

- Information Asset Protection Policy (ISP-S2)
- Operations Policy for IT Service Providers (ISP-S6)
- Information Handling Policy (ISP-S7)
- User Management Policy (ISP-S8)
- Use of Computers Policy (ISP-S9)
- System Management Policy (ISP-S11)
- Network Management Policy (ISP-S12)
- Software Management Policy (ISP-S13)

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

**Document history:**

<table>
<thead>
<tr>
<th>Date</th>
<th>Document Version</th>
<th>Action Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>12 July 2010</td>
<td>C. Nelson</td>
<td>Approved.</td>
</tr>
<tr>
<td>16 August 2010</td>
<td>C. Nelson</td>
<td>Minor change to list of documents in 9.1.</td>
</tr>
<tr>
<td>18 May 2011</td>
<td>C. Nelson</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.
1. Introduction

1.1. This information security policy document sets out responsibilities and requirements for those managing computer systems. It is a sub-document of Information Security Policy (ISP-S1).

1.2. Definitions:

- System manager - someone who configures and maintains a multi-user computer or software application service.
- Back out plan - a planned course of action to restore a system to its previous state should a change fail to successfully complete or causes an undesirable effect.

1.3. This document includes statements on:

- System managers
- Responsibilities and duties of system managers
- System change management
- Access control
- Monitoring and logging system activity
- Importing software and files
- System clocks

2. System managers

2.1. University computer systems must be managed by competent staff to oversee their day-to-day running and to preserve security and integrity:

2.2. System management policy applies to all staff that use administrator privileges on any University multi-user computer or software application service.

3. Responsibilities and duties of system managers

3.1. 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.

3.2. Computer system managers are required to be aware of University information security policies in general. They must be familiar with this document and these other documents which are of particular relevance to system managers:

- Network Management Policy (ISP-S12)
- Information Handling Policy (ISP-S7)
- Software Management Policy (ISP-S13)
• **Use of Computers Policy (ISP-S9)**
• **Computer Account Passwords (ISP-I9)**
• **Institutional IT Usage Monitoring and Access (ISP-I6)**

3.3. System managers must take into account the confidentiality and value of the information they are managing, and the impact that a serious incident may have, when determining what security controls and risk mitigation measures to use. It is recommended that system managers perform a risk assessment on deploying new systems and from time to time thereafter. See also:

• **Managing Information Asset Security (ISP-I4)**

3.4. System managers are required to be proactive in working with information owners to help ensure that security requirements, expectations and limitations are mutually understood and agreed. A basic example of this is to ensure that information owners are aware of the backup arrangements, ensure that backups take place as specified and keep information owners informed of any changes or problems. For policy on making backups refer to the “Backups” section of:

• **Information Handling Policy (ISP-S7)**

3.5. Basic information about the security posture of a computer system should be made available to its users by the system manager. This is intended to enable information owners or custodians to make an informed decision as to whether the system meets their security requirements. This information should not include any details that would be of practical use to potential intruders; however, it might outline:

- Physical security of the system and its data storage.
- Access control.
- Operating environment.
- Backup frequency and security of backup data.
- Firewalling and protection against malware.
- Monitoring and systems administration staffing.
- Relevant policies implemented.
- Uses for which the system is not suitable.

3.6. Recognised managers of computer and network systems are encouraged to promote and implement information security policy. They are authorised to act promptly to protect the security of the systems and information for which they have responsibility. There must, however, be reasonable grounds for taking actions which impact users such as: temporarily removing devices from the network, disabling software or system functionality, or locking user accounts.

3.7. System managers and staff who have elevated access privileges are prohibited from going beyond the boundaries of their legitimate professional duties in relation to accessing users’ computer data. Any access to, or disclosure of, the contents of user data or communications must be appropriate, justified and follow correct procedures. See:

• **Institutional IT Usage Monitoring and Access (ISP-I6)**
3.8. System managers must be vigilant and immediately seek advice through their line management if they become, or are made, aware that any information served by the systems for which they have responsibility may:

- Not be lawful.
- Contain direct links to material which is unlawful.
- Purport to trade on the University's name in a commercial activity or goods without the approval of the University.
- Promote unapproved commercial activity.
- In any way damage the University's name or reputation.
- Not comply in some other way with University policies.

4. System change management

4.1. Changes to computer systems that provide a user service must be planned, tested, approved, publicised and implemented in a controlled manner.

- It is recommended that an appropriate “change management” procedure is established and followed for systems other than those managed and used exclusively by an individual user and where the changes would not put at risk other University systems or services.
- The change management procedure should involve stakeholders, create an audit trail, consider security implications, and include communication to users about forthcoming changes. (Change management is intended to help minimise and manage undesirable impacts on service users and the business.)
- The planning and testing of changes should include consideration of security factors including: information confidentiality requirements, data access controls, exposure of network services, known issues with software, data backup and the business continuity plan.
- Preparation for a change should include formulation, and where possible testing, a “back out plan”.
- Where possible, and always for key systems, testing should be undertaken in a separate test environment or using another method that avoids significant risk to the service.
- Changes to systems must be approved by management before made live or moved to the live environment.
- System managers should ensure that system users are advised about forthcoming changes before implementation.

4.2. IT Services staff manage changes to central services using a procedure based on Information Technology Infrastructure Library (ITIL). Some staff in other departments are able to implement changes either directly to IT Services managed systems, or changes which may significantly affect operation of those systems. Those departmental staff must submit proposals for such changes to the IT Services change management system for approval before implementation.

5. Access control
5.1. Access to all University information services and computer systems must be via a secure log on process, except for read-only access to public domain information.

5.2. Granting of access to University IT resources should be carefully controlled. There should be formal procedures in place for granting, changing and revoking access to information systems and services for handling the various scenarios. See:

- **User Management Policy (ISP-S8)**

5.3. University IT system managers must wherever technically possible enforce password policy. See:

- **Use of Computers Policy (ISP-S9)**
- **Computer Account Passwords (ISP-I9)**

5.4. The individual responsible for each computer account must be identifiable. This also applies to group accounts to the extent that the individual responsible for management of the account is known and can identify all others with access. See also:

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

5.5. The Administrator account, or administrator level access, should be used only at times when it is necessary to perform specific system administration or configuration tasks. (Unnecessary routine use of administrator level access by system managers has been a factor in many system compromises.)

5.6. System managers must ensure that user privileges are configured on the basis of “least privilege”, i.e. users should not be granted privileges to do things that they do not need to do and which might cause problems. Access to any operating system commands and utility programs which elevate the privilege of the user should also be appropriately restricted.

5.7. System managers should normally not allow users to work with elevated privileges (for example by placing normal user accounts in the “Administrator” or “Power Users” group on Windows systems). In exceptional cases, for example where technical problems require elevated privileges to make legacy or badly designed applications work, system managers should endeavour to work round or remove the problems - there is usually a more secure solution.

5.8. Access to files, folders and other resources should, wherever possible, be managed using group permissions rather than by individual account. The purpose, or intended membership, of each group should be defined clearly, for example “users”, “administrators”, “backup operators”, “managers” etc. The membership of each group should be correctly set and periodically reviewed.

5.9. Wherever appropriate and possible, systems and applications should be configured so that inactive connections shut down after a defined period of inactivity to help prevent access by unauthorised persons.

5.10. Recommended access controls for sensitive or high risk systems include:

- Allocate privileges through a formal authorisation process.
- Maintain a record of any access permissions granted that exceed basic user permissions.
- Maintain documentation of the purpose or intended membership of user groups.
- Log and preferably actively monitor access to help identify signs of misuse.
5.11. For very sensitive or high risk systems additional recommended access controls include:

- Limit privileged access according to physical or network location.
- Control privileged access based on time of day.
- Use of secondary security tokens.
- Use a secure console server arrangement.

6. Monitoring and logging system activity

6.1. Logging and monitoring of computer system activity should be implemented to adequately support security, compliance and capacity management.

6.2. System managers must act on any current legal compliance requirements pertaining to logging that apply to their systems.

6.3. The Data Protection Act requires that personal data is deleted when no longer needed for the purpose for which it was originally obtained. Procedures should therefore be implemented to ensure obsolete log data containing personal data (such as usage information by username) is deleted.

6.4. For systems where an intrusion or misuse could have a significant impact on the University, at the minimum, basic usage logging should be undertaken. This may consist of recording logs showing when users were logged in, when they accessed system resources etc.

6.5. Where logging is undertaken with a view to possibly using the logs as evidence in the case of an intrusion, then it is recommended that the logs are recorded on a different system to the one being monitored. (Usage logs are likely to be deleted or modified by an intruder.)

6.6. System logging can often be configured to record both successful and failed attempts to access system resources. For sensitive systems, audit logging may be configured to record access failures, which may indicate an intrusion attempt or operational problem.

6.7. Capacity demands of systems supporting business processes should be monitored and projections of future capacity requirements made to enable adequate processing power, storage and network capacity to be made available. System managers should report capacity risks or concerns that they have identified to their line manager.

6.8. Major systems, configured to produce useful levels of security and operational log information, typically produce more data than it is realistic to monitor manually. Where the sensitivity of a system justifies it, use of automated log monitoring and alerting technology is recommended to help make best use of security and operational log data.

7. Importing software and files

7.1. Software and data files intended for installation on critical computer systems should be downloaded or installed into a secure environment, scanned for malicious software and tested in a test environment before deployment in a live environment.

8. System clocks

8.1. All networked computers should be referenced to a reliable time server. Incident investigation often depends on accurate event log dates and on examining creation and modification dates of files and folders.
**Document history:**

<table>
<thead>
<tr>
<th>Date</th>
<th>Month</th>
<th>Year</th>
<th>Author</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>06 October</td>
<td>2009</td>
<td></td>
<td>C. Nelson</td>
<td>Began first draft.</td>
</tr>
<tr>
<td>06 July</td>
<td>2010</td>
<td></td>
<td>C. Nelson</td>
<td>Steering Group changes:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>- Changed scope of this document such that it does not apply to those who only administer their personal computers (as distinct from multi-user services).</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>- In 2.1 replaced “should” with “must” and “suitably trained and qualified” with “competent”.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>- In 2.1 removed bullets: “Wherever possible system management tasks should be undertaken by professional departmental or central computing staff” and “All systems management staff should be given general training on information security relevant to their role and sufficient specialised training to securely operate the systems they are required to manage.”</td>
</tr>
<tr>
<td>16 August</td>
<td>2010</td>
<td></td>
<td>C. Nelson</td>
<td>ISP-I4 is renamed “Managing Information Asset Security”.</td>
</tr>
<tr>
<td>14 October</td>
<td>2010</td>
<td></td>
<td>C. Nelson</td>
<td>“System managers must at all times take every reasonable care to ensure that all material which is served by systems for which they have responsibility...” was changed to “System managers must handle any reports or complaints about information, served by the systems for which they have responsibility, to help ensure that it...”.</td>
</tr>
<tr>
<td>02 November</td>
<td>2010</td>
<td></td>
<td>C. Nelson</td>
<td>Further revision of the section concerning System Managers’ responsibility relating to information being served, as recommended by the Steering Group.</td>
</tr>
<tr>
<td>18 May</td>
<td>2011</td>
<td></td>
<td>C. Nelson</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.
1. Introduction

1.1. This information security policy document covers management, operation and use of the University data networks and is a sub-document of Information Security Policy (ISP-S1).

1.2. Definitions:

- Network device - a device that is part of the network infrastructure such as a router, switch, gateway, firewall, network wall socket, wireless access point etc.

- Networked device - any device that can communicate via the University network including: PCs, servers, workstations, Personal Digital Assistants (PDA’s), environmental sensors, access control systems, cameras, printers, scientific instruments, IP phones etc.

- Device – a “Network” or “Networked” device (see above).

- Network interface - part of a device that enables it to communicate via a network.

- MAC (Media Access Control) address or “Ethernet address - a 48-bit number used to uniquely identify each network interface in a network. The network interfaces in most devices have a unique MAC address set during manufacture.

- IP - Internet Protocol. Currently IP version 4 (IPv4) is used as the communication language by almost all devices connected to the University network.

- For correct operation IP network interfaces must be configured to use suitable 32-bit numbers for the “IP address”, “subnet mask”, “default gateway” etc. (The IP address of a device is often also referred to as its “network address”.)

- Two significantly different levels of network connectivity are available depending on whether the user connects to the “wired” or “wireless” network. Wireless connections provide access to the Internet and to a limited range of Internet enabled University computing services.

- Network Organisation – an IT Services term meaning a group of networked devices which are managed by a particular sub-organisation of the University.

- Network Authority - an individual, nominated by a Head of Department, to be the primary point of contact for matters relating to security of networked devices in a particular Network Organisation; they authorise connection of devices to the “wired” network and may delegate this task to assistants known as “NetworkAuthorisers”.

- NDOR - the IT Services “Network Device Online Registration” database. It holds network address and other data about devices registered for connection to the “wired” network.
1.3. This document includes statements on:

- Management of the network
- Network design and configuration
- Physical security and resilience
- Connecting devices to the network
- Management of networked devices
- Acceptable use of the network
- Network services and protocols
- Controlling access to and from other networks
- Incidents and emergency procedures

2. Background

2.1. This policy refers to the University network, including the “wired” and wireless networking around the University. The University network covers all buildings on the main University campus, most off-campus University locations and University presence in the three University Hospitals of Leicester.

3. Management of the network

3.1. The high level strategy for central IT provision, including data and voice networks, is determined by the Information Communications Technology Committee (ICTC). IT Services is responsible for the campus networks. The Data & Voice Network Services (DVNS) Team within IT Services has principal day to day accountability for managing and operating the networks.

3.2. IT Services is responsible for administering all network devices such as routers, switches, gateways, firewalls, network wall sockets, wireless access points and wall sockets forming the University network infrastructure. The Campus network cabling extends to nearly all University buildings and departments and is also the responsibility of IT Services. Note:

- No unauthorised changes or other interference with these network devices or cabling is permitted.
- Moves, changes and other reconfigurations of cabling and users’ network access points will only be carried out by staff authorised by IT Services according to procedures laid down by them.
- IT Services is responsible for providing the enterprise wireless network service. Departments are prohibited from establishing their own wireless networks and adding wireless access points since these may conflict with the central provision of wireless hotspots.

3.3. The implementation of new equipment or upgraded network software or firmware must be carefully planned tested and managed. Formal change control procedures, with audit trails, shall be used for all changes to critical systems or network components.

3.4. IT Services reserves the right to make changes to network security as and when necessary. This may be in relation to a security threat or to improve existing arrangements.
3.5. 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 devices or sub-sections of the network from service.
- Manage network resource allocation (such as bandwidth).

3.6. Control of network address allocation rests with IT Services although this may be delegated to departmental support staff for specific address schemes.

3.7. It is IT Services policy to endeavour, within the networking resources available, to equitably satisfy the legitimate and justified demands of all network users and to meet any relevant service level agreements that might be in place.

3.8. Users of University networks are to be explicitly advised that normal operational network management procedures will include: probing devices to test their security and the monitoring of network traffic to detect operational problems or possible policy violations. See also:

- Institutional IT Usage Monitoring and Access (ISP-I6)

4. Network design and configuration

4.1. The network must be designed and configured to deliver levels of performance, security and reliability suitable for the University’s business needs, whilst providing a high degree of control over access.

4.2. Controls should be used where practical to partition the network into domains on the basis of security requirements. Access controls and routing should be used to prevent unauthorised access to network resources and unnecessary traffic flows between domains. In particular, appropriately configured firewalls should be used to help protect the University’s critical computer systems.

4.3. Networking serving discrete buildings or departments is connected to the campus network only on the understanding that:

- Either, designated departmental network support staff are identified who will work in cooperation with IT Services. (Such staff should be available for consultation during normal working hours. In addition they should be available, with reasonable notice, when out-of-hours development and maintenance is taking place.)
- Or, all rights and responsibilities, including privileged access to any network devices, are ceded to IT Services.

