# Guide to legislation relevant to the Electronic Information Systems Security Policy

## Contents



## Introduction

This document contains guidance on some of the principal relevant legislation that is relevant to the information systems of the University. This legislation must be adhered to in order for the University to remain legally compliant in the storage, processing or transmission of information. The guidance is outline only more detailed queries should be address to the University Legal Advisers for guidance

http://www.bath.ac.uk/university-secretary/legal/index.html

## UK Legislation

### Computer Misuse Act 1990

http://www.legislation.gov.uk/ukpga/1990/18/contents

The Computer Misuse Act is intended to deter criminals from using a computer to assist in the criminal offences or from impairing or hindering access to data stored in a computer. The three criminal offence defined in the act are:

1. Unauthorised access to computer material.
2. Unauthorised access with intent to commit or facilitate commission of further offences.
3. Unauthorised acts with intent to impair, or with recklessness as to impairing, operation of computer, etc.

The Crown Prosecution Service offer further guidance in relation to the Computer Misuse Act.

http://www.cps.gov.uk/legal/a_to_c/computer_misuse_act_1990/

### Data Protection Act 1998

http://www.legislation.gov.uk/ukpga/1998/29/contents

Data protection act is underpinned by these guiding principles

1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless –
    (a) at least one of the conditions in Schedule 2 is met, and
    (b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.
2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.
3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
4. Personal data shall be accurate and, where necessary, kept up to date.
5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
6. Personal data shall be processed in accordance with the rights of data subjects under this Act.
7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Further guidance from the University is available from

http://www.bath.ac.uk/data-protection/index.html

## The Freedom of Information Act 2000

http://www.legislation.gov.uk/ukpga/2000/36/contents

The Freedom of Information Act 2000 promotes greater openness and accountability across the public sector and gives a general right of access to all types of recorded information held by public authorities, subject to exemptions applying. The University has an obligation to the public under the Freedom of Information (FOI) act, requests and responses are managed by the Freedom of Information Officer, based in the Office of the University Secretary. The act covers all recorded information held in documents, memos, emails and other written communications that are produced by any member of staff. Almost any document we write at work could potentially be released. Do not write anything in an email that you would not be happy to see printed on University letterhead.

As an employee of the University, if you receive a non-routine request for information you should forward it immediately to the Freedom of Information Officer [1]by email to the contact address of freedom-of-information@bath.ac.uk or telephone on 01225 383225. Please remember there is a 20 working day legal deadline to respond to requests (starting from next working day after the request is received).

The University Secretary publishes further guidance on the act and on managing requests

http://www.bath.ac.uk/foi/

## Regulation of Investigatory Powers Act (RIPA) 2000

http://www.legislation.gov.uk/ukpga/2000/23/contents

RIPA regulates the powers of public bodies to carry out surveillance and investigation, and covering the interception of communications. The Home Office offers guidance and codes of practice on it's application and the circumstances that it should be used.

https://www.gov.uk/guidance/surveillance-and-counter-terrorism

A Draft Investigatory Powers bill is passing through parliament and will reform the requirements of RIPA.

## Copyright, Designs and Patents Act (CDPA) 1988

http://www.legislation.gov.uk/ukpga/1988/48/contents

The act defines and regulates ownership of rights in intellectual property generally provides the owner with a right to prevent others using it unless they have permission or a licence. CDPA categorises the different types of work that are protected by copyright:

- Literary, dramatic and musical works;
- Artistic works includes buildings, photographs, engravings and works of artistic craftsmanship.
- Sound recordings and films;
- Broadcasts;
- Cable programmes;

[1] Currently James Button at time of writing (Jan 2016

- Published editions.

The library provides further information and guidance on copyright - http://www.bath.ac.uk/library/infoskills/copyright/index.html

## Counter-Terrorism and Security Act (CTSA) 2015

http://www.legislation.gov.uk/ukpga/2015/6/contents

CTSA has a number of measures and contains a duty on specified authorities including Higher Education to have due regard to the need to prevent people from being drawn into terrorism. This is also known as the Prevent duty.

Further guidance for HE is published by the Home Office

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/445916/Prevent_Duty_Guidance_For_Higher_Education__England__Wales_.pdf

More specific elements on application at the University are published in the University's Prevent Policy:

http://www.bath.ac.uk/university-secretary/guidance-policies/preventpolicy.pdf

## Defamation Act 1996

http://www.legislation.gov.uk/ukpga/1996/31/contents

Defamation is speaking, broadcasting, printing or publishing something which might harm a person, company or institution's reputation. This includes not only the words themselves but also their implications. Personal digital archives may include opinions which another person could consider as libelous and by making such records available in a digital archive, whether online, or in a designated reading area, the digital archivist could be considered as 'publishing' that archive.. Actions can be brought against individual members of staff as well as the University itself.

## Human Rights Act 1998

http://www.legislation.gov.uk/ukpga/1998/42/contents

The Human Rights Act 1998 allows an individual to assert the rights of the ECHR (European Convention on Human Rights) against public bodies in UK courts and tribunals. Article 8 ECHR provides:

- for the right to respect for private life, family life, one's home and correspondence, and
- that there shall be no interference by a public authority with the exercise of this right, except if it is in accordance with the law, for a legitimate social purpose, or for the protection of the rights and freedoms of others

Personal data (particularly medical data) is therefore protected by Article 8 of the ECHR as part of an individual's right to respect for a private life. The Human Rights Act is intended to prevent any communication or disclosure of personal data as may be inconsistent with the provisions of Article 8 ECHR. These rights are also embedded within the Data Protection Act

The Human Rights Act puts the rights set out in the 1953 European Convention on Human Rights into UK law. Article 8, relating to privacy, is of most relevance to information security it provides a right to respect for an individual's "private and family life, his home and his correspondence", a right that is also embedded within the Data Protection Act.

