Guide to legislation relevant to Information Security Policy

Introduction

There are a number of pieces of legislation relevant to information security that must be adhered to if the University is to remain legally compliant when using, storing and handling information. A summary of the main pieces of UK legislation are below.

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

The Data Protection Act regulates the use of personal data by organisations. Personal data is defined as information relating to a living, identifiable individual.

The Act is underpinned by eight guiding principles:

1. Personal data shall be processed fairly and lawfully.

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. [Data subjects have the right to gain access to their personal as held by the University]

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.

As a data controller, the University must also notify annually with the Information Commissioner's Office: http://www.bris.ac.uk/secretary/data-protection

The Information Commissioner has the power to issue fines of up to £500,000 for a breach of the Data Protection Act. For any advice, please contact: data-protection@bristol.ac.uk

The University has advice and guidance available at:
www.bristol.ac.uk/secretary/data-protection

Freedom of Information Act 2000
http://www.legislation.gov.uk/ukpga/2000/36/contents

The Freedom of Information Act gives individuals a right of access to information held by the University, subject to a number of exemptions. Requests for information must be made in writing (email, letter or fax) but can be received by any member of staff at the University. Such requests must be responded to within 20 working days. The University has an internal appeal process if a requester is unhappy with a response to a request and the Information Commissioner regulates the Act.

The University has further guidance and advice at: www.bristol.ac.uk/secretary/foi or you can also contact: freedom-information@bristol.ac.uk

Privacy and Electronic Communications Regulations 2003
http://www.legislation.gov.uk/uksi/2003/2426/contents/made

Section 11 of the Data Protection Act allows individuals to control the direct marketing information they receive from organisations. The Privacy and Electronic Communications Regulations specifically regulate the use of electronic communications (email, SMS text, cold calls) as a form of marketing and allow individuals to prevent further contact.

The University has some guidance on direct marketing at:
www.bris.ac.uk/secretary/dataprotection/depts/marketing.html

The Information Commissioner also provides further information at:
http://www.ico.gov.uk/for_organisations/privacy_and_electronic_communications/the_guide.aspx

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 also deals with the interception of communications. The Home Office offers guidance and codes of practice relating to RIPA.

Copyright, Designs and Patents Act 1988
http://www.legislation.gov.uk/ukpga/1988/48/contents

The Copyright, Designs and Patents Act (CDPA) defines and regulates copyright law in the UK. CDPA categorises the different types of works that are protected by copyright, including:

- Literary, dramatic and musical works;
- Artistic works;
- Sound recordings and films;
- Broadcasts;
- Cable programmes;
- Published editions.

The Copyright Tribunal adjudicates in copyright/intellectual property disputes.

The University offers guidance in relation to copyright issues at:
http://www.bristol.ac.uk/secretary/legal/copyright/

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

The Computer Misuse Act was introduced partly in reaction to a specific legal case (R v Gold and Schifreen) and was intended to deter criminals from using a computer to assist in the commission of a criminal offence or from impairing or hindering access to data stored in a computer. The Act contains three criminal offences for computer misuse:

- Unauthorised access to computer material;
- Unauthorised access with intent to commit or facilitate commission of further offences;
- Unauthorised modification of computer material.

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

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

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 Directgov website.

Equality Act 2010
http://www.legislation.gov.uk/ukpga/2010/15/contents

The Equality Act was introduced in October 2010 to replace a number of other pieces of legislation that dealt with equality, such as the Equal Pay Act, the Disability Discrimination Act and the Race Relations Act. The Equality Act implements the four major EU Equal Treatment Directives.

The University has advice and guidance available at:
www.bristol.ac.uk/equalityanddiversity or contact: equality-diversity@bristol.ac.uk

Terrorism Act 2006
http://www.legislation.gov.uk/ukpga/2000/11/contents

The Terrorism Act creates a number of offences in relation to 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.

Limitation Act 1980
http://www.legislation.gov.uk/ukpga/1980/58

The Limitation Act is a statute of limitations providing legal timescales within which action may be taken for breaches of the law – for example, six years is the period in which an individual has the opportunity to bring an action for breach of contract. These statutory retention periods will inform parts of the University's records management policy.

Official Secrets Act 1989
http://www.legislation.gov.uk/ukpga/1989/6/contents

University members of staff may at times be required to sign an Official Secrets Act provision where their work relates to security, defence or international relations. Unauthorised disclosures are likely to result in criminal prosecution.

Section 8 of the Act makes it a criminal offence for a government contractor (potentially the University) to retain information beyond their official need for it and obligates them to properly protect secret information from accidental disclosure.

Malicious Communications Act 1988
http://www.legislation.gov.uk/ukpga/1988/27/contents

The Malicious Communications Act makes it illegal to "send or deliver letters or other articles for the purposes of causing stress or anxiety". This also applies to electronic communications such as emails and messages via social networking websites.

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

The Digital Economy Act regulates the use of digital media in the UK. It deals with issues such as online copyright infringement and the obligations that internet service providers (ISPs) have to tackle online copyright infringement.

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

Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2011
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.

More information is available from the ICO website.

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.

Counter-Terrorism and Security Act 2015
http://www.legislation.gov.uk/ukpga/2015/6/contents

Accessing websites or other material which promotes terrorism or violent extremism or which seeks to radicalise individuals to these causes will likely constitute an offence under the Counter-Terrorism and Security Act 2015.

Further information is available via the Home Office website.