4.4. In principle, permission to use particular protocols, and registration of addressing information, are not necessary for departmental networks that are completely isolated from the campus network, and will never share traffic with it. However, it is very strongly recommended that such networks be managed as though they were part of the campus network, since this will minimize future inconvenience if it is found at a later date that an interconnection is desirable. It will also prevent the problems that might arise if an unplanned connection between networks is made inadvertently.

5. Physical security and resilience

5.1. Reasonable measures based on an assessment of risk, such as fire and water protection, padlocks, secure cabinets etc, must be taken to protect networks and
communication equipment against accidental damage, potential security breaches, theft or malicious intent.

5.2. The network should where possible incorporate logical and physical resilience features to help mitigate the impact failure of, or physical damage to, cabling and other network equipment.

5.3. See also:
- Operations Policy for IT Service Providers (ISP-S6)
- Building Security (ISP-I1)

6. Connecting devices to the network

6.1. Ownership of networked devices
- Only 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.
- All devices whether privately owned, or owned by other organisations, must meet the hardware and software requirements, as set out below, and their usage must conform to University policies.
- Regardless of ownership of a device, its connection to University networks is conditional on IT Services having the right to inspect its configuration, test its security and monitor its network traffic in accordance with normal operational network management procedures.

6.2. Administration of networked 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.
- Networked devices on the “wired” network may be administered by IT Services, departmental staff or an organisation contracted to undertake their administration.
- It is recommended that where possible administration of networked devices on the “wired” network is restricted to, and undertaken by, computer support specialists. However; departments may choose to delegate administrative privileges for specific devices to other suitably qualified staff, where there are specialised requirements.
- Users of privately owned networked 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.

Adequate support and maintenance arrangements must be in place for University owned wireless devices.
6.3. Authorisation to connect a 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.)

- Network Authorities and Authorisers must only approve connection of devices to the “wired” network when they are certain that candidate devices meet all relevant requirements set out in the “Connecting devices to the network” section of this document.

- 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.

6.4. Authentication of network users

- Users of University IT facilities must not masquerade as another user or tamper with audit or activity logs.

- It is the responsibility of Network Organisations to manage their computers in a way that ensures that local account users can be identified.

- It should be possible to identify the administrator of each device. Each administrator should be able to be able to identify who is authorised to use any accounts they have created. It is not acceptable for accounts on networked University computers to provide anonymous access or the equivalent of anonymous access.

- Where it is necessary for an account to be shared, the system administrator, or the individual designated as responsible for managing that account, must have full knowledge of the users that have been authorised to share the account.

- In response to security audits or investigations, users and administrators must respond to request for information from IT Services in a timely manner.

6.5. Networked device registration

- Except where IT Services has delegated responsibility for allocating particular groups of addresses to departmental support staff, all devices using the “wired” network must be registered with IT Services.

- Registration of static devices is to be undertaken using the NDOR system.

- The DVNS team in IT Services should be contacted directly about registration of “roaming” devices.

6.6. Hardware and software requirements

- Networked devices must meet current hardware and software requirements, where any such requirements are specified and published by IT Services. At the discretion of IT Services any devices not meeting any such requirements may be denied network access.
- 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 firewalling).

- 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 networked 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, networked devices should have current and automatically updated anti-virus software installed.

- Where applicable, networked 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.

- Given the variation in software licence agreements, only University-owned machines are considered eligible to become CFS clients.

- Mechanisms intended to ensure University compliance with software licensing restrictions must not be disabled, or their operation interfered with.

7. Management of networked devices

7.1. Those responsible for networked devices must work in cooperation with IT Services such that it can discharge its responsibility for managing the overall network.

7.2. Responsibility for devices must be clear and should fall within the line-management of the University, through Heads of Department.

7.3. Primary control over access to the “wired” network is to be implemented by staff in the Network Authority and Authoriser roles who must:

- Decide whether to approve requests for connection of devices to the “wired” network on the basis of the connection requirements set out in this policy document.

- Be a point of contact with IT Services in relation to the security of the networked devices within their area of responsibility i.e. their Network Organisation.

- Take responsibility for handling security problems that arise in relation to networked devices in a timely manner. Technical support is to be provided to departmental staff by IT Services. Nevertheless, for devices not fully managed by IT Services, ultimate responsibility for ensuring configuration and usage complies with policy rests with departments.

- Where necessary, remove a device from the network to help protect operation or security of the wider network. This should be undertaken in collaboration with IT Services and where possible the person with day-to-day responsibility for the device.

8. Acceptable use of the network
8.1. Connectivity of University networks to the Internet is provided by "JANET" (Joint Academic NETwork) and is subject to compliance with JANET policies. See also:

- Compliance Policy (ISP-S3)

8.2. It is a condition of using University networks that the owners, administrators and users of devices comply with all relevant University policies. In particular, responsibilities and required behaviour of users of University IT systems, including University networks, are described in:

- Use of Computers Policy (ISP-S9).

8.3. All use of the network should be undertaken on the basis of responsible use of a finite shared resource. If there is any doubt as to whether some intended usage of the network is permitted, or could significantly impact performance of the network, then advice should be sought from IT Services before proceeding.

8.4. If some intended use of the network is not explicitly disallowed or controlled it is not necessarily condoned or encouraged.

8.5. Unauthorized eavesdropping will be treated as a serious breach of policy. For the same reason, network monitors and similar devices which allow the inspection of network traffic must not be used without the prior approval of IT Services. See also:

- Institutional IT Usage Monitoring and Access (ISP-I6)

9. Network services and protocols

9.1. Unless there is a compelling reason to do otherwise; existing central or recognised departmental web servers should be used for publishing University generated content.

9.2. Deploying web servers or other types of network servers which do not support recognised University research, teaching or administrative activities is prohibited.

9.3. Only IT services, or Network Organisations with delegated responsibility for management of IP address groups may operate Dynamic Host Configuration Protocol (DHCP) or TCP/IP Bootstrap Protocol (BOOTP) servers.

9.4. IP routing protocols are managed by DVNS on routers in the core of the network. Routing protocols, for example RIP, IGRP, BGP etc should not be enabled when setting up IP-connected nodes.

9.5. The use of network management tools that use protocols such as SNMP and CMIP, is restricted to IT Services staff, other than by prior agreement.

9.6. University servers running Domain Name Service (DNS) are managed by DVNS other than by prior agreement.

9.7. University servers running Network Time Protocol (NTP) are managed by DVNS other than by prior agreement.

9.8. Where access credentials, or other confidential information, may otherwise be transmitted on the network in clear text (i.e. unencrypted), use of encrypted network protocols is strongly recommended. See also:

- Information Handling Policy (ISP-S7)
- Outsourcing and Third Party Access Policy (ISP-S4).docx
- Mobile Computing Policy (ISP-S14).docx
10. Controlling access to and from other networks

10.1. IT Services is responsible for controlling the network gateway between the University of Leicester networks and the Internet. At this gateway IT Services may exert control over which incoming or outgoing network connections are permitted. This access control may be used for:

- Limiting the scope of exposure of University network services to the Internet in order to reduce the risk of hacking, denial of service attacks, unauthorised disclosure of information etc.
- Preventing propagation of malware or network traffic associated with malware.
- Applying control consistent with implementing current University IT strategy.

10.2. Exposure of network services to incoming connections from the Internet is not permitted without prior agreement from IT Services. Note:

- “Incoming connections” are those initiated from devices on the Internet.
- All established provision of network services to the Internet may subject to review.
- IT Services’ agreement to permit connections into departmental systems will be consistent firstly with current University IT strategy then secondly with departmental IT strategy.
- These network services include, however, are not limited to: websites, login access for offsite users or automated processes, connection into remote desktop access software etc.

10.3. Access to the University network from the Internet via Virtual Private Network (VPN) connections is not permitted without prior agreement from IT Services.

10.4. Dial up access to a device on the University network using a modem is not permitted without prior agreement from IT Services.

11. Incidents and emergency procedures

11.1. Any incident or emergency relating to the University network should be reported to the Service Desk in IT Services.

11.2. IT Services must ensure that prompt and effective action is taken in response to requests and information from JANET CSIRT (Computer Security and Incident Response Team).

---

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

---

**Document history:**

12 August 2009 (C. Nelson) Began first draft – based on “Network Connection Policy and Usage Guidelines”.

10 November 2009 (C. Nelson) Revision based on input from Lee Robinson (DVNS).
There are circumstances under which it is appropriate for a privately owned device to be connected to the “wired” network.

Redundant bullet point removed from 6.4. Removed words “and approved” from 9.1.

Revisions resulting from review within IT Services and additional clarification and removal of repetition.

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.
1. Introduction

1.1. This information security policy document contains high-level descriptions of expectations and principles for managing software on University computer systems. It is a sub-document of Information Security Policy (ISP-S1).

1.2. Definitions:

- Software management - any procurement, development, installation, regulation, maintenance or removal of software that takes place on University owned computers or computers permitted connection to University networks.

1.3. Software is very important to the University because it is used extensively to enhance, or enable, performance of many key activities. Software management decisions taken across the University influence efficiency, economy and information security. This document is primarily concerned with security aspects of software management.

1.4. This document includes statements on:

- General software management principles
- Managing security risks relating to software
- Permitted, regulated and prohibited use of software

2. General software management principles

2.1. All software, including operating systems and applications must be managed correctly.

2.2. There must be an identifiable individual or organisation taking current responsibility for every item of software deployed.

2.3. Those responsible for software must monitor relevant sources of information which may alert them to a need to act in relation to new security vulnerabilities.

2.4. Software is to be patched as soon as possible to remove security vulnerabilities.

2.5. Staff involved in managing software must have experience, training or qualification commensurate with the importance of the software and risk levels involved. At the minimum all staff involved must be aware of, and proactive in managing, information security related risks associated with software. University departments must support this policy by ensuring that permission and responsibility for systems and software management is delegated accordingly.

2.6. University software management procedures must incorporate measures for controlling these information security risks:

- Illegal use of software
- Use for of software for illegal purposes
- Software copyright infringement
3. Managing security risks relating to software

3.1. Software procurement

- When business requirements for new systems or enhancements are being specified, the specification documents should describe any special or essential requirements for security controls.
- When software for use by the University is being procured there must be an assessment of whether the software incorporates adequate security controls for its intended purpose.
- It must be investigated and taken into account whether proposed new software or upgrades are known to have outstanding security vulnerabilities or issues.
- At the time of software procurement, the basis of future support and the expected supported lifetime of the product should be established. It may be important to have assurance that manufacturers will provide updates to correct any serious security vulnerabilities discovered in future.
- Consideration should be given to software escrow for mission critical applications. In a software escrow agreement the software source code is deposited into an account held by a third party escrow agent. Escrow is typically requested by a software licensee to ensure maintenance of the software. The software source code is released to the licensee if the licensor fails to maintain and update the software as promised in the software license agreement. (Expertise and advice on purchasing matters is available from the University Purchasing Office.)

3.2. Software development

- Software developed at the University must be assessed for its potential to introduce information security risks and any such risks must be adequately addressed.
- Upgrades or other changes to locally developed software must be assessed in terms of whether they may introduce an increased risk to information security. Any risks identified must be suitably addressed.

3.3. Software modification

- In-house customisation of externally written software should be avoided where it may lead to future difficulty for the University in obtaining external support. Only strictly controlled essential changes should be permitted and all changes made should be fully documented.

3.4. Software installation

- For each item of software managed by a department a master copy of any media, enabling codes and installation instruction must be stored safely in accordance with departmental procedures.
Software must not be put into user service on University systems unless a department or group has assessed and committed to providing sufficient resourcing for its ongoing management. (Software applications and systems utilised by the University vary widely in cost, relative importance, user numbers, complexity, maintenance requirements and code quality. These factors must be taken into account when evaluating the ongoing resourcing commitment that will be required.)

3.5. Software regulation

- Use of illegal software and using software for illegal activities could be construed to be gross misconduct.
- 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.
- Use of software which causes operational problems that inconvenience others, or which makes demands on resources which are excessive or cannot be justified, may be prohibited or regulated.
- Software found on University systems which incorporates malware of any type is liable to automated or manual removal or deactivation.
- Use of software that monitors the activities of other people is subject to regulation. For further information refer to:
  - Institutional IT Usage Monitoring and Access (ISP-I6)

3.6. Software maintenance

- Change control procedures, with comprehensive audit trails, must be used for all changes or upgrades to software of importance. Where correct operation of the software is itself important, or of importance to a wider system, changes must be authorised and tested before being applied to the live environment.
- Software must be actively maintained to ensure that all fixes and patches, needed to avoid significant emerging security risks, are applied as promptly as possible.
- Changing software of critical importance that is in service may sometimes be judged too risky. For example the risk of something going wrong as a result of installing a patch may seem greater than the risk associated with not installing it. It is good software management practice to assess such risks, make an informed judgement and document the reason for the decision. When it is necessary to defer installing a security fix, a less risky way or time to proceed with the installation must be sought.
- Systems running software, including the operating system, which are clearly not being maintained adequately and which may be presenting a wider risk to security are liable to have their University network connectivity withdrawn. This decision may be made by the Network Authority for the department responsible for the system; however, it may also be made by the Network Services Section of IT Services. Related information may be found in:
  - Network Management Policy (ISP-S12)

3.7. Software removal
- 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. Systems and application software that are no longer required should be decommissioned; where they will not be managed for an extended temporary period they should be removed from service.
- When decommissioning a computer system, for disposal or re-use, appropriate measures must be taken in relation to any software and data stored on it. Software must be removed, where not doing so could lead to breaking the terms of its licence. Further details relating to secure disposal or re-use of equipment may be found in:
  - Information Handling Policy (ISP-S7)

4. Permitted, regulated and prohibited use of software

4.1. The University must comply with its overriding legal and contractual obligations. Some of these obligations affect software and the uses to which it may be put. Further information may be found in:

  - Compliance Policy (ISP-S3)

4.2. 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. For example it may be necessary to regulate use of particular software applications or limit usage of particular types of application in order to prevent operational problems.

4.3. Heads of Department may implement additional specific local policies relating to IT management, which may include further restrictions affecting software.

---

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

---

### Document history:

<table>
<thead>
<tr>
<th>Date</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>07 July 2008</td>
<td>Began first draft.</td>
<td>(C. Nelson)</td>
</tr>
<tr>
<td>03 July 2009</td>
<td>Minor change.</td>
<td>(C. Nelson)</td>
</tr>
<tr>
<td>07 July 2010</td>
<td>Steering group advised changing “Use of illegal software and using software for illegal activities is not permitted.” to “Use of illegal software and using software for illegal activities could be construed to be gross misconduct.”</td>
<td>(C. Nelson)</td>
</tr>
<tr>
<td>18 May 2011</td>
<td>Revisions resulting from review within IT Services.</td>
<td>(C. Nelson)</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.
1. Introduction

1.1. This information security policy document sets out additional principles and expectations relating to using mobile computing devices and using computers away from the office. It is a sub-document of Information Security Policy (ISP-S1).

1.2. 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.

- Mobile computing device – a portable computing or telecommunications device that can execute programs or store digital data. Examples: laptop, handheld computer, notebook, palmtop computer, personal digital assistant (PDA), mobile phone, digital camera, portable printer, portable scanner, CD, DVD, diskette, magnetic tape, external/removable hard drive, flash memory card/drive.

1.3. Mobile computing and telecommunications devices make it easy to work away from the office and thereby expose information to different and probably increased security risks. In particular, mobile devices are prone to loss or theft.

1.4. The availability of home computers and networked computers managed by third-party organisations can also enable staff or research students to process University information when away from the office. The University cannot assume, or ensure, that such devices have security controls adequate for secure handling of confidential information.

1.5. Use of mobile computing to work securely with confidential data may involve additional cost and effort; this may be an unnecessary expense where suitable centrally administered services are already available. The business need should justify committing additional resources to mobile computing.