Further information on the Human Rights Act is available from the Ministry of Justice.

https://www.justice.gov.uk/downloads/human-rights/act-studyguide.pdf

## Obscene Publications Act (OPA) 1959

http://www.legislation.gov.uk/ukpga/Eliz2/7-8/66/contents

OPA has impact on English law as its precedents serve to provide a definition of obscenity that are used in other legal contexts. In addition to the OPA there are a number of other acts that define material that is illegal to hold

- Section 63 of the Criminal Justice and Immigration Act 2008 ("extreme pornography")
- Protection of Children Act 1978
- Video Recordings Act 1984 and 2010
- Indecent Displays (Control) Act 1981
- Customs Consolidation Act 1876, Amendment Act 1887 (Importation of Indecent and Obscene Material)
- Children and Young Persons (Harmful Publications) Act 1955.[1]

The JANET acceptable use policy prohibits the 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.

## Protection of Children Act 1978

http://www.legislation.gov.uk/ukpga/1978/37

An Act to prevent the exploitation of children by making indecent photographs of them; and to penalise the distribution, showing and advertisement of such indecent photographs.

## Police and Justice Act 2006

http://www.legislation.gov.uk/ukpga/2006/48/contents

Section 39 and Schedule 11 of the Police and Justice Act amend the Protection of Children Act 1978 to provide a mechanism to allow police to forfeit indecent photographs of children held by the police following a lawful seizure

## Criminal Justice Act 1988

http://www.legislation.gov.uk/ukpga/1988/33/contents

The act contains clauses to create a summary offence of possession of an indecent photograph of a child.

## Terrorism Act 2006

http://www.legislation.gov.uk/ukpga/2000/11/contents

The Terrorism Act creates a series of offences in relation to terrorism intented to assist the police in tackling terrorism. Section 19 of the Act imposes a duty on organisations to disclose information to

the security forces where there is a belief or suspicion of a terrorist offence being committed. Failure to disclose relevant information can be an offence in itself.

The Home Office offer further information and guidance.

https://www.gov.uk/government/publications/the-terrorism-act-2006

### Digital Economy Act 2010

http://www.legislation.gov.uk/ukpga/2010/24/contents

The act addresses media policy issues related to digital media. The items contained within the act of particular relevance are sections on online copyright infringement and the obligations that internet service providers (ISPs) have to tackle online copyright infringement. It includes an amendment to the Copyright, Designs and Patents Act 1988 to increase the penalty in connection with criminal liability for copyright and performing rights to a maximum of £50,000.

JISC provide some useful guidance on the Act's relevance to educational institutions.

https://www.jisc.ac.uk/guides/intellectual-property-rights-in-a-digital-world

## EU Directives

### Privacy and Electronic Communications (EC Directive) Regulations 2003 and amendments (2004, 2011 and 2015)

http://www.legislation.gov.uk/uksi/2011/1208/contents/made

An amendment to the Privacy and Electronic Communications Regulations in 2011 obliged websites to inform users about their use of cookies and seek consent for setting more privacy intrusive cookies. It also regulates organisations that wish to send electronic marketing messages (by phone, fax, email or text).

More information is available from the ICO website

https://ico.org.uk/for-organisations/guide-to-pecr/

### European Union Data Protection Directive 95/46/EC (Data Protection)

Directive 95/46/EC is the reference text, at European level, on the protection of personal data. It sets up a regulatory framework which seeks to strike a balance between a high level of protection for the privacy of individuals and the free movement of personal data within the European Union (EU). To do so, the Directive sets strict limits on the collection and use of personal data and demands that each Member State set up an independent national body responsible for the supervision of any activity linked to the processing of personal data.

Transfers of personal data from a Member State to a third country with an adequate level of protection are authorised. However, although transfers may not take place when an adequate level of protection is not guaranteed, there are a number of exceptions to this rule listed in the Directive, e.g. the data subject himself agrees to the transfer, in the event of the conclusion of a contract, it is necessary for public interest grounds, but also if Binding Corporate Rules or Standard Contractual Clauses have been authorised by the Member State.

### European Union Directive 2009/136/EC (Cookie Directive)

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:0036:en:PDF

The directive provides obligations on service providers on the security and privacy of users data. The directive was introduced into English law in the Privacy and Electronic Communications amendments of 2011 in particular with relation to cookies.

The web polices of the University address the implementation of cookies on our services

http://www.bath.ac.uk/web/privacy/

### European Union Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46/EC (Safe Harbour)

This area is currently under review as a European Court of Justice decision has overturned previous agreements.

The Safe Harbour Privacy Principles are principles which enable some US companies to comply with privacy laws protecting European Union and Swiss citizens. US companies storing customer data may self-certify that they adhere to 7 principles, to comply with the EU Data Protection Directive and with Swiss requirements. The US Department of Commerce developed privacy frameworks in conjunction with both the European Union and the Federal Data Protection and Information Commissioner of Switzerland

Within the context of a series of decisions on the adequacy of the protection of personal data transferred to other countries, the European Commission made a decision in 2000 that the United States' principles complied with the EU Directive - the so-called "Safe Harbour Decision". However, after a customer complained that his Facebook data were insufficiently protected, the European Court of Justice declared in October 2015 that the Safe Harbour Decision was invalid, leading to further talks being held by the Commission with the US authorities towards "a renewed and sound framework for transatlantic data flows.

## Document Control Information

| | |
|---|---|
| Owner | Mark Acres IT Security Manager |
| Version Number | 0.01 |
| Approval Date | |
| Approved By | |
| Date of Last review | |