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 sure 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. Prevent Duty

The University has a statutory duty under Section 26(1) of the Counter-Terrorism and Security Act 2015, known as the Prevent duty, to have due regard to and aid the process of preventing people from being drawn into and supporting terrorism. It is part of the Government’s counter-terrorism strategy with the aim of reducing the threat to the UK.
University members must not create, download, store or transmit extremism-related material with the intention of supporting or spreading terrorism. The University reserves the right to block or monitor access to such material.

16. 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.

17. The Human Rights Act 1998

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. |

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.