1.6. This document includes statements on:

- Mobile Computing.
- Information handling requirements.
- Mobile computing equipment - purchase, suitability and support.
- Management of mobile computing devices.
- Reassignment, repair and disposal of equipment.
- International transfer of personal data and the Data Protection Act.

2. Policy scope

2.1. This policy relates to storing and accessing University information:
• Using mobile computing devices.
• Using computers away from the office.

3. Mobile Computing

3.1. 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 or home computing device to store or access confidential data, then a suitably configured University owned device must be provided.

3.2. Staff and students are strongly advised not to store or access any confidential information from: privately owned home computers, public computers in libraries, cyber cafes, hotels etc. (This is because the University has no control over the specifications, operation or administration of such devices and therefore cannot be confident of their security.)

3.3. Staff or students nevertheless electing to store or access confidential information from devices not owned by the University should take appropriate security precautions based on a risk assessment that takes into account the nature and quantity of the data involved. They should be aware that certain data supplied by external bodies may be subject to specific security requirements. (In the event of loss or disclosure of confidential information, individuals responsible for handling that data will be expected to give an account of the security precautions in use.)

3.4. Individuals must not allow any access to, or use of, equipment that may put confidential information at risk of loss or disclosure. Examples:

• Individuals must not permit others, including family or friends, to use or modify any equipment provided by the University to carry out their professional duties.

• Individuals, electing to take personal responsibility for storing or accessing confidential information using privately owned home computers, must ensure that others do not have access to or see that information. In addition they must ensure that unauthorised persons do not have privileges to install software or otherwise put the security of the system at risk.

3.5. Any loss, or possible unauthorised disclosure, of confidential information must be reported to the relevant Head of Department and Information Assurance Services.

4. Information handling requirements

4.1. 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 information it may also be necessary also to encrypt it. Refer to:

• Cryptography Policy (ISP-S16)

4.2. 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.) 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. (The data will then be secure regardless of whether all, none or only some of the stages in the network link use an encrypted protocol.)

4.3. Where confidential information is being handled using a mobile device also:

• Where possible anonymise personal data.
• Handle the minimum amount of data necessary for the work in hand.
• Hold the data for the minimum time.
• Make backups. Mobile computing devices can fail, be damaged or stolen – have an appropriate backup regime for any important data stored on the device.
• Use a password protected screen saver / screen lock. (Should the device be left unattended this may help to avoid unauthorised access).
• Use strong passwords for all accounts which have access to the device. (Weak passwords have been a major cause of compromised systems and data).
• Actively manage physical security and not leave the device unattended where there is a significant risk of theft. Examples: do not leave it in a parked car, lock it in an office draw when not in use, lock the door when leaving it in an office etc.
• Do not leave the device logged in and unlocked where there is a significant possibility that it may be accessed by an unauthorised person.
• Do not work with confidential data where there is a risk of “shoulder surfing” i.e. someone looking over your shoulder at the screen or keyboard.

4.4. See also:

• Information Handling Policy (ISP-S7)

5. Mobile computing equipment – purchase, suitability and support

5.1. When considering use or purchase of a mobile computing device, that may be used to manage any confidential information, it is essential to ensure that:

• Where the device is to be used to handle data provided to the University by external bodies or vice versa, it is capable of meeting any specific security requirements demanded.
• The device is technically capable of providing acceptable security for data whether that data is being stored, downloaded or uploaded to the device.
• There will be adequate technical support available to ensure that the device can be configured and used in a way that keeps confidential data secure.

5.2. Advice and support for approved University devices and software may be requested from departmental computing staff or IT Services.

6. Management of mobile computing devices

6.1. To help ensure security, even on devices with full disk encryption, they must be actively managed in terms of configuration and maintenance. (Encryption may not prevent access to data if a running full disk encrypted system is infected or hacked).

6.2. Ensure that devices have current and automatically updated anti-virus software installed where applicable. (Presence of malware such as viruses or worms may be a threat to security of data on the device).

6.3. Ensure that the device remains up to date with security patches for both the operating system and any software applications installed.

6.4. Ensure that devices have correctly configured firewall software installed where applicable. (Vulnerable network services may be a threat to security of data on the device).
6.5. Ensure user privileges are configured on the basis of “least privilege”. (For example under Windows ensure that users that do not need administrator privileges are not in the “Administrator” or “Power Users” group.)

6.6. Ensure that for normal business activities the user does not work with administrative rights. (Administrative rights should be used only when it is necessary to perform specific system administration or configuration tasks.)

6.7. Installing software from untrusted sources must be avoided. (Such software is far more likely to harm security than tried and tested software obtained from well known legitimate sources.)

7. Reassignment, repair and disposal of equipment

7.1. Departmental procedures must ensure that data is removed as appropriate before a loan mobile computing device is reassigned to another person. Preferably this should be done routinely at the time the device is returned.

7.2. Data must be securely deleted when disposing of mobile computing devices. 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.)

7.3. Where a mobile computing device is to be repaired by another organisation there are two options relating to personal or confidential data stored on the device:

   - Remove the data from the device before the repair or maintenance work is undertaken.
   - Use a company that is subject to a suitable contractual agreement stipulating secure data handling.

8. International transfer of personal data and the Data Protection Act

8.1. Transportation of personal data to a country or territory outside the European Economic Area (i.e. the EEC plus Norway, Lichtenstein and Iceland) potentially breaches Principle 8 of the Data Protection Act 1998. For further information consult the University Data Protection Code of Practice and for advice contact Information Assurance Services.

---

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

---

Document history:

4 November 2008 (C. Nelson)  Began first draft.
3 July 2009 (C. Nelson)   Minor change.
<table>
<thead>
<tr>
<th>Date</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>16 December 2009</td>
<td>(C. Nelson) Revised to be more explicit about home computing and third-party facilities to avoid the need for restatement in Teleworking Policy.</td>
</tr>
<tr>
<td>01 March 2010</td>
<td>(C. Nelson) Approved by the InfoSec Policy Steering Group.</td>
</tr>
<tr>
<td>18 May 2011</td>
<td>(C. Nelson) 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.
1. Introduction

1.1. This information security policy document sets out high level principles and expectations that apply to teleworking. It is a sub-document of Information Security Policy (ISP-S1).

1.2. Definitions:
   - Teleworking - Article 2 of the European Framework Agreement on Telework of 2002 defines Teleworking as: “a form of organising and / or performing work, using information technology, in the context of an employment contract / relationship, where work, which could also be performed at the employer’s premises, is carried out away from those premises on a regular basis.” (Note: Teleworking can encompass a variety of working arrangements, including home-working telecentres and working from satellite offices in different locations. Teleworkers may be University employees or self-employed.)

1.3. This document includes statements on:
   - Teleworking security policy scope and purpose.
   - Authorisation for teleworking.
   - Provision of teleworking equipment.
   - Security of information while teleworking.

2. Teleworking security policy scope and purpose

2.1. This policy relates to any arrangement where particular staff work at an offsite location, on a regular or long term basis, and which also involves them in:
   - Holding significant quantities of confidential University information offsite, whether in electronic or paper format
   - Or having a type or level of remote access to information or applications on University servers which exceeds that which is ordinarily available to all staff.

2.2. The purpose of this policy is to ensure that teleworking is undertaken safely from an information security perspective. It is therefore required that information security risks, related to each specific teleworking scheme, are identified assessed and managed.

2.3. These other information security policies are particularly relevant to users of mobile computing devices and those handling confidential information outside secure University locations. They may also therefore be particularly relevant for teleworkers:
   - Information Handling Policy (ISP-S7)
   - Mobile Computing Policy (ISP-S14)
   - Cryptography Policy (ISP-S16)
3. Authorisation for teleworking

3.1. Only if the University wishes, and is able, to provide suitable teleworking facilities, may a member of staff undertake teleworking and only in cases where:

- It is the University that requires the member of staff to undertake teleworking or it has been approved for the member of staff to adopt a formal flexible working arrangement. (Note: Staff also applying to adopt formal flexible working arrangements are subject to the University policy on flexible working which is managed by the Human Resources Division.)

3.2. Staff must also be authorised by their Head of Department to undertake teleworking as distinct from other remote working arrangements.

3.3. The teleworking authorisation process should involve an assessment of information security risk taking into account several factors: criticality of the information assets being accessed, confidentiality of information being handled and suitability of the teleworking technology and location.

3.4. Those providing or supporting remote access facilities must do so in cooperation and with approval of IT Services. See also:

- Network Management Policy (ISP-S12)

4. Provision of teleworking equipment

4.1. Arrangements must be in place to ensure that any University teleworking solutions that should be provided are fully supported and maintained.

4.2. Those responsible for managing provision of teleworking equipment must ensure, on termination of the arrangement, the secure return or disposal of all equipment and information, in electronic and paper form, held by the teleworker.

4.3. Procedures relating to correct usage of any teleworking solution provided must be documented and explained to teleworking staff. In particular the solution must support adequate data backup and teleworkers must understand the backup procedure.

4.4. Any software used as part of a University teleworking solution must be appropriately licensed.

4.5. Any teleworking equipment which provides remote access to the University network, and the authentication method that it uses to access University resources, must be approved by the Network Services Section in IT Services.

4.6. Those responsible for managing provision of teleworking equipment should be mindful that teleworking systems will use an external Internet service provider. It cannot be assumed that behind the scenes technical security measures will be the same as those implemented to help protect campus network devices.

4.7. Provision and support of teleworking must reliably implement normal information security measures. For details see “Management of mobile computing devices” section in:

- Mobile Computing Policy (ISP-S14)

4.8. Where it is unavoidable that a teleworker must handle confidential information they must be provided with a computer incorporating full disk encryption and where necessary file encryption tools. See:

- Cryptography Policy (ISP-S16)

5. Security of information while teleworking
5.1. Staff, provided with computing and communications equipment for teleworking specifically to protect the security of confidential information, must not put the information at risk by using other less secure equipment.

5.2. Teleworking equipment provided by the University may only be modified or replaced if that has been authorised.

5.3. Teleworking equipment supplied by University is only to be used by University staff, particularly since others are not bound by University agreements and policies.

5.4. Teleworking staff must ensure that adequate backup procedures for any information held offsite are implemented. (It would normally, however, be preferable to remotely access data that is held onsite and already subject to routine backup).

5.5. Only when unavoidable should staff take, send or print hardcopies of confidential documents out of secure University locations. Where absolutely necessary to handle confidential hardcopy documents they should be kept in locked cabinets when not attended (clear desk policy), sent by recoded delivery post, delivered by hand where possible and disposed of by shredding.

---

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

---

**Document history:**

<table>
<thead>
<tr>
<th>Date</th>
<th>Event Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>07 July 2010</td>
<td>(C. Nelson) Input from Chris Sharp requested and incorporated as recommended by the Steering Group.</td>
</tr>
<tr>
<td>19 July 2010</td>
<td>(C. Nelson) Revised policy approved by Chris Sharp.</td>
</tr>
<tr>
<td>02 November 2010</td>
<td>(C. Nelson) Approved by the Steering Group.</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.
1. Introduction

1.1. This information security policy document sets out principles and expectations about when and how encryption of University digital information should (or should not) be used. This is a sub-document of Information Security Policy (ISP-S1).

1.2. This document includes statements on:

- Cryptography and UK law
- Data encryption for secure network transit
- Required use of encryption
- Management of encryption keys
- Required use of digital signatures
- Unsupported use of encryption
- Cryptography implementation

2. Related policies

2.1. Refer also to:

- Information Handling Policy (ISP-S7)
- Mobile Computing Policy (ISP-S14)

3. Cryptography and UK law

3.1. Export regulations relating to cryptography technologies are complex. (Any member of the University becoming involved in export of cryptography is advised to seek specialist advice. Information Assurance Services can assist by coordinating access to such advice.)

3.2. The Regulation of Investigatory Powers Act (RIPA) came into force in October 2000. Section 49 includes a provision for public authorities to demand, where it is judged there are reasonable grounds, decryption keys or decryption of information stored on computer systems in the UK. Anyone who could be assumed to have encrypted and stored data is very strongly advised to ensure that they retain the means to decrypt it.

4. Data encryption for secure network transit

4.1. Provided no other restrictions apply, it is permitted for all University staff and students to use computer systems which would normally and by default use encryption, in order to secure data in transit on a communications network.

4.2. Whenever possible and appropriate, encryption shall be used to support security of remote access connections to the University’s network and computing resources.

5. Required use of encryption
5.1. 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:

- Any personal data classed as “sensitive” by the Data Protection Act.
- Any data, that is not in the public domain, about a significant number of identifiable individuals.
- 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:

- 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. (Computers used to access remotely stored data or to process locally stored data may create cache files. Depending on the technology in use persistent and unencrypted cache files may be created.) Any such device when outside a secure University location is considered to be at significant risk, including home computers.
- 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.
- 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.

5.2. 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.

5.3. 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 below to the “Cryptography implementation” section.

5.4. Individuals must be authorised by the Head of Department before taking or sending confidential information out of a secure University location. Optionally the Head of Department may elect to authorise specific individuals to routinely undertake a particular activity involving a specific type of data. A departmental record of such authorisations is to be established and maintained recording the following details:

- The data name or description.
- Who has been authorised to remove the data.
- Purpose for which the data is being removed.
- Date of data removal or an indication where removal is routine, e.g. “during exam marking”.
- Where the data is being taken or sent.
- Any agreed external security requirements that apply to the data.
- Confirmation that the data will be encrypted and handled securely.
- Encryption technology used e.g. name of encryption hardware or software.
5.5. 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).

6. **Management of encryption keys**

6.1. Departmental procedures must be in place:

- To manage encryption keys in a way that ensures encrypted stored data will neither become unrecoverable nor accessible by an unauthorised person.
- To facilitate authorised officers of the University to obtain prompt access to the encrypted information in the case of an emergency or investigation.
- To ensure that encryption keys are stored and always communicated securely.
- To record who holds encryption keys relating to important information.
- To revoke encryption keys when key holders leave.

6.2. Where practical, an unencrypted backup copy of critical University data should be securely maintained. Critical backup data should be stored where there are appropriate physical security measures in place (e.g. on resilient computer servers in an alarmed computer room or on backup tapes stored in a fire safe preferably in a different building).

6.3. Where University information received as email has been encrypted for secure transit, and is information which may be needed again later, it should be securely stored in a form which does not rely on ongoing accessibility of the sender's public key.

7. **Required use of digital signatures**

7.1. Significant University business information being communicated electronically should be authenticated by use of digital signatures; information received without a digital signature should not be relied upon. Staff involved must assess the level of risk and decide whether to require use of digital signatures or whether to use an alternative means to authenticate the communication.

8. **Unsupported use of encryption**

8.1. Staff and students should:

- Not store encrypted data on University systems except where they are able to justify doing so for legitimate purposes.
- Be aware that the University reserves the rights to request sight, at any time, of the unencrypted version of any data stored on its systems and the option to remove any data.

9. **Cryptography implementation**

9.1. All encryption products, standards and procedures used to protect sensitive University data must be ones which have received substantial public review and have been proven to work effectively.

