|  |  |
| --- | --- |
| University of leicester logo | *Information Assurance Services Policy Documentation* **Implementation Details** |

**Policy: ISP-I5**

**Title: Guide to Information Legislation**

**Status: Approved**

## Introduction

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

 Areas of legislation relevant to information security are summarised below.

 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.)

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.

##  International law and the Internet

 Caution is necessary in considering what laws and regulations may be applicable to internet usage.

 Basic rules:

* all users of the University of Leicester'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.

## 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.

## Computer Misuse Act 1990

 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. The maximum penalty on indictment is 2 years imprisonment.
* 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. The maximum penalty on indictment is 5 years imprisonment.
* Section 3 contains the offence of doing any knowingly unauthorised act in relation to a computer, with requisite knowledge and intent, that; impairs its operation, prevents or hinders access to any program or data or impairs the operation of any program or the reliability of data held

 For Section 3, the maximum sentence on indictment is 10 years' imprisonment.

 Section 41(2) of the Serious Crime Act 2015 must also be considered. Inserted section 3ZA came into effect on 3 May 2015. Section 3ZA is designed to cater for computer misuse, where the impact is to cause serious damage to human welfare or national security where the maximum penalty of ten years available under Section 3 of the Computer Misuse Act 1990 may be inadequate.

## Data Protection Act 2018 and The General Data Protection Regulation (GDPR)

 The **General Data Protection Regulation** (GDPR) is a legal framework that sets guidelines for the collection and processing of personal information from individuals who live in the European Union (EU).The UK rules are also set by **The Data**

* obtaining data
* recording data
* keeping data
* using data in any way
* sharing or disclosing data
* erasing and/or destroying data.

Persons processing personal data must complete the appropriate training and must make themselves aware of the general requirements of the Data Protection Act 2018, and in particular must abide by the six Data Protection Principles as set out in Schedule I of the Act and further explained in Schedules II and III.

These stipulate that the data must:

1. Be processed fairly, lawfully and transparently' In order for us to process data 'fairly’
2. Be processed only for specific, explicit and legitimate purposes and shall not be further processed in any manner incompatible with that purpose or those purposes
3. Be adequate, relevant, and not excessive in relation to the purpose or purposes for which they are held
4. Be accurate and, where necessary, be kept up to date
5. Be kept for no longer than is necessary for the specified purpose
6. Be processed in a secure manner, taking appropriate security measures with regard to rights of accidental or unauthorised access to personal data, or accidental or unauthorised destruction, lose, use modification or disclosure of personal data

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.

All personal data which is processed by the University must be covered by our registration with the Information Commissioner. Most routine uses of personal data by employees will be covered by our registration. However, if you are processing any data (for example, maintaining a database or running a research project involving the use of personal data) and think it may involve us handling new personal data for the first time or using personal data for a new purpose, please email the Information Assurance Team, ias@le.ac.uk.

Access to personal data will only be granted to staff insofar as is necessary for legitimate operational purposes. The personal or private use of personal data held by the university is strictly forbidden.

All staff with access to personal data must be mindful that they play a role in ensuring that it is always kept securely. They must familiarize themselves with the University's Compliance policies and follow our guidance on data security.

Copies of the University's current guidance on data protection can be obtained from the Information Assurance Team, ias@le.ac.uk.

## Freedom of Information Act 2000

The **Freedom of Information Act 2000** provides public access to information held by public authorities. It does this in two ways: public authorities are obliged to publish certain information about their activities (the publication scheme, usually published on the organisation’s website); and members of the public are entitled to request information from public authorities.

Under the Freedom of Information Act 2000, a public body is obliged, subject to limited exceptions, to disclose information held by that body following receipt of a request made in accordance with the Act.

Members of the University should be aware that their electronic communications and any other documents may be subject to the requirement to be disclosed under the Freedom of Information Act. Non-routine requests for access to University information must all be directed to the Information Assurance Team 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.

## The Environmental Information Regulations 2004

The **Environmental Information Regulations 2004** (EIR) provides a statutory right of access to environmental information held by public authorities. Requests for access to environmental information are processed according to these regulations rather than the Freedom of Information Act 2000.

The definition of "environmental information" is varied but can be summarised as:

* The state of the elements of the environment, such as air and atmosphere, water, soil, land, landscape and natural sites including wetlands, coastal and marine areas, biological diversity and its components, including genetically modified organisms, and the interaction among these elements.
* Factors, such as substances, energy, noise, radiation or waste, including radioactive waste, emissions, discharges and other releases into the environment.
* Measures, such as policies, legislation, plans, programmes, environmental agreements, and activities affecting or likely to affect environmental elements.
* Human health and safety, including the contamination of the food chain, where relevant, conditions of human life, cultural sites and built structures
* Reports on the implementation of environmental legislation.

The Freedom of Information Act 2000 and the Environmental Information Regulations 2004 are broadly similar in purpose but vary in their detail; EIR permits information requests to be submitted orally as an alternative to permanent form. The regulations also allow for recovery of the full cost of providing information as there is no threshold for fees charging.

Information requested under EIR may be subject to exceptions (not exemptions) all of which must be considered under the public interest test.

