Guide to legislation relevant to the Information Security Policy

Table of Contents

Introduction

This document provides guidance on some of the principal relevant legislation applicable to the University's information systems. 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 outlined, and more detailed queries should be addressed to the University Legal Advisers for guidance:

https://www.bath.ac.uk/publications/internal-request-for-legal-advice/

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 criminal offences or from impairing or hindering access to data stored in a computer. The three criminal offences defined in the act are:

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

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

https://www.cps.gov.uk/prosecution-guidance/computer-misuse-act

Data Protection Act 2018

https://www.legislation.gov.uk/ukpga/2018/12/contents

The Data Protection Act is underpinned by six legal principles:

1. Be processed fairly, lawfully and transparently
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 regarding rights of accidental or unauthorised access to personal data, or accidental or unauthorised destruction, loss, use, modification or disclosure of personal data

Further guidance from the University is available on the Data Protection Act:
https://www.bath.ac.uk/legal-information/data-protection-act/

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, providing a general right of access to all types of recorded information held by public authorities, subject to applicable exemptions. 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 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 at freedom-of-information@bath.ac.uk or by telephone on 01225 383225. Please remember there is a 20-working-day legal deadline to respond to requests (starting from the 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 covers the interception of communications. The Home Office offers guidance and codes of practice on its application and the circumstances under which 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 providing the owner with a right to prevent others from 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 include buildings, photographs, engravings and works of artistic craftsmanship
- Sound recordings and films
- Broadcasts;
- Cable programmes
- 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

The CTSA has several measures and imposes a duty on specified authorities, including higher education, to have due regard for 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://assets.publishing.service.gov.uk/media/65e5a5bd3f69457ff1035fe2/14.258_HO_Prevent+Duty+Guidance_v5d_Final_Web_1_.pdf

More specific elements on application at the University are published in the University's Prevent Policy: https://www.bath.ac.uk/legal-information/prevent-policy/

Defamation Act 1996 and 2013

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

https://www.legislation.gov.uk/ukpga/2013/26/contents

Defamation is speaking, broadcasting, printing, or publishing something that 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 libellous, 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 staff members as well as the University itself.

The Defamation Act 2013 has introduced significant changes to libel law, including new defences and a requirement for proof of 'serious harm' to bring a claim.

Human Rights Act 1998

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

The Human Rights Act 1998 enables individuals to assert their rights under 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 that may be inconsistent with the provisions of Article 8 ECHR. These rights are also embedded within the Data Protection Act.

The Human Rights Act incorporates the rights outlined in the 1953 European Convention on Human Rights into UK law. Article 8, relating to privacy, is of most relevance to information security, as 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.

Obscene Publications Act (OPA) 1959

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

OPA has an impact on English law as its precedents serve to provide a definition of obscenity that is used in other legal contexts. In addition to the OPA, there are several 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

The Jisc 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 2000 and 2006

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

https://www.legislation.gov.uk/ukpga/2006/11/contents

The Terrorism Act establishes a series of offences related to terrorism, designed to assist the police in combating 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 offers 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/

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/direct-marketing-and-privacy-and-electronic-communications/guide-to-pecr/

General Data Protection Regulation (GDPR)

https://gdpr-info.eu/

The GDPR, officially known as Regulation (EU) 2016/679, was enacted on May 25, 2018, to harmonise data privacy laws across Europe and protect the personal data of EU citizens. It replaces the previous Data Protection Directive (95/46/EC) and aims to give individuals more control over their personal information while simplifying the regulatory environment for international business by unifying the regulation within the EU.

Transfers of personal data from an EU Member State to a third country are permitted under the General Data Protection Regulation (GDPR) when the European Commission has determined that the third country ensures an adequate level of data protection (Article 45). In the absence of such an adequacy decision, transfers may still take place if appropriate safeguards are provided, such as Standard Contractual Clauses (SCCs) adopted by the Commission or Binding Corporate Rules (BCRs) approved by a competent supervisory authority (Article 46). Additionally, under specific circumstances outlined in Article 49, transfers may occur without adequacy or safeguards—for example, where the data subject has explicitly consented after being informed of the risks, where the transfer is necessary for the performance of a contract, for important reasons of public interest, or for the establishment, exercise, or defence of legal claims.

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 regarding the security and privacy of users' data. The directive was introduced into English law in the Privacy and Electronic Communications amendments of 2011, in relation to cookies.

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

https://www.bath.ac.uk/legal-information/privacy-and-cookie-policy/

Last review: Nov 2025

Next review: Nov 2028

Document owner: CISO / SecAssurance