9.2. Where a department elects to undertake an activity that would incur a cost, in order to remain compliant with security policy, then that cost should normally be found from the departmental budget. For example, where a research project requires measures for secure data handling it is appropriate that costs for any necessary additional security measures are factored into the tender.
9.3. Further guidance about which encryption technologies are considered suitable for particular tasks and any supporting implementation details will be provided in policy sub-document:

- Cryptography Implementation (ISP-I7)

---

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

---

**Document history:**

<table>
<thead>
<tr>
<th>Date</th>
<th>Month</th>
<th>Year</th>
<th>Author</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>13 June</td>
<td></td>
<td>2008</td>
<td>(C. Nelson)</td>
<td>Began first draft.</td>
</tr>
<tr>
<td>5 November</td>
<td></td>
<td>2008</td>
<td>(G. Hamp)</td>
<td>Minor changes made.</td>
</tr>
<tr>
<td>5 December</td>
<td></td>
<td>2008</td>
<td>(C. Nelson)</td>
<td>Revised following feedback from the Steering Group.</td>
</tr>
<tr>
<td>3 July</td>
<td></td>
<td>2009</td>
<td>(C. Nelson)</td>
<td>Minor changes to document style.</td>
</tr>
<tr>
<td>18 May</td>
<td></td>
<td>2011</td>
<td>(C. Nelson)</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.
Policy:  ISP-S17  
Title:  ResNet Acceptable Use Policy  
Status:  Approved  

1. Introduction  
1.1. This information security policy document sets out principles and expectations about acceptable use of networking facilities provided by the University in student residences. It is a sub-document of Information Security Policy (ISP-S1).  
1.2. This document includes statements on:  
   - Student residences network acceptable use policy  

2. Student residences network acceptable use policy  
2.1. The University of Leicester residential networking (ResNet) service is provided by Keycom. The acceptable use policy for this service is available on the Internet here:  
   - http://www.keysurf.net/uolhelp/aup.html  
2.2. Any misuse of the ResNet service may lead to disciplinary action.  

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

Document history:  
22 January 2010 (C. Nelson)  Began first draft.  
07 July 2010 (C. Nelson)  As advised by the Steering Group, removed: “A condition of using the Residential Internet Service provided by the University is that students must comply with both: The acceptable use policy of the network service provider (see above), and University Policy in general, including all applicable aspects Information Security Policy.”  
31 August 2010 (C. Nelson)  The RIS AUP URL was changed from http://www.uolhelp.co.uk/Other/AcceptableUse.aspx to http://www.keysurf.net/uolhelp/aup.html on advice from Frances Stone / Andrew Gahagan in RACS.  
01 Sept 2010 (C. Nelson)  Revisions made as advised by Mark Maynard: replaced references to “RIS” with “ResNet” etc.  
02 Nov 2010 (C. Nelson)  Approved by the Steering Group.  

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.
1. Introduction

1.1. This document gives additional details about implementing the "Physical Security" policy stated in Operations Policy for IT Service Providers (ISP-S6).

2. Building security

2.1. Normal / medium level physical security

- This applies to offices and other locations which house information, information systems or IT equipment and where no sensitive or highly confidential information is stored (in an unencrypted form). It also applies to data and voice network infrastructure housed outside secure computer rooms.

- In general there should at least be one substantial physical security measure in place at all times to protect unattended information assets.

- 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.

- Data and voice network infrastructure housed outside secure computer rooms must be physically secured, e.g. in locked security cabinets.

- Arrangements must be periodically reassessed in terms of performance and ongoing suitability.

2.2. High level physical security

- This applies typically to computer server rooms housing important information systems or communications systems equipment. However, it may also apply to other situations where high value or highly sensitive information in an unencrypted form is being held or handled.

- Physical security to an appropriate higher standard is required. Special requirements to achieve this may involve use of:
  - Intruder detection (burglar alarms)
  - Environmental monitoring and alerting systems
  - Strong rooms
  - Door and window locks
  - Systems to control and log access to sensitive areas
  - Out-of-hours security support
  - Specialised fire extinguishing systems (which may be automatic)
Arrangements must be periodically reassessed in terms of performance and ongoing suitability.

2.3. Departmental managers are responsible for defining to Estates their building security requirements and Estates is responsible for determining the specifics of how to implement those requirements.

2.4. University Staff are obliged to implement or comply with building security arrangements affecting the areas they work in or visit.

2.5. A proper system to manage building access controls must be in place to cover all University buildings. This system is ultimately the responsibility of Estates.

2.6. Where Estates directly manages access controls it must hold accurate data about who is in possession of keys, access cards and access codes.

2.7. Where responsibility for managing access controls is delegated to departments, then Estates must maintain accurate data about what access controls are delegated and to whom.

2.8. 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.

---

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

Document history:

23 March 2007 (C. Nelson) Began first draft.


06 July 2010 (C. Nelson) Steering group advised change to “data and voice communications equipment”; replaced it with “data and voice network infrastructure”.

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.
1. Introduction

1.1. This document gives additional details about implementing the "Reporting Software Faults" policy stated in Operations Policy for IT Service Providers (ISP-S6).

2. Rationale for reporting software faults

2.1. Software faults can interfere with availability and integrity of information. It is clearly desirable that all University software systems perform well, regardless of whether they support teaching, research or administration. Adopting a systematic approach to managing software faults will contribute to achieving the best possible software performance. Software faults on University IT systems must be reported, logged and dealt with in an appropriate way.

3. Reporting software faults

3.1. Where a software fault has been identified, a detailed description of the problem should be reported to, and logged by, someone who is responsible for handling problems relating to the software system in question.

3.2. Individuals, groups or organisations with the University responsible for providing software for others to use, must be prepared to receive, log and deal with fault reports relating to those software systems.

3.3. Software users should be provided with information about what level of support they can expect; preferably this information should be documented and readily available. It is important that those supporting software, or operating a fault logging service, are able to advise software users of the level of support available.

3.4. A person who has logged a software fault should be kept informed, or be able to find out, how management of the fault is progressing. Where it is impossible to rectify a fault, that fact should be logged and the person who reported the fault should be informed.

3.5. It is important that an escalation procedure should be brought into play where a reported fault is serious, e.g. represents a significant security risk, and cannot be rectified immediately. A decision to remove a software system with a severe problem from service may be needed.

3.6. Problems with Central Service software systems supported by IT Services should be reported to the IT Service Desk (email ithelp@le.ac.uk). The IT Service Desk will log details of the fault, manage investigation of the problem and report back to the person that has logged the fault.

3.7. Problems with software systems supported by other individuals, groups or organisations should be directed to those responsible for their administration.

Failure to comply with University Policy may lead to disciplinary action.
Document history:

23 March 2007  (C. Nelson)  Began first draft.
03 July 2009  (C. Nelson)  Minor change.
29 June 2010  (C. Nelson)  Approved by the Steering Group.

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.
1. Introduction

1.1. This document gives additional details about implementing the "Reporting Information Security Incidents" policy stated in Operations Policy for IT Service Providers (ISP-S6).

2. Rationale for centralised reporting of information security issues

2.1. It is important that information security incidents, and suspected information security weaknesses, are reported, logged, then dealt with.

2.2. Information security issues should be reported to IT Services, because IT Services:

- Is responsible for many key University information systems and must be made aware of any potential threat to those systems
- Is the division of the University Administration that specialises in providing IT services and support
- Has overall responsibility for ensuring that University networks connected to JANET are not misused. Most computer equipment used by the University is connected to these networks
- Is empowered to prohibit devices suspected of being compromised, misused or misconfigured, from connection to University networks until the issue is resolved
- Provides services enabling the University to fulfil its statutory obligations in relation to the Data Protection Act
- Will discretely handle any information security issues that are reported

2.3. The result of reporting an issue to IT Services should be that:

- Necessary resources are allocated to investigating and monitoring the issue until it has been resolved. (*The profile of issues logged may inform IT Services’ development decisions.*)
- Where necessary and feasible, measures to counter problems will be implemented as quickly as possible
- Other organisations are advised or consulted about incidents as appropriate, and in particular:
  - Security incidents involving the loss of sensitive or confidential information are to be reported to the Estates Insurance Services Office (x7630 or email insurance@le.ac.uk) and Information Assurance Services (x7946 or informationsecurity@le.ac.uk) as soon as possible
  - Incidents such as fire, flood or theft affecting IT systems are to be reported promptly to both the Estates Security Office (emergencies x888, other calls x2023 or email control@le.ac.uk) and the Estates Insurance Services Office (x7630 or email insurance@le.ac.uk)
Where the cost of recompiling lost data may become the subject of an insurance claim, the Estates Insurance Services Office (x7630 or email insurance@le.ac.uk) is to be informed promptly.

- The relevant Directors of College and Heads of Department are informed by IT Services of the incident where this is appropriate.

3. Reporting information security incidents

3.1. Staff and students must report to IT Services, information security incidents and any suspected security weaknesses found in relation to any University IT-based information systems. This applies to all systems that are used for University business or connected to University networks, whether or not they are administered by IT Services.

3.2. Information system security incidents (suspected or confirmed) relating to University of Leicester computers, data, networks or people should normally be reported to the IT Service Desk (x2253 or ithelp@le.ac.uk). Where the matter to be reported is sensitive or urgent it may be reported to Information Assurance Services (x7946 or informationsecurity@le.ac.uk).

3.3. The details of security issues must be properly logged by IT Services (i.e. who, what where and when). Logs should include a description of the issue, history of actions taken and status of the problem on closure.

3.4. Breaches of security, where serious Staff or student misconduct is suspected, will be reported to the Registrar and Secretary who will decide any further action to be taken.

4. Reporting other types of security incident

4.1. Security incidents not relating to IT, involving suspected or actual breach of University physical security, possible crime, possible theft or violence must be reported to the Estates Security Office (Security Lodge):

- The Estates Security Office is distinct from Information Assurance Services.
- The University Estates Security Office is located in the Security Lodge, Wyggeston Drive, University Entrance No 1.
- Where appropriate the Estates Security Office will contact IT Services regarding any security matters relating to University information systems.
- To contact the Estates Security Office in emergencies the internal phone extension number to call is 888, for other enquiries call extension 2023.
- Where appropriate the Estates Security Office will contact Estates Insurance Services Office Services (using the 24hr contact number as necessary)

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

Document history:

23 March 2007 (C. Nelson) Began first draft.
3 July 2009 (C. Nelson) Minor change.
<table>
<thead>
<tr>
<th>Date</th>
<th>Month</th>
<th>Year</th>
<th>Author</th>
<th>Action/Changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>15 July</td>
<td>2008</td>
<td></td>
<td>C. Nelson</td>
<td>Title changed and instructions on reporting physical incidents to Estates Security Office added as agreed by the Steering Group.</td>
</tr>
<tr>
<td>01 March</td>
<td>2010</td>
<td></td>
<td>C. Nelson</td>
<td>Simplified section 2.3. IT Services will advise or consult other organisations about incidents as necessary or appropriate (which includes the Estates Security Office). Further clarification about reporting other security incidents.</td>
</tr>
<tr>
<td>14 October</td>
<td>2010</td>
<td></td>
<td>C. Nelson</td>
<td>The Estates Insurance Services Office must be informed promptly of: loss of personal data, loss of data for which cost of replacement may become the subject of an insurance claim and fire or flood incidents affecting IT systems.</td>
</tr>
<tr>
<td>02 November</td>
<td>2010</td>
<td></td>
<td>C. Nelson</td>
<td>Some minor changes made as approved by the Steering Group.</td>
</tr>
<tr>
<td>18 May</td>
<td>2011</td>
<td></td>
<td>C. Nelson</td>
<td>Revisions resulting from review within IT Services.</td>
</tr>
<tr>
<td>18 July</td>
<td>2011</td>
<td></td>
<td>C Atkinson</td>
<td>Requirement of ITS to inform Head of Department where appropriate.</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.
1. Introduction

1.1. This document supports implementation of "operational level protection of information assets" as referred to in Information Asset Protection Policy (ISP-S2) and "physical security" as referred to in Operations Policy for IT Service Providers (ISP-S6).

1.2. The term “information asset” is used below to refer to a useful or valuable:
   - Store of information in any format
   - Information processing system of any type
   - Facility used to transfer information

1.3. An approach to conducting a basic information security assessment is outlined below. This is offered as guidance for departments or individuals wishing to ensure that many risks, that commonly affect information assets, are systematically reviewed. (Additional guidance in this area is offered by Information Assurance Services.)

2. Operational protection of information assets and strategic risk management

2.1. It is important to note that the procedure outlined here is not an alternative or replacement for the University’s mandatory strategic risk management policy, which requires each department to establish and maintain its own strategic risk register. The procedure described here supports that strategic risk management process by working at a lower level, helping to identify and assess risks to departmental information assets. Regardless of what leads to significant risks to the business of the department being identified, such risks must be reported to senior management for potential inclusion in the departmental strategic risk register.

3. Methodologies

3.1. Various methodologies can be applied to assessing the risks to information assets. Some approaches are more quantitative whilst others are mainly qualitative. Whilst deploying a good quantitative risk assessment methodology has potential to give the most objective and repeatable results, quantitative methods are rarely used to measure risk in information assets. Reasons for this include difficulty of determining sufficiently accurate input data and poor cost-effectiveness. (Quantitative approaches often revolve around use of specialised software applications.) A simple qualitative approach, based on judgement, best practice and experience, is a practical proposition capable of producing useful results.

4. Risk optimisation

Broad systematic consideration of information security risks with prioritised defensive action is more likely to be cost-effective than implementing measures piecemeal. It is rarely feasible and often not desirable to attempt to reduce risks to zero. This is because there is normally a point at which marginal risk reduction ceases to be cost-effective or would unacceptably hamper a business activity. Availability of resources and "risk appetite" are major factors in determining security levels. Risk management is intended to
tie these factors together by assisting management in determining where to direct resources to achieve acceptable risk levels at an acceptable cost.

5. **Requirements**

5.1. Information security assessment may be undertaken by an individual or a team. However, the team approach is recommended because a broad range of knowledge may be required and group discussions help when weighing up perceived risks. (For convenience the text below will refer only to using a team.)

5.2. The information security assessment team should have access to extensive knowledge of both the departmental information assets to be examined and understanding of the significance of those assets to the business activities of the department and University.

5.3. Senior management approval, support and input is required if security of departmental information assets is to be managed effectively. The assessment team may require special authorisation from management to examine systems and processes in detail. Senior management will also need to review significant findings and make decisions about implementing any challenging or costly security measures.

6. **Selecting and scoping information assets for review**

6.1. The locally managed information assets of most importance to the business activities of the department should normally be prioritised for review. If the assessment team is charged with deciding which assets to focus on then it must first be clear on the context in which it is working. What is important to an individual or small group may not be as important in the wider context.

6.2. It is necessary to judge an appropriate level of granularity at which to work so as not to generate too much or too little detail. It may be possible to group similar assets together so that they can be assessed and treated collectively. In some cases it may be more practical to assess an information system or business activity in its entirety rather than analysing each of its components separately. IT and non-IT asset examples:

   - An IT asset that delivers a particular business function may include locations, power supply, networking, servers, data storage, client PCs, users and administrators.

   - A paper-based information asset may be a processing system involving handling and processing paperwork in several locations, movement of paperwork between locations and the personnel involved.

6.3. The team should ensure there is good common understanding of what each asset does and includes. Details about each asset to be considered should include:

   - Purpose and what it includes
   - Where it is located
   - What information it handles
   - Whether it is used to store personal data about living people
   - Dependence on any other departmentally managed assets or facilities
   - Dependence on any assets or facilities managed outside the department
   - How long it could be unavailable before the situation would become unacceptable
7. Identifying potential risk areas

7.1. A methodical way to identify areas of possible concern is to consider a checklist of threat types in relation to each information asset being assessed. Any areas which may require further consideration should be noted. For a list of common threat types that may impact information assets see:

- Information Asset Security Measures (ISP-I8)

8. Assessing risk levels

8.1. Assessing levels of risks to information assets will almost certainly involve making judgements based on imperfect information. For most scenarios statistical likelihood data will be limited or unavailable and potential impact may also be difficult to estimate. However, identifying significant concerns is of more practical importance than attempting to assign precise risk level values.

8.2. Review and give more detailed consideration to the assets and the applicable threat types that have been noted. If, on further consideration, a specific and relevant risk can be defined, then assess its risk level. Refer to the risk level matrix and descriptions in Appendix 1.

9. Reporting, logging and managing information asset risks

9.1. Risks that have been assessed should be recorded and reported through line management.

9.2. The status of risks should be reviewed regularly by management to decide which of these possible actions is currently appropriate:

- Accept - the risk is to be accepted because it's worth taking or is unavoidable
- Reduce - measures to help reduce threat likelihood or impact are to be taken
- Transfer – responsibility for bearing or mitigating the risk is to be transferred to another individual or organisation
- Escalate - it is an unacceptable risk that must be escalated because it cannot be managed locally

9.3. Risk ownership should be assigned to an individual or group who realistically can be expected to manage the risk and who could take action deemed necessary for adequate mitigation of the risk. Risks that cannot be managed by the current risk owner should be escalated.