## The Regulation of Investigatory Powers Act 2000

**The Regulation of Investigatory Powers Act 2000**, or 'RIPA', governs the use of covert surveillance by public bodies, it provides public bodies with the powers to carry out surveillance and investigation, and covering the interception of communications.

Before using RIPA, a public body must evidence a valid reason for its use and consideration must be given to the use of less intrusive methods in all scenarios.

The legislation provides provision for law enforcement agencies to ask the University to intercept communications without consent for specific purposes such as detecting crime.

Given the legal basis for these requests, the University does not need to gain consent before intercepting for these purposes, although we are required to inform staff and students that such interceptions may take place.

Any interception of communications and monitoring undertaken by the University must comply with The Regulation of Investigatory Powers Act 2000.

## The Privacy and Electronic Communications Regulations 2003

The **EC Directive on Privacy and Electronic Communications**, and the **Privacy and Electronic Communications (EC Directive) Regulations 2003**, ‘PECR’ came into force in December 2003. The regulations place restrictions on sending unsolicited commercial marketing emails and marketing and advertising by electronic means.

Whilst this may include emails promoting University courses or services, the definition of direct marketing is not limited to advertising goods or services for sale but includes promoting an organisation’s aims and ideals

Organisations must not send marketing emails or texts to individuals without their specific prior consent. Consent must be knowingly given, clear and specific.

The Directive also imposes the following 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.
* 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

## Official Secrets Acts 1911-1989

The **Official Secrets Acts 1911-1989** establishes 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.

The legislation covers 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.

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

## The Defamation Act 2013

**The Defamation Act 2013** provides legislation to balance the right to freedom of expression and the protection of reputation against 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.

Such messages may be transmitted to 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.

The Act provides protection for scientists and academics publishing peer-reviewed material in scientific and academic journals, and to those publishing material on a matter of public interest where they reasonably believe that it is in the public interest.

We 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.

University members must:

* 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
* ensure that all published facts are accurate
* Remember that all electronic communications are publications.
* Remember that messages which have only one intended recipient may reach a vast audience through the Internet.

University members must not:

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

## The Communications Act 2003

**The Communications Act 2003** provides the regulation of the provision of electronic communications networks and services in terms of access and use of telecommunications, including telephone calls and electronic communications including the internet.

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 Communications Act 2003 or any of the following:

* The Obscene Publications Act 1959
* The Protection of Children Act 1978
* The Telecommunications Act 1984
* 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 2003a 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. Section 127(1) of the Act covers offensive and threatening messages sent over a "public" electronic communications network. The University will report individuals to the police for messages posted to social media sites such as Twitter and Facebook.

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 and may lead to prosecution.

## Copyright, Designs and Patents Act 1988

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/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.

The University Library may be contacted for further advice:

Email: library@leicester.ac.uk

Tel: 0116 252 2043

The Equality Act 2010

**The Equality Act 2010** protects people against discrimination, harassment or victimisation in employment, and as users of private and public services based on nine protected characteristics: We are committed to providing equality for everyone, regardless of:

• Age;

• Disability;

• Ethnicity (including race, colour and nationality);

• Sex;

• Gender reassignment;

• Religion or belief;

• Sexual orientation;

• Marriage and civil partnership; and

• Pregnancy and maternity (whether or not you are pregnant or have given birth recently).

Introduced in October 2010, it replaced previous anti-discrimination laws with a single Act, making the law easier to understand and strengthening protections in many situations.

## The Human Rights Act 1998

**The Human Rights Act 1998** incorporates rights and freedoms guaranteed by the European Convention and safeguards human rights including, but not limited to freedom of expression, freedom of thought, conscience and religion. It also impinges on Data Protection Act and e-monitoring legislation.

## The Common Law Duty of Confidentiality

**The Common Law Duty of Confidentiality** is not written out in documented form, such as in an Act of Parliament. It is a form of law based on previous court decisions.

The duty of confidentiality occurs where confidential information comes to the knowledge of a person in circumstances where it would be unfair if it were then to be disclosed to others.

Anyone who receives information must respect its confidentiality and not disclose it without consent or other strong justification. Common Law prescribes the principle that to disclose confidential information about a living person without consent is, generally speaking, to wrong an individual.

The principle of confidentiality only applies to information to the extent that it is confidential. Once it has entered into the public domain, the principle of confidentiality can have no application . The duty of confidentiality applies neither to useless information, nor to trivia.

The duty of confidentiality is not absolute and is not protected by legal privilege. Exceptions occur when:

• The individual to whom the information relates has consented to disclosure.

• Disclosure of the information is necessary to safeguard the individual, or others, or is in the public interest.

• There is a legal duty to disclose, for example a court order, or to the police as part of an on-going investigation.

In instances where consent of the individual cannot be obtained and no other exception occurs, solid justification is required in the form of a public interest test before individual rights are set aside

The law's protection of confidence states that there is a public interest that confidences should be preserved and protected by the law.

Guidance on disclosure of confidential information, or on any other legislation covered by this document, can be obtained from the Information Assurance Team, ias@le.ac.uk.

**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. Last updated 22 July 2020.