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 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.)

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 purchased for official University business is normally procured by IT Services and deployed by either IT Services or departmental IT professionals. It is the responsibility of the Director of IT to ensure that an appropriate software licence management procedure is defined and in operation. For policy applicable to the proper management of software refer to:

- Software management Policy (ISP-S13)

For applicable regulations and controls that apply to the acquisition and use of software in compliance with the above policy refer to:

- Software Regulations (ISP-I11)

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.**

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.