9.4. Proposals for risk mitigation measures are to be considered by management, who will consider factors including whether proposals are affordable and justified.

9.5. Where mitigating actions are to be taken, priorities and timescales should also be decided. In addition to a list of threat types, some generic suggestions for mitigation are included in:

- Information Asset Security Measures (ISP-I8)

9.6. Senior management should add risks of strategic significance to the departmental risk register for ongoing management and monitoring.
Appendix 1

Risk level matrix:

<table>
<thead>
<tr>
<th>Impact</th>
<th>Likelihood</th>
<th>Rare</th>
<th>Unlikely</th>
<th>Possible</th>
<th>Likely</th>
<th>Almost Certain</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>Severe</td>
<td>L</td>
<td>M</td>
<td>H</td>
<td>C</td>
<td>C</td>
</tr>
<tr>
<td>4</td>
<td>Major</td>
<td>L</td>
<td>M</td>
<td>L</td>
<td>H</td>
<td>C</td>
</tr>
<tr>
<td>3</td>
<td>Moderate</td>
<td>L</td>
<td>L</td>
<td>M</td>
<td>M</td>
<td>H</td>
</tr>
<tr>
<td>2</td>
<td>Minor</td>
<td>L</td>
<td>L</td>
<td>L</td>
<td>M</td>
<td>M</td>
</tr>
<tr>
<td>1</td>
<td>Insignificant</td>
<td>L</td>
<td>L</td>
<td>L</td>
<td>L</td>
<td>L</td>
</tr>
</tbody>
</table>

Risk level descriptions:

Low (L) This risk can be tolerated, as the necessary mitigating action is already taken on a routine basis, through established local management processes.

Medium (M) This risk can still be tolerated, but some additional mitigating action will need to be implemented, beyond that already taken on a routine basis, and monitored by local managers.

High (H) This risk can only be tolerated if significantly increased and/or additional mitigating action is implemented and closely monitored by senior management.

Critical (C) This risk cannot be tolerated. A detailed and comprehensive action plan will need to be implemented as a matter of urgency, and closely monitored, with the aim of reducing this risk to a lower level.

---

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

---

Document history:

15 August 2007 (C. Nelson) Began first draft.

27 September 2007 (C. Nelson) Began reworking the procedure.
Now outlines an approach instead of including the specifics of the procedure to be used.

Revised.

Minor changes.

Minor change.

Added likelihood timescale to table 1.

Reviewed and approved by Phil Simpkin.

ISP-S2 is renamed “Information Asset Protection Policy”

ISP-I4 is renamed “Managing Information Asset Security”.

Reworked, including harmonising the choice of risk likelihood and impact descriptions with those to be used in departmental risk registers (as specified by the University Governance and Planning section).

Approved, with minor changes, by Neil Cox.

Approved by Phil Simpkin.

Approved by the Steering Group.

Revisions resulting from review within IT Services.

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.
1. Introduction

1.1. This document gives additional details about implementing the "Compliance with legal requirements" policy stated in Compliance Policy (ISP-S3).

1.2. Areas of legislation relevant to information security are summarised below.

1.3. The University makes policy statements and provides explanatory information about legal compliance matters with the intention of helping its members to ensure their legal obligations are not breached though a lack of awareness. (University of Leicester information security policy documentation relating to the law is provided for informational purposes as distinct from being professional legal advice.)

1.4. It is the responsibility of each individual to ensure that they do not break the law. University information security policy regulations, based on legislation, are intended to help students and staff avoid breaking UK laws though lack of awareness.

2. International law and the Internet

Since, at present, there is no international convention on Internet regulation, caution is necessary in considering what law may be applicable. Basic rules:

- all users of Leicester University's computing services must note that although certain materials may be considered legal in their places of origin, that does not prevent the application of UK law if those materials are considered to be illegal under the law in this country

- material transmitted world-wide may be subject to the laws of whichever country it is viewed in

3. Contractual obligations

It is possible to enter into legally binding contracts by email or through a web site.

- Staff should not make any statement or take any action which could be construed as an agreement by the University to enter into a contract unless authorised to do so.

- Staff should ensure their use of email, bulletin boards, and websites is fully compliant with the terms of any confidentiality agreements which may cover aspects of their work from time to time.

4. Cookies and commercial activity

The EC Directive on Privacy and Electronic Communications, and the Privacy and Electronic Communications (EC Directive) Regulations 2003, which came into force in December 2003, places restrictions on sending unsolicited commercial marketing emails, which may include emails promoting University courses or services. The Directive also imposes requirements on the owners of web sites where 'cookies' are used.
• Consent of recipients must be obtained before sending any emails promoting the University’s commercial activities.

Under the Directive, organizations must disclose their information collection practices in their privacy policy, including the information they collect, how they will use or share the information, and the use of cookies or other tracking devices. At points where personal data is being collected, a link to the privacy policy must be provided. Website owners can only use cookies and other tracking devices if EU users:
  • are given clear and comprehensive information about the purpose of website cookies
  • give consent to the use of cookies
  • are offered the chance to refuse these cookies


The Computer Misuse Act 1990 (now amended by the Police and Justice Act 2006) was introduced primarily to deal with computer hacking. It contains three main offences to do with unauthorised acts relating to computers:

• Section 1 contains the basic ‘hacking’ offence of knowingly gaining unauthorised access to any program or data held in a computer.

• Section 2 makes it an offence to commit a Section 1 offence with a view to commit, or facilitate the commission of, a further offence.

• Section 3 contains the offence of doing any knowingly unauthorised act in relation to a computer, with requisite knowledge and intent, that:
  o impairs its operation
  o prevents or hinders access to any program or data
  o impairs the operation of any program or the reliability of data held

Maximum sentences for these offences range from six months imprisonment and/or a £500 fine to ten years imprisonment and/or an unlimited fine.


Copyright is legal protection for an author/creator which restricts the copying of an original work they have created and in the UK it is governed by the Copyright, Designs and Patents Act (1988). Copyright ownership can be transferred, bought and sold but ideas are not subject to copyright, they are covered by patent law.

Copyright works can be written material, dramatic, music, computer programs, web sites, databases, sound recordings, films and broadcasts and protection has varying durations. UK copyright law limits the amount of material that you can legally copy. You can copy a ‘fair’ amount for your own private study, research or critical review, but such copying is restricted to whichever is the greater of:

• Up to 5% or one chapter of a book
• Up to 5% or one article from a single issue of a journal
• Up to 5% or one paper of one set of conference proceedings
• Up to 5% of an anthology or one short story or one poem of not more than 10 pages
• up to 5% or one case of one report of judicial proceedings
Music, films and sound recording are NOT covered by ‘fair’ copying so always look for permission.

Material on the web is still copyright protected so in the absence of clear guidance consider applying the ‘fair’ copying terms above, but bear in mind that such material can be there illegally, for example pirated material. Do not download or link to such material, or use "peer-to-peer" file-sharing software to obtain or share it.

Infringement of copyright by University of Leicester staff and students is taken seriously and further action will be taken.

The University Library provides access to electronic journals, books and databases which are supplied subject to licence agreements with individual publishers. Generally you can download and/or print individual items for personal use but do not download works in their entirety or systematically, for example an entire journal issue.

The making of multiple copies or scanning of printed works for teaching purposes is licensed by the Copyright Licensing Agency (CLA), whilst electronic journal content is subject to separate individual licence agreements held by the University - these may allow you to incorporate parts of a resource in a printed or electronic course pack. Please contact the library for further advice or consult the University’s web pages (see details below) if you are planning to make copies of works available to students.

The libraries web pages (http://www.le.ac.uk/library/about/copyright.html) contain more specific copyright information on:

- Copyright and Studying
- Copyright and Teaching
- Copyright and Research
- Copyright and Printed Course Packs
- Copyright and Scanning under the CLA Licence
- Copyright and University Licences

The University Library may be contacted for further advice:
Email: copyright@le.ac.uk
Tel: 0116 252 2039
Fax: 0116 252 2066

7. Data Protection

The Data Protection Act 1998 regulates the processing of personal data using computers (and/or manual files). ‘Personal data’ means any information relating to a living individual, and ‘processing’ means almost anything done with it, including, for example, storing it. The Act gives rights to those individuals about whom information is recorded and demands good practice in handling information about people.

Subject to a number of exceptions, every person or organisation holding personal data (data controller) must notify the Office of the Information Commissioner. The University Data Protection Officer is responsible for ensuring that the University is registered appropriately for uses of data covered by the Data Protection Act. Any use of personal data by or on
behalf of the University of Leicester which is outside the scope of the University’s notification to the Information Commissioner is illegal. In order to find out whether any proposed use of personal data complies with the University’s registration contact the University’s Data Protection Officer, Mr Colin Atkinson, Assistant Director, IT Services, (Tel - 2412 : ca46@le.ac.uk).

The Data Protection Act 1998 also gives individuals certain rights of access to personal data held about them by others. Any personal data processed by a person at the University, using the resources of the University, will be deemed to be held by the University for the purposes of the Act, unless that person has registered as a Data Controller with the Information Commissioner’s Office (ICO). Therefore personal data processed by any person at the University may have to be made available if an individual applies to the University for access to it.

Persons processing personal data must have the proper authorisation from their Head of Department/Office and must make themselves aware of the general requirements of the Data Protection Act 1998, and in particular must abide by the eight Data Protection Principles as set out in Schedule I of the Act and further explained in Schedules II and III. Copies of the University's current guidance on data protection can be obtained from Heads of Department, the University's Data Protection Officer or the University website.

Any person who wishes to use the University's resources for private purposes such as consultancy or any other activity which is unrelated to their studies or work at the University and who is handling personal data, must have the proper authorisation to do this and must be registered as a 'data controller' with the ICO. This applies, for example, to spin-offs and Associates. It should be noted that any person failing to register with the ICO in such circumstances may be liable to criminal prosecution.

Persons who fail to comply with any Guidance or Code of Practice in force may be held personally liable for any resulting breaches of the Data Protection Act 1998.

In brief:

- Ensure that personal data is: fairly and lawfully obtained; accurate; kept up-to-date; held securely.

- Ensure that personal data is not put onto an Internet site or taken outside of the European Economic Area without:
  - either the consent of the individual concerned
  - or that individual having contractually agreed to the University publishing the personal data

- Ensure that personal data is deleted or destroyed when it is no longer relevant to retain it.

- Ensure that the use of University-related personal data is restricted to the minimum and is consistent with the achievement of academic purposes.
● Only use personal data that is legitimately held by the University for approved University-related purposes.

● Contact the University's Data Protection Officer before conducting any activity which involves the collection, storage or display of personal data through the University's computing services.

● Assume that anything written about someone could be seen by them, since they may be entitled under the Act to have access.

● Requests for access to personal information must all be directed to the Data Protection and Freedom of Information Officer to ensure that they are handled correctly.

● Data subjects, wishing to make requests to the University for information under the Data Protection Act, must follow the instructions in the "Data Protection and Freedom of Information Request Pack" which is available via the University website.

8. Freedom of Information

Under the Freedom of Information Act 2000, a public body is obliged, subject to limited exceptions, to disclose information following receipt of a request made in accordance with the Act. These points must be noted:

● Non-routine requests for access to University information must all be directed to the Data Protection and Freedom of Information Officer to ensure that they are handled correctly.

● Those making non-routine requests for University information must following the instructions in the "Data Protection and Freedom of Information Request Pack" which is available via the University website.

● Members of the University should be aware that emails and any other documents may be subject to the requirement to be disclosed under the Freedom of Information Act.


The Official Secrets Acts 1911-1989 establish severe criminal penalties for any person who discloses any material which relates to security, intelligence, defence or international relations and which has come into that person's possession through an unauthorised disclosure by a Crown Servant or Government contractor. They also cover material which has been legitimately disclosed by a Crown Servant or Government contractor on terms requiring it to be kept confidential or in circumstances in which it might reasonably be expected to be treated as confidential. This means that certain information handled by the University's departments may be covered by the provisions of the Acts, particularly if such information concerns a project specifically commissioned by a Government office.

● Staff must ensure that any information subject to the Official Secrets Act is securely stored and avoid displaying it on the University's computing services.
10. Defamation

Defamation consists of the publication of opinions and untrue statements which adversely affect the reputation of a person or a group of persons. If such a statement is published in a permanent form, as is the case with statements published on the Internet, including messages transmitted by e-mail, an action for libel may be brought against those responsible.

In accordance with the **Defamation Act 1996**, the University acknowledges the convention of academic freedom, but will take all reasonable care to avoid the dissemination of defamatory material and will act promptly to remove any such material which comes to its attention. Messages which have only one intended recipient may reach a vast audience through the Internet who may be able to take action in a number of different countries and as a result, the transmission of statements which discredit an identifiable individual or organisation may lead to substantial financial penalties.

University members must:

- ensure that all published facts are accurate
- ensure that opinions and views expressed on web pages or via bulletin boards do not discredit their subjects in any way which could damage their reputation
- REMEMBER THAT E-MAIL COMMUNICATIONS ARE PUBLICATIONS

University members must not:

- place links to bulletin boards or other websites which are likely to publish defamatory materials

11. Obscenity

The University is committed to the prevention of publication through any of the University's computing services of any material which it may consider pornographic, excessively violent or which comes within the relevant provisions of the **Obscene Publications Act 1959**, the **Protection of Children Act 1978**, the **Telecommunications Act 1984** or the **Criminal Justice Act 1988**. The University will regard any such publications as a very serious matter which it will not hesitate to report to the police. In addition, under the **Communications Act 2003** a person may be guilty of an offence if they send or cause to be sent by means of a public electronic communications network a message or other matter that is offensive or of indecent or menacing character.

Users of the computing services are reminded that these are principally for use in connection with academic purposes, therefore any use of the computing services to publish or gain access to obscene, pornographic or excessively violent material is inappropriate.

- University members must not disseminate, access or encourage access to materials which the University deems to be obscene, pornographic or excessively violent through the University's computing services.
12. Discrimination

The **Sex Discrimination Act 1975**, the **Race Relations Act 1976** and the **Disability Discrimination Act 1995**, the **Employment Equality (Religion or Belief) Regulations 2003**, the **Employment Equality (Sexual Orientation) Regulations 2003** and the **Employment Equality (Age) Regulations 2006** are guided by the principle of prevention of unfair discrimination on the grounds of sex, including discrimination against persons who have undergone gender reassignment, race or disability, religion and/or belief, sexual orientation and age. The Acts impose civil liability for unlawful discrimination, and in certain other circumstances the law is supported by criminal sanctions.

The University has a wider proactive duty including the need to actively eliminate unlawful discrimination and promote equality of opportunity under **The Race Relations (Amendment) Act 2000**, **The Disability Discrimination Act 2005** and **The Equality Act 2006**. These Acts impose a number of general and specific duties on the University including the need to set out in a document how it intends to meet these general and specific duties. The University has hitherto fulfilled its duty under these Acts through the publication of a Race Policy, a Disability Equality Scheme and Gender Equality Scheme. It is now consulting on a new Single Equality Scheme to replace those documents and extend the reach of such proactive treatment to include the equality strands of sexual orientation, religion and/or belief and age. It is anticipated that new future legislation will require such an extension of cover.

Harassment of an individual may result in both criminal and civil sanctions under the **Protection from Harassment Act 1997** and the **Crime and Disorder Act 1998**. Such harassment can be through emails, bulletin board postings or websites. Therefore, any material located on or disseminated through the University's computing services which is considered discriminatory or may encourage discrimination on grounds of sex, gender, race, colour ethnic or national origins, religious belief, sexual orientation or disability, or which constitutes harassment may be unlawful. Any such material will also be against the University's Equal Opportunities Policy. It is also a criminal offence to incite racial hatred under the **Public Order Act 1986**.

Under the **Disability Discrimination Act 1995**, there is a general obligation on service providers to take all reasonable steps to ensure that it is not impossible or unreasonably difficult for a disabled person to use their services. This duty applies to University Websites which are accessible by the public or members of the University who may have a visual disability. People who are blind use speech synthesis software to read aloud the content of a Web page. University Web content publishers should endeavour to ensure that content can be accessed in this way by always using alternative text to describe an image or non-text element.

With the implementation of the **Special Educational Needs and Disability Act 2001 (SENDA)**, from September 2002, it is now a legal requirement to take steps to ensure Web sites are accessible to disabled people. SENDA was introduced to include educational establishments that were previously exempt from the Disability Discrimination Act (1995). SENDA requires the University to ensure that information on Websites is accessible to everyone and we have an obligation to make 'reasonable adjustments' in order to achieve this. Where information cannot be accessed by a disabled person an alternative form of provision must be provided so as not to disadvantage the person concerned.
The W3C (World Wide Web Consortium) has produced the **Web Content Accessibility Guidelines**. These explain in detail what is needed to do to allow as wide an audience as possible view a Web site.

Questions or problems with checking or adjusting the accessibility University of Leicester Websites may be directed to the CWIS Officer at cwis@le.ac.uk.

University members must:

- not use the University's computing services to place or disseminate materials which discriminate or encourage discrimination on grounds of sex, gender, race, colour, ethnic or national origins, religious belief, sexual orientation or disability, or which are or might be considered to be harassment of one or more individuals

- take all reasonable steps to ensure that web sites providing access to services are not impossible or unreasonably difficult for disabled persons to use

13. Incitement to crime

The incitement to commit a crime is a criminal offence in itself, regardless of whether a crime has actually been committed or not. This includes the provision of information via computerised services which facilitates any of the activities which this code has highlighted as criminal offences.

University members must not:

- place links to sites which facilitate illegal or improper use

- place links to sites where copyright protected works, such as computer software, are unlawfully distributed

- place links to sites which display pornographic materials

- place links to bulletin boards or websites which are likely to contain discriminatory statements

14. Terrorism Act 2000

An attack on any electronic systems can be classed as an act of terrorism as well as a criminal office. What constitutes an attack within the scope of the Act includes hacking websites or blocking websites, with a political agenda or public intimidation in mind.

- University members must not participate in any form of interference or disruption of an electronic system.

15. Interception of communications and monitoring

The **Regulation of Investigatory Powers Act 2000** makes provision for and about the interception of communications, the acquisition and disclosure of data relating to communications, the carrying out of surveillance, the use of covert human intelligence sources and the acquisition of the means by which electronic data protected by encryption or
passwords may be decrypted or accessed; to provide for Commissioners and a tribunal with functions and jurisdiction in relation to those matters, to entries on and interferences with property or with wireless telegraphy and to the carrying out of their functions by the Security Service, the Secret Intelligence Service and the Government Communications Headquarters; and for connected purposes.

- Note: any interception of communications and monitoring undertaken by the University must comply with The Regulation of Investigatory Powers Act 2000.


The Act incorporates rights and freedoms guaranteed by the European Convention and safeguards human rights including, but not limited to freedom on expression, freedom of thought, conscience and religion. It also impinges on Data Protection Act and e-monitoring legislation.

---

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

---

**Document history:**

<table>
<thead>
<tr>
<th>Date</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>16 October 2007</td>
<td>Began first draft.</td>
</tr>
<tr>
<td>29 January 2009</td>
<td>Revised according to recommendations from the Steering Group. (Input from the Library about Copyright and from Personnel Services about Discrimination.)</td>
</tr>
<tr>
<td>13 February 2009</td>
<td>Data Protection - added University publishing specific personal data in accordance with contractual agreement.</td>
</tr>
<tr>
<td>3 July 2009</td>
<td>Minor change.</td>
</tr>
<tr>
<td>18 May 2011</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.
1. Introduction

1.1. This document describes policy relating to how the University may monitor usage of its IT systems (including University Mobile Phones) and the circumstances in which it may access user information on its systems and networks that is normally private. It gives additional details about implementing the "Compliance with the University's own information security standards" policy stated in Compliance Policy (ISP-S3).

2. Institutional IT system usage monitoring and access to accounts

2.1. 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.

3. General monitoring and access policy


3.2. Where undertaken on behalf of the University, access and monitoring must be:

- For legitimate business reasons.
- Justifiable, fair and proportionate.
- Done with the minimum possible intrusion and disruption to both the subject and any third parties involved.

3.3. Information on University IT equipment and networks, including mobile phones, may be examined on behalf of the University by authorised persons to:

- Support detection or prevention activities that are in breach of University policy.
- Comply with legislation.
- Support detection or prevention of activities that are illegal.
- Defend against attacks against its systems or data.
- Identify or investigate an operational problem or monitor for correct operation.
- Investigate suspected unauthorised access to or use of systems.
- Perform monitoring or support activities with consent of the subject.

3.4. Monitoring of particular University information systems and access to data in user accounts may only be undertaken by specific members of staff as a recognised part of their normal duties and with management approval.

3.5. Unapproved information system monitoring or access is a breach of University regulations and may also be illegal; such activities may therefore lead to disciplinary or legal action.
3.6. Any information collected must be handled securely, treated as confidential and only revealed to or examined by those authorised.

3.7. Any information collected must only be retained for the period deemed necessary for the specific purpose for which it was collected.

3.8. Where a crime is to be investigated, that investigation must be left to the Police and their instructions must be followed relating to identifying, seizing and preserving any digital evidence.

4. **Routine monitoring**

4.1. The University undertakes limited monitoring of the activities of students, staff and others for compliance with information security policies and other University regulations. In agreeing to abide by the University information security policies, members of the University are advised that user-specific information may be routinely monitored by authorised staff with respect to:

- Login and logout events and locations.
- System resource usage.
- Software usage.
- Software auditing to support compliance.
- Network bandwidth usage.
- Network bandwidth usage and traffic patterns.
- Power consumption.
- Detection of email spam.
- Detecting security vulnerabilities.
- Identifying and controlling security threats.
- Serving inappropriate content, which may include material which is obscene, violent, illegal, damaging to the University or otherwise in breach of University policy.

4.2. Other than automated monitoring as described in 4.3 below, routine monitoring does not include examining the contents of files and communications for any purpose which has not been previously approved as a requirement of legitimate University business.

4.3. Use of automated systems which scan user files and communications for an approved purpose is permitted.

4.4. Those with elevated access privileges, such as IT system and network administrators, are not entitled, simply by virtue of having those privileges, to examine the contents of user files and communications on the systems they have access to.

5. **Monitoring and access in special circumstances**

5.1. In special circumstances authorised University staff may access and examine the content of any data stored in, or being transmitted by, University information systems. This includes examining the content of data files and communications which should otherwise be treated as confidential and therefore goes beyond what is permitted in routine monitoring. When this takes place full details of the specific authorisation and investigation
must be recorded and the records must be securely retained by the institution for an appropriate period. This will be undertaken where:

5.1.1. The Registrar considers there are reasonable grounds to suspect a specific breach of University regulations or the terms of an employment contract which justify access. (Departments wishing to access the confidential data belonging to a member of the University should make their request to the Registrar via Information Assurance Services.) This examination of data, in exceptional circumstances, may be undertaken whether or not consent is given. However; normally consent should first be requested, except where this is inappropriate because of circumstances or inadvisable because of the nature of the suspected breach.

5.1.2. The Registrar has agreed to respond to a request from a non-institutional body for information which may otherwise be subject of a court order.

5.1.3. The University is required by virtue of a Court Order or other competent authority to provide information in relation to taxation, detection and prevention of a specified crime or national security. The Registrar must be made aware of any such orders.

5.1.4. Access to a personal computer account belonging to an absent member of the University is necessary, however:

- It should not be done if it can reasonably be avoided.
- It should be done only for University business purposes and limited in scope to achieving only the purpose specified in advance.
- If appropriate, the account holder must be contacted and consent sought for access to the specific information required. Wherever possible consent should be sought and obtained in writing (email will suffice) and a record kept of the correspondence.
- Where consent is not or cannot be obtained, then written permission to access the account must be sought from the University Data Protection Officer who will specify the procedure to follow. Should the University Data Protection Officer not be available then the Registrar must be contacted.
- The Data Protection Officer or, where involved, the Registrar may require that someone supervise access to the account of the absent person.
- Accounts to which temporary access has been granted by a password change should be locked as soon as access is no longer needed.

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

**Document history:**

7 November 2007  (C. Nelson)  Began first draft.

5 December 2008  (C. Nelson)  Requests to Registrar for data access to go via ISO.

13 February 2009 (C. Nelson) 4.1/4.2 modified.

3 July 2009 (C. Nelson) Minor change.

8 March 2009 (C. Nelson) Clarify that scope includes University mobile phones.

18 May 2011 (C. Nelson) Revisions resulting from review within IT Services.

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.
1. Introduction

1.1. This document gives additional details about implementing the policies stated in Cryptography Policy (ISP-S16). How use of encryption will be supported, facilities available and some guidance for computer support staff is outlined below.

1.2. IT Services will work with departmental computing staff to assist members of the University that have a requirement to use encryption in their work. An explanation of where using cryptography is required, or may be appropriate, is given in “Cryptography Policy (ISP-S16)”.

1.3. Specific details are to be made available, e.g. via the Web, of currently recommended encryption solutions and whether they are supported by IT Services or within departments.

1.4. It will be practical for computing staff to support a limited range of encryption solutions. However; other encryption solutions that meet all necessary requirements may be used.

1.5. The encryption technology to be used for a particular purpose must comply with requirements of an external body where applicable, and at least be deemed suitable by the University.

1.6. Minimum cryptography standards suitable for general University use, at the time of writing, are outlined in this document. (This document should be revised periodically.)

2. Encryption of data in general

2.1. Where it is required to encrypt personal or sensitive data, encryption must be:

- Either to the standard specified in an agreement between the University and an external organisation relating to the data in question or,
- Where another organisation has not specified any encryption requirements the data must be secured to at least minimum University standards as specified below.

2.2. Before an agreement is made with an external organisation that specifies use of encryption, it must be ascertained whether it is feasible to implement the encryption standards demanded.

2.3. Advice and assistance in the use of encryption is offered by the IT Services department. IT Services will support use of a limited range of encryption solutions that:

- Equal or exceed the minimum standards indicated below and,
- Where possible, equal or exceed typical requirements currently being specified for handling data from external organisations.

2.4. To ensure that locally stored data can be recovered in the event of a computer problem, such as a hard disk failure, it is vital that recoverable backups are maintained. Use of encryption does affect the need for backups; if anything it makes them more important because it is likely to remove the chance of recovering any data from a failed system.
2.5. Where encryption is used careful management of recovery keys and passwords is essential, see also Management of encryption keys in Cryptography Policy (ISP-S16).

3. Encrypting email

3.1. Unless information sent by email is encrypted before sending, its confidentiality should not be assumed. This applies to email either sent within the University or between the University and another organisation. (The University email system may encrypt its network communications with an email system at another site, provided the remote email server is also configured to support encryption. Although this type of encryption reduces opportunities for eavesdropping it does not guarantee that the content of an email message could only be seen by the intended recipient.)

3.2. Whilst unencrypted (plain text) email messaging is adequate for general purpose communications, there may be occasions where it is necessary or prudent to use encryption. There may, for example, be a requirement to use encryption when communicating by email with certain other organisations.

3.3. Where it is necessary to send encrypted information by email the current recommendation is to send it as an encrypted attachment. The attached file should be first encrypted using a suitable tool (see “Encrypting Microsoft Office documents” and “Encrypting files and folders” below).

4. Encrypting Microsoft Office documents

4.1. The encryption option built into Office 2007 uses a strong algorithm, AES 128-bit, by default. This is suitable for official University purposes; however, other organisations may require use of even stronger algorithms when working with their data.

4.2. Encrypted files created using Office 2007 may be decrypted using Office 2003 using the Office 2007 Compatibility Pack (which can be downloaded from Microsoft’s website).

4.3. Do not rely on the strength of the encryption features in Microsoft Office software previous to Office 2007.

4.4. Brute force is currently considered the only way to break into encrypted Office 2007 documents. Therefore to ensure security, difficult to guess passwords must be used. Use passwords that combine uppercase and lowercase letters, numbers, and symbols. Passwords should be 8 or more characters in length. A pass phrase that uses 14 or more characters is safer.

4.5. Neither IT Services nor Microsoft can recover encrypted Office 2007 documents or forgotten passwords.

5. Encrypting files and folders

5.1. There may be a requirement to encrypt a single file or a collection of files and folders. This may be useful where the encrypted data is to be sent as an email attachment, burnt onto CD/DVD for posting etc.

5.2. 7-Zip is a free open source file compression and archiving program that features optional password protection for the archive files that it creates (in 7z or ZIP formats). When a password is set the data in the archive is encrypted using a strong algorithm (AES-256). Provided strong passwords are used this software is suitable for encrypting files and folders. (Note that 7-Zip does not encrypt data unless a password is specified when creating an archive file.)

6. Encrypting whole disk drives
6.1. “Whole disk encryption” will be the most satisfactory encryption solution for many users of portable devices who regularly deal with personal data. (In some cases, use of whole disk encryption may be stipulated by suppliers of the data being handled.)

6.2. Manually keeping track of whether there are unencrypted copies of sensitive files on a system is prone to oversight. There is normally no need, however, for a user to explicitly manage encryption of specific files and folders when they reside on an encrypted disk; everything on the disk is always encrypted. However; it should be noted that file level encryption may be needed, in addition to whole disk encryption, to secure documents against access by other authorised users of the computer (particularly anyone with administrator privilege).

6.3. Any new device purchased by the University that features a disk drive may sooner or later be used to store confidential data. Where such purchases are being made, the possible need to use whole disk encryption should therefore be carefully considered. Whole disk encryption can be achieved using hardware or software based solutions.

6.4. Existing disk drives in certain devices, including Windows laptops and some PDAs, may be protected by installing whole disk encryption software. Encryption software is installed after the operating system, and can be installed to a system that has already been in use with applications and data.

6.5. Beware that when using whole disk encryption solutions, data copied to local media such as CD may not be encrypted – see also “Encrypted USB drives DVDs/CDs etc.” below.

6.6. Disk drives with built-in encryption

- Internal and external hard drives incorporating encryption technology are now available. These have the benefit of placing minimal processing load on the CPU and do not require installation of separate encryption software.
- Use of hard drives with built-in encryption is likely to become commonplace; however, at the time of writing this document, few laptop suppliers offer supported models incorporating internal hardware encrypted drives. Staff contemplating new laptop purchases should, nevertheless, consider this option and if necessary consult suppliers and computing staff for the latest advice.
- Where a hardware encrypted drive is to be used to store personal or sensitive data provided by another organisation, it should be established whether the encryption provided meets the standards stipulated by that organisation.

6.7. Whole disk encryption software

- Whole disk encryption software encrypts disk partitions. Solutions typically encrypt the operating system drive and use “pre-boot authentication”, so completely preventing unauthorised use of the computer, tampering or access to its data. (Some solutions may also be able to encrypt other drives or create virtual encrypted disks within files.)
- IT Services will recommend a limited range of software whole disk encryption packages for which it is able offer some support. Contact IT Services for the latest information.
- Vista Enterprise version operating system can be installed and configured to use BitLocker encryption on the entire C: drive of a PC or laptop. This has some impact on performance and it is preferable, though not essential, to have a PC with a Trusted Platform Module (TPM) hardware chip, version 1.2 or better. BitLocker has not yet been evaluated by IT Services and support may not be
offered. (Since this option requires use of Vista and installing the operating system from scratch it is anticipated that other more flexible software based whole disk encryption solutions will be preferred.)

- Where a software encrypted drive is to be used to store personal or sensitive data provided by another organisation, it should be established whether the encryption provided meets the standards stipulated by that organisation.

7. Encrypted USB drives DVDs/CDs etc.

7.1. Encryption of data on portable storage devices or media may be a requirement, where it is the subject of an agreement, or may be highly advisable. Where such devices are to contain confidential data an assessment must be made of the likelihood and implications of the data being lost, stolen or accessed by the “wrong person”.

7.2. Options for encrypting data on portable storage devices include:

- Using a device with built-in encryption. External hard drives and flash drives are available with built in encryption. Access to such drives may typically be controlled by one or two factor authentication (e.g. password and fingerprint). Contact IT Services for the latest information about any recommendations in this area.
- Encrypting files before they are copied or written to the device e.g. using a program such as 7-Zip.
- Using a software application installed on the local system that is designed to encrypt data automatically as it is written to an external storage device. Suppliers of whole disk encryption software typically also offer such software. Subject to demand and satisfactory evaluation, IT Services may provide support for a limited range of such software. Contact IT Services for the latest information.

8. Encrypted backups and archives

8.1. There must be an assessment of the need to encrypt backup or archive media. It should take into account sensitivity or value of the data, and the physical and technical protections in place. This is particularly important if the media is sent or held offsite.

8.2. If encrypted backups are created, key management is particularly important. It must be possible for keys to be readily found in a disaster recovery situation.

8.3. Where encrypted media is archived the keys must also be separately and securely archived to ensure that the media remains usable.

8.4. Beware that when using whole disk encryption solutions, data backed up to local media or remote storage will not necessarily be encrypted – see also “Encrypted USB drives DVDs/CDs etc.” above.

9. Encrypted databases

9.1. Where databases hold very sensitive information then an assessment should be undertaken of the risk of unauthorised access to the data whilst in storage or in transit between the database server and any applications which access the data. It may be that additional encryption measures would be needed to secure the data in storage or network transit.

10. Minimum cryptography requirements for University data

10.1. This section is primarily intended for computer support staff involved in selecting or configuring encryption solutions. It gives a summary of cryptography standards considered suitable for use in the University in situations where more specific
requirements do not apply. (Acceptable standards may change over time and this document should be periodically revised to take that into account.)

10.2. Symmetric ciphers with key lengths of at least 128 bits. (Symmetric ciphers use the same key to encrypt and decrypt the data.) The following symmetric block ciphers, in which a block of plain text is encrypted to produce a block of text the same length, are suitable for University use:

- AES (Advanced Encryption Standard). Key size of 128 bits or more should be used. This is the preferred block cipher.
- Triple-DES (or 3DES). Data is encrypted three times using three 64 bit keys.
- Blowfish with at least 256 bit key size.

10.3. The following symmetric stream ciphers, in which a digital data stream is encrypted one bit or byte at a time, are suitable for University use where a better alternative is unavailable:

- Rivest Cipher 4 (RC4) with key length at least 128 bits. Where poorly implemented RC4 may be vulnerable to attack and it is recommended to migrate to AES/3DES block ciphers if possible.

10.4. Asymmetric ciphers with strength considered comparable or better than a 128 bit key symmetric cipher. (Asymmetric ciphers are used in public key cryptography. Two keys are used: public and private. The private key is kept securely and the public key is published.)

- RSA with 1024 bit composite modulus

10.5. Use of industry standard "key agreement" or "key exchange" methods. (In key agreement two or more parties to agree upon the same key value to use without the need for a previously-established shared secret. In key exchange the key to be exchanged is encrypted with the recipient’s public key. The recipient can decode the exchanged key by using their private key.) Suitable algorithms include:

- Diffie-Hellman with 1024 bit prime and 160 bit generator - for key agreement
- RSA with 1024 bit composite modulus - for key exchange
- Elliptical Curve Diffie-Hellman (ECDH) - for key exchange

10.6. Use of industry standard digital signing. (A digital signature is a hash value encrypted with the sender’s private key.) Suitable cryptographic primitives for use in digital signing used by the University include:

- DSS with 1024 bit prime and 160 bit long term private key
- RSA with 1024 bit composite modulus
- Elliptic Curve Digital Signature Algorithm (ECDSA)

10.7. Where University data is to be encrypted for network transmission, especially to wrap any clear text protocol or service not encrypted by another method, the cryptography requirements are:

- SSLv3
- TLSv1
- SSH2
- Kerberos
- pcAnywhere
• PGP
• Terminal Services
• IPSec

10.8. Hashing algorithms take a variable length input and produce a fixed length output. The output value is known as a “message digest” or “hash value”. Basic requirements of hashing algorithms are:

• The output of the algorithm must not be invertible i.e. the operation must be one-way.
• The algorithm must also be highly collision resistant, i.e. the chance that distinct inputs will produce the same hash value must be extremely small.

10.9. Use of a one-way hash function to irreversibly encrypt data should be used for:

• Authentication information e.g. passwords.
• Integrity checksums e.g. as a tamper-evident seal for a file.
• Digital signatures (used with asymmetric algorithms).

10.10. These cryptographic hashing algorithms are suitable for use by the University:

• SHA-256
• SHA-512
• Whirlpool
• RIPEMD-160

10.11. Use of the following cryptographic hashing algorithms is not recommended. These should be phased out in due course because of proven vulnerability to collision attacks:

• SHA-1
• MD5

10.12. (H)MAC – (Hashed) Message Authentication Code is used to provide a means of data integrity and origin authentication. A secret key shared between the sender and recipient is concatenated with the message and the result is put through a hashing algorithm (possibly one of those mentioned above). It is possible for the recipient to be sure where the message came from and that it has not been intercepted and modified. HMAC is utilised within various cryptographic protocols including TLS and IPsec. The following documents are considered to describe suitable HMAC implementations and standards:

• HMAC FIPS 198
• HMAC RFC 2104

---

Failure to comply with University Policy may lead to disciplinary action.
Document history:

<table>
<thead>
<tr>
<th>Date</th>
<th>Month</th>
<th>Year</th>
<th>Author</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>5 November</td>
<td></td>
<td>2008</td>
<td>G. Hamp</td>
<td>Minor changes made.</td>
</tr>
<tr>
<td>9 December</td>
<td></td>
<td>2008</td>
<td>C. Nelson</td>
<td>Revised following feedback from the Steering Group.</td>
</tr>
<tr>
<td>29 January</td>
<td></td>
<td>2010</td>
<td>C. Nelson</td>
<td>Removed reference to Outlook email signing and encryption support by IT Services.</td>
</tr>
<tr>
<td>18 May</td>
<td></td>
<td>2011</td>
<td>C. Nelson</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.
1. Introduction

1.1. This document supports “operational level” protection of information assets and is provided to assist the process outlined in Managing Information Asset Security (ISP-I4).

1.2. A basic operational level information asset security review may be undertaken by carefully considering a checklist of well known threat types in order to prompt identification of any specific concerns. Such a checklist is provided in section 2 below.

1.3. The University has developed mandatory requirements, for both “strategic level” risk management and business continuity planning, that must be implemented across all departments, under a project administered by the Governance Section in the Division of Student and Academic Services. Managing information security risks at the lower operational level, as described in Managing Information Asset Security (ISP-I4), can complement and provide input to these mandatory higher level management processes.

1.4. Departmental strategic risk registers must be maintained in accordance with the University’s strategic risk management procedures. It is appropriate that when significant risks to important information assets are identified, they should be reported to departmental senior management for recording in this risk register.

1.5. For further information about strategic risk management and business continuity planning refer to the University of Leicester business continuity planning procedures (contact the Governance Section).

1.6. This document is for guidance:

- It recognises that the reader and those undertaking an information security review will not necessarily be authorised or able to implement all necessary countermeasures themselves.

- It is not suggested that the typical countermeasures listed in section 2 below will necessarily be appropriate or feasible to implement in all cases. *(Determining an appropriate combination of risk control measures to protect an information asset must take into account numerous factors, especially its importance to the business. Deciding whether to implement a specific security measure should involve assessing its relevance, feasibility, and estimated cost-effectiveness.)*

- It is assumed, however, that security review of an information asset would realistically be entrusted to a team with access to sufficient knowledge about the asset. *(Lack of resources to undertake such a review may reasonably be considered a risk in itself.)*
2. Threat types and typical countermeasures

2.1. A range of threat types, that commonly affect information assets, are listed below with some typical countermeasures. Each threat listed in the table below has been roughly classified as "Physical", "Administrative", "IT Specific" or "Miscellaneous" according to its dominant characteristic.

<table>
<thead>
<tr>
<th>Physical</th>
<th>Threat Types</th>
<th>Typical Countermeasures</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Is any part of the asset particularly vulnerable to accidental damage or vandalism with serious consequences?</td>
<td>Physically protect the information asset. Manage risks created by building/maintenance work. Minimise access to where the asset is located.</td>
</tr>
<tr>
<td></td>
<td>Could destruction of a particular room or building, e.g. by fire, result in the asset effectively being unrecoverable?</td>
<td>Deploy fire alarms and suitable extinguishing systems. Review contingency arrangements or business continuity plans.</td>
</tr>
<tr>
<td></td>
<td>Is it likely that an intruder could gain physical access to the asset and cause a serious problem, e.g. by theft, damage, access to sensitive data etc?</td>
<td>Limit physical access only to trusted people. Enhance physical security: building access management, locks, alarms, security staff cover etc.</td>
</tr>
<tr>
<td></td>
<td>Does degradation resulting from age or environmental conditions such as heat, damp, pollution, light (or damage by rodents) seem likely to lead to a serious problem? This may be significant to equipment, cables or archived media including CDs/DVDs.</td>
<td>Improve or provide protection against adverse environmental conditions. Ensure that media to be stored long term is not prone to degradation over that period and is stored in accordance with suppliers recommendations.</td>
</tr>
<tr>
<td></td>
<td>Is any part of the asset located where water damage caused by flooding, burst pipes, pressure washing etc. seems a realistic possibility, and if it happened would the consequences be serious?</td>
<td>Relocate the asset. Consult Estates. Review contingency arrangements or business continuity plans. Precautionary water protection.</td>
</tr>
<tr>
<td>Administrative</td>
<td></td>
<td></td>
</tr>
<tr>
<td>----------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Threat Types</strong></td>
<td><strong>Typical Countermeasures</strong></td>
<td></td>
</tr>
</tbody>
</table>
| Is sensitive or personal data being handled in a way that would make it easy for it to fall into the wrong hands causing damage to reputation, e.g. left unattended on a desk, sent through the post on a CD/DVD, stored on a home PC, laptop in a public place etc? | Communicate correct information handling procedures to follow. 
Advise staff of University policy on information handling. 
Ensure that confidential information is protected. This may include managing physical security of information, encryption of digital information etc. |
| Are staff, handling important information, unaware of its importance or unaware of any procedures that must be followed to help prevent loss, corruption or disclosure? | Make staff aware; if personal data is being handled ensure staff have attended DP awareness training. 
Communicate correct information handling procedures to follow. 
Advise staff of University policy on information handling. |
| Does it seem likely that a shortage of sufficiently trained or experienced staff could seriously limit the performance or ongoing viability of the asset during the coming year? | Review and revise allocation of staff effort and staffing level. 
Additional staff training. 
Consider transferring provision of services provided by the asset elsewhere. |
<p>| Is there evidence that the asset in question is being used for any illegal activities? | Immediate actions and or ongoing countermeasures will vary depending on the nature of the activity. <em>(If in doubt report and seek advice.)</em> |</p>
<table>
<thead>
<tr>
<th>IT Specific</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Threat Types</strong></td>
</tr>
<tr>
<td>Does the possibility that someone may gain access to the system using false credentials, e.g. borrowed or stolen from another person, represent a particularly significant and serious risk for the asset in question?</td>
</tr>
<tr>
<td>Is the asset entirely reliant on an air conditioning system for correct operation and is there no contingency in case of failure of the air conditioning?</td>
</tr>
<tr>
<td>Is the possibility of a hacking incident badly affecting the asset of serious concern, taking into account existing countermeasures?</td>
</tr>
<tr>
<td>Is the use of elevated privileges, e.g. by users unaware or unconcerned about security, significantly increasing the chance that the asset will be compromised?</td>
</tr>
<tr>
<td>Is delegation of privileged access to the asset poorly controlled such that it is either not known who has such privileges or that people have greater privileges than they need?</td>
</tr>
<tr>
<td>Question</td>
</tr>
<tr>
<td>-------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Does infection of the asset by computer worm, virus or Trojan leading to serious problems seem likely taking into account existing countermeasures?</td>
</tr>
<tr>
<td>Taking into account existing security and recovery measures, does the possibility of data stored by the asset being corrupted, destroyed or stolen seem to warrant any further technical security measures?</td>
</tr>
<tr>
<td>If the asset features use of data encryption, do you have any concerns about the security, location or availability of the encryption key?</td>
</tr>
<tr>
<td>Is any of the IT equipment that is part of the asset particularly vulnerable to theft or other types of interference as a result of not being physically secured?</td>
</tr>
<tr>
<td>If the asset makes use of a network service provided by another organisation, is there any significant likelihood that problems with that service may occur resulting in a serious problem?</td>
</tr>
<tr>
<td>Is it likely that the time needed to replace any critical hardware would cause an unacceptably long recovery time?</td>
</tr>
<tr>
<td>Is there reason to suspect that any of the IT hardware that the asset relies on is particularly prone to failure and that such a failure would have a serious impact?</td>
</tr>
<tr>
<td>Question</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Can it be predicted that the asset will be incapable of delivering the necessary performance level, with serious consequences, at any time in the coming year as a result of inadequate specification?</td>
</tr>
<tr>
<td>Is there insufficient documentation about how the asset is designed or configured to support a rebuild?</td>
</tr>
<tr>
<td>Is there a lack of accessible knowledge, which may include an external source of support no longer available, about how the asset is designed or configured to support a rebuild?</td>
</tr>
<tr>
<td>It there any documentation that may be important to operating or recovering the asset which is not stored securely in at least two locations?</td>
</tr>
<tr>
<td>Are operating system patches or software upgrades applied to systems of critical importance without prior testing on non-critical systems?</td>
</tr>
<tr>
<td>Are you aware of any resources that could readily be misused resulting in serious consequences, e.g. disk space etc?</td>
</tr>
<tr>
<td>Does the asset feature any application known to potentially provide users with inappropriate levels of access to data?</td>
</tr>
<tr>
<td>Are there concerns that data and system recovery procedures, such as restore from tape etc., for the asset are unproven and therefore may not work as expected if required?</td>
</tr>
<tr>
<td>Question</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Is there any doubt about accessibility or availability of any software media and enabling keys that might be needed during a recovery?</td>
</tr>
</tbody>
</table>
| Are backups inadequate in terms of: what is backed up, frequency of backup, capability or reliability of backup system, storage of backup media in safe alternative and preferably fireproof location? | Review backup coverage.  
Revise frequency of backups.  
Improve backup system capability.  
Remotely and securely store backup data. |
| Is the asset vulnerable to the possibility that a data source could provide it with incorrect or out-of-date input data leading to significant problems? | Improve input data validation and sanity checking, especially for manually entered data.  
Implement detection, alerting and control of anomalous data input events. |
### Miscellaneous

<table>
<thead>
<tr>
<th>Threat Types</th>
<th>Typical Countermeasures</th>
</tr>
</thead>
<tbody>
<tr>
<td>Is ensuring that maximum tolerable downtime is not exceeded, reliant on service levels from other assets etc. that have not yet been discussed or agreed, or are unrealistic?</td>
<td>Review Service Level Agreements and contracts for services on which the asset depends and make improvements where practical. Ensure that any SLAs given for the asset take dependence on other assets into account.</td>
</tr>
<tr>
<td>Is high availability important, and there is reason to think that a failover or more resilient solution needs to be implemented?</td>
<td>Consider implementing a resilient solution featuring redundancy or failover.</td>
</tr>
<tr>
<td>Should the telephone system be unavailable for a significant length of time, would it cause serious problems in relation to the asset in question?</td>
<td>Make the telephone system more resilient. Plan to use mobile phones instead in an emergency.</td>
</tr>
<tr>
<td>Are there any communication mechanisms between components of the information asset that seem particularly vulnerable to a failure leading to a serious problem?</td>
<td>Make the communication mechanism more resilient, robust or fault tolerant. Make the asset more resilient to disruption caused by communication failure. Investigate automatic alerting to such problems where they may otherwise go for some time unnoticed.</td>
</tr>
<tr>
<td>Would further measures be needed to prevent a power cut, lasting less than a few minutes, from causing serious disruption or damage to the asset?</td>
<td>Improve power supply resilience, e.g. use an UPS.</td>
</tr>
<tr>
<td>Would further measures be needed to prevent a power cut, lasting more than a few minutes, from causing serious disruption or damage to the asset?</td>
<td>Improve power supply resilience, e.g. use an UPS and emergency supply or generator. Consider establishing a fallback procedure ready to provide the business function of the asset until power is restored.</td>
</tr>
</tbody>
</table>

---

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

---
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.
1. Introduction

1.1. This document gives additional details about implementing the "Passwords" policy outlined in Use of Computers Policy (ISP-S9).

2. Password based access control

2.1. This document specifies the main password policy parameters to use for University computer accounts. The intention is that sufficiently strong password based access control is enforced.

2.2. There may be circumstances where a password system cannot be configured to enforce the minimum requirements outlined here. In such cases:

- Use of other configurations, that may enforce password security weaker than recommended here, must be considered and approved by management.

- As far as possible the minimum requirements should be implemented, even where they cannot be enforced by computer configuration settings.

3. Password length and complexity

3.1. Minimum password length and complexity requirements, as specified below, must be used in combination to help ensure that passwords chosen by computer users are very difficult to guess.

3.2. All types of computer account should have passwords of at least 8 characters.

3.3. Password complexity rules must be set that require passwords to contain at least one character from 3 of the 4 character sets i.e. uppercase, lowercase, numerical digits and non-alphanumeric characters.

4. Account lockout parameters

4.1. An account lockout is intended to impede password guessing attacks by automatically locking an account after a number of failed authentication attempts. The maximum number of failed login attempts permitted before lockout is known as the “lockout threshold”. The account lockout may be temporary for a period known as the “lockout duration”. The time window during which multiple failures leading to lockout must occur is called the “observation window”.

4.2. For accounts to which account lockout can and should apply, it is recommended that the lockout threshold should be set to 10 and the lockout duration set to 30 minutes. The observation window setting should be 30 minutes. (It is safe to reduce the lockout duration to 5 minutes if inconveniently long lockouts are clearly being caused by failures of legitimate automated login processes. Lockouts may result from automated login processes having not being reconfigured following an account password change.)

5. Password history and maximum and minimum password age settings
5.1. “Password history” can be set to prevent users from repeatedly using the same passwords they used in the past. The “maximum password age” limits the time for which a given password is valid. Expiring use of a password after a certain time helps to reduce the chance that a cracked password is still in use. It also helps avoid the possibility that an intruder would be able to continue accessing a compromised account indefinitely. “Minimum password age” can be used with password history to prevent a user from repeatedly changing a password until they are able to reuse their original password.

5.2. Using password age based expiry of passwords and the password history mechanism is recommended. (It is, however, recognised that automatic expiry of passwords may not be practical for services with large numbers of users because it may increase the workload of the support staff that need to perform password resets.)

5.3. Password aging should not be enabled for accounts which are authenticated against by automatic processes (such as Microsoft Windows scheduled tasks).

5.4. It is recommended that, for accounts where it is applicable, password history should be set to 24, minimum password age set to 1 day and maximum password age set to 90 days. (Practicalities of account management for some services may, however, require users to be able to reset temporary passwords within a day, in which case a minimum password age setting of 0 days is acceptable.)

---

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

---

**Document history:**

<table>
<thead>
<tr>
<th>Date</th>
<th>Month</th>
<th>Year</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>30 July</td>
<td></td>
<td>2009</td>
<td>Began first draft.</td>
</tr>
<tr>
<td>6 August</td>
<td></td>
<td>2009</td>
<td>Automatic password expiry is recommended, however, not compulsory on the basis that in some situations user support costs may exceed the security benefits.</td>
</tr>
<tr>
<td>24 September</td>
<td></td>
<td>2009</td>
<td>A 15+ character password requirement to protect against weak LAN Manager (LM) hashes was dropped on the basis that LM should be set to disabled by domain policy and is disabled by default in Windows Server 2008 and Vista. Also use 8+ password characters instead of 7+ for good measure.</td>
</tr>
<tr>
<td>8 January</td>
<td></td>
<td>2009</td>
<td>The minimum password age may need to be 0 days if account management procedures require users to immediately reset temporary passwords.</td>
</tr>
<tr>
<td>01 March</td>
<td></td>
<td>2010</td>
<td>Approved by the InfoSec Policy Steering Group.</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.
1. Introduction

1.1. This document supports implementation of the "Payment Card Industry Data Security Standard (PCI DSS) compliance" policy referred to in policy document Compliance Policy (ISP-S3).

1.2. The Payment Card Industry Data Security Standard (PCI DSS) is a worldwide information security standard defined and published by the Payment Card Industry Security Standards Council. The standard was created to help payment card industry organisations that process card payments prevent payment card fraud through increased controls around data and its exposure to compromise. The standard applies to all organisations that hold, process, or exchange cardholder information. 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 payment card payments and being audited and/or fined.

1.3. Definitions

- Payment card - A card backed by an account holding funds belonging to the cardholder, or offering credit to the cardholder such as a debit or credit card.
- PCI DSS - The “Payment Card Industry Data Security Standard” (see above).
- Stripe / track data - Information stored in the magnetic strip or chip on a payment card.
- PAN - A “Primary Account Number” is a 14 or 16 digit number embossed on a debit or credit card and encoded in the card’s magnetic strip which identifies the issuer of the card and the account.
- PIN - A “Personal Identification Number” is a secret numeric password used to authenticate payment cards.
- CAV2/CVC2/CVV2/CID – 3-digit security code displayed on payment cards.
- Cardholder Data – Payment card data including: Primary Account Number (PAN), name of cardholder, expiration date and service code.
- Sensitive Authentication Data - Full magnetic stripe data or equivalent on a chip, CAV2/CVC2/CVV2/CID or PINs/PIN blocks.
- Cardholder Data Environment (CDE) - Area of computer system network that possesses cardholder data or sensitive authentication data and those systems and segments that directly attach or support cardholder processing, storage, or transmission.
- PDQ Machine – A credit card swipe machine.
- PED – PIN Entry Device.
• Qualified Security Assessor (QSA) – A person who has been certified by the PCI Security Standards Council to audit merchants for Payment Card Industry Data Security Standard (PCI DSS) compliance.

1.4. This document includes statements on:
• Scope
• PCI DSS outline
• PCI DSS compliance policy
• Authorisation and responsibilities
• Payment card processing
• Electronic cardholder data handling
• Paper cardholder data handling
• Retention of cardholder data
• Physical security of payment card processing equipment

2. Scope
2.1. Policy statements in this document apply to:
• All staff involved in payment card processing
• All payment card processing arrangements across the University
• Both manual and IT-based payment card processing

3. PCI DSS outline
3.1. The Payment Card Industry Data Security Standard (PCI DSS) sets out an extensive and detailed list of requirements and security assessment procedures. The goals and requirements of the standard (currently v2.0) are summarised as:
• Build and Maintain a Secure Network
  o Requirement 1: Install and maintain a firewall configuration to protect cardholder data
  o Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters
• Protect Cardholder Data
  o Requirement 3: Protect stored cardholder data
  o Requirement 4: Encrypt transmission of cardholder data across open, public networks
• Maintain a Vulnerability Management Program
  o Requirement 5: Use and regularly update anti-virus software or programs
  o Requirement 6: Develop and maintain secure systems and applications
• Implement Strong Access Control Measures
  o Requirement 7: Restrict access to cardholder data by business need to know
  o Requirement 8: Assign a unique ID to each person with computer access
  o Requirement 9: Restrict physical access to cardholder data
• Regularly Monitor and Test Networks
o Requirement 10: Track and monitor all access to network resources and cardholder data
o Requirement 11: Regularly test security systems and processes.

- Maintain an Information Security Policy
  o Requirement 12: Maintain a policy that addresses information security for all personnel.

4. PCI DSS compliance policy

4.1. All University card processing activities and related technologies must comply with the Payment Card Industry Data Security Standard (PCI-DSS).

4.2. This policy document forms part of University of Leicester information security policy and directly meets the PCI DSS requirement to “Maintain a policy that addresses information security for all personnel”.

4.3. Card processing activities must be conducted as described herein and in accordance with the PCI DSS standards. No activity may be conducted nor any technology employed that might obstruct compliance with any portion of the PCI-DSS.

4.4. All relevant staff must be made aware of the importance of cardholder data security and must be aware of the requirements stated in this policy.

4.5. This policy shall be reviewed annually and updated as needed to reflect changes to business objectives, to the risk environment or to PCI DSS.

(Note: Certain requirements stated in this policy are not part of the PCI DSS itself; however, are included to facilitate University PCI DSS compliance.)

5. Authorisation and responsibilities

5.1. Staff or departments must not plan, commission, use or modify any payment card processing procedures or systems without consultation with the Finance Office (University Cashier) and authorisation by the Head of Finance. (This includes any payment card processing activity to be undertaken on behalf of the University or which involves any use of University IT or networking equipment.)

5.2. The Finance Office is responsible for managing PCI DSS compliance across the University and may remove any payment card processing activity causing unacceptable risk.

5.3. IT Services is responsible for arranging and assessing the results of the external and internal network security scans required for PCI DSS compliance. (Approved external and internal network scans must be run at least quarterly to check for security against external access to any networked devices that process payment card data.)

5.4. The Finance Office and Information Assurance Services are jointly responsible for making all relevant staff aware of the importance of cardholder data security and the requirements stated in this policy.

5.5. The Finance Office is responsible for ensuring that for service providers with whom cardholder information is shared:

- Contracts require adherence to PCI-DSS by the service provider.
- Contracts include acknowledgement or responsibility for the security of cardholder data by the service provider.
5.6. A list of all staff currently authorised to use devices routinely used to process payment cards, such as tills, PEDs, PDQ machines etc. must be maintained by the department responsible for providing that service and a copy submitted to the Finance Office (University Cashier) who will maintain a central log.

5.7. Staff are reminded of the requirement to report security incidents and any suspected security weaknesses as specified in Reporting Information Security Incidents (ISP-I3).

6. Payment card processing

6.1. Students wishing to pay course fees by payment card must be directed to use the online payment system. Where that is not possible another form of payment i.e. cheque, draft or bank transfer must be used instead.

6.2. Staff must not request or accept transmission of any payment card information from University customers via email or other end-user messaging technologies.

6.3. Departments should, under no circumstances, ask students/customers to release the three-digit security code held on the reverse of their card. (The University pays a higher payment card transaction fee to avoid having to collect and process the security code.)

6.4. Staff must not ask for 3D Secure or Verified by Visa codes, when processing through an online interface.

6.5. When staff process card details on screen, for example when using web interfaces to WPM or YESPay, they should press the Enter key in order to skip the three-digit security code entry field.

6.6. Any electronically stored legacy payment card data, or data stored in error, must be deleted.

6.7. Payment card information, including full PAN numbers, must not be displayed or made visible to anyone except authorised staff. For example, payment equipment such as tills must not show the full PAN. (The first six and last four digits are the maximum number of digits that may be displayed.)

6.8. Full credit card numbers may only be viewed by authorised staff with a need to see them as part of their duties.

7. Electronic cardholder data handling

7.1. Staff must not store any electronic payment card information, whether or not encrypted, on any computers or storage devices whether by scanning, keying or any other means. Note:

- This applies to all types of payment card data including PAN, PIN, three-digit security codes and full track data.
- This requirement limits the scope of the CDE and so controls the cost, difficulty and feasibility of implementing and maintaining the PCI DSS controls necessary for compliance.

7.2. Staff must not transfer cardholder data via email, or other end-user messaging technologies, whether or not encrypted.

7.3. Systems which are specifically designed and deployed to transfer cardholder data electronically such as tills, PEDs and PDQs and outsourced e-commerce solutions must do so in a way that meets PCI DSS compliance requirements. When planning and
deploying such systems, the Finance Office will work with departments, IT Services, system vendors and QSAs as appropriate to achieve and maintain PCI DSS compliance.

7.4. Computers being used by University staff to access outsourced e-commerce solutions, such as WPM or YESPay, on behalf of customers must:

- Run automatically updating anti-virus software that stores accessible audit logs for at least one year.
- Have vendor supplied security patches installed within one month of release.
- Be operated using accounts with normal user level privilege.

(Note: Standard CFS clients logged in with normal domain accounts meet these requirements).

8. Paper cardholder data handling

8.1. The aim should be to reduce and preferably eliminate the need for cardholder data to be held in paper form. Processes should be regularly reviewed to determine whether online payment processes can be implemented to replace paper-based procedures.

8.2. Sensitive card authentication data must not be recorded on paper.

8.3. Cardholder data stored on paper, which must exclude sensitive authentication data, must be:

- In a locked cabinet whenever not in use or supervised. Offices housing such cabinets must also be locked when not occupied.
- Destroyed when no longer required by secure onsite cross-cut shredding, incineration or pulping. (Paper records holding unwanted payment card information must be locked away until destroyed.) (also see 9.2 below.)
- Marked to distinguish it from other paperwork. Departments may use their own classification and marking system for cardholder data paperwork. A suitable solution would, for example, be to use distinctively coloured stationery.

8.4. Where it is necessary to transfer paper cardholder data within the site:

- The only acceptable method is delivery by hand during office hours.
- The internal mail system must not be used.

8.5. Incoming mail containing cardholder data from outside the University may be received through the internal mail system. However, regard should be had to Section 8.1 with a view to eliminating the need for paper-based processes.

8.6. There should not be any requirement for cardholder data to be sent via an external postal service. However, if in exceptional circumstances a need should arise, approval must be first obtained from the Director of Finance. In such cases the data must be delivered by hand to the Post Room and a “Recorded Signed For” service used.

8.7. A record must be kept detailing any transfer of payment card data within the University and by external postal service should a need arise. Management approval is required prior to the transfer.

9. Retention of cardholder data

9.1. Cardholder data, excluding any sensitive authentication data, may be retained only as paper records.
9.2. Except in exceptional circumstances and with explicit approval of the Finance Office, retained cardholder data for any financial year (August-July) must be destroyed by the end of the following January.

10. Physical security of payment card processing equipment

10.1. Devices used to process payment cards, such as tills, PEDs and PDQ machines must:

- Only be used by staff authorised to do so as part of their duties.
- Be protected from physical access out-of-hours by those not authorised to use the equipment or authorised to be in the area. (Small devices such as PDQs must be locked away and larger devices such as tills must be in rooms with restricted access when not in use.)
- Be subjected to routine visual inspection, preferably each day or before use. Equipment, cabling and connections should be inspected for signs of tampering. The working area in the vicinity of the equipment should be checked for any suspicious devices, “hidden” cameras etc.

10.2. Out-of-hours visitors to areas giving access to payment equipment must be supervised and details of such visits must be logged.

---

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

---

**Document history:**

<table>
<thead>
<tr>
<th>Date</th>
<th>Author(s)</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>28 April 2011</td>
<td>Gary Hague</td>
<td>Reviewed and minor changes made.</td>
</tr>
<tr>
<td>14 June 2011</td>
<td>Colin Atkinson</td>
<td>Section 8 Paper cardholder data handling amended.</td>
</tr>
<tr>
<td>07 July 2011</td>
<td>Colin Atkinson/S McShane</td>
<td>Section 8.7 re transfer of data</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.