# Guide to legislation relevant to Information Security Policy

*Last reviewed by Information Security Team IT Services in November 2022*

## Contents



## Introduction

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

## Data Protection Act 2018 and UK GDPR

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

The UK's current Data Protection Act came into force on 25th May 2018, alongside the General Data Protection Regulation (GDPR).

The Act gives individuals rights over their personal data and protects them from the erroneous use of their personal data. The Act also imposes responsibilities and requirements on any organisation that handles personal data, obligating them to comply with a number of important principles and legal obligations.

The Data Protection Principles state that personal data shall:

1. Be collected and processed fairly, lawfully and transparently
2. be obtained only for specified, 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 limited to what is necessary for the purpose or purposes for which they are held
4. be accurate and, where necessary, be kept up to date
5. held in a form which permits identification of data subjects for no longer than is necessary for the purpose it was collected for
6. be held securely, incorporating appropriate technical and organisational measures to prevent unauthorised or unlawful processing of personal data and protect against accidental loss or destruction of, or damage to, personal data

The following key rules must also be complied with at all times:

i Personal data must not be transferred outside of the European Economic Area (EEA), including the use of websites or applications hosted on servers based outside of the EEA, unless appropriate safeguards are in place.

ii Data subjects right in relation to their personal data must be fully respected. This includes the rights of access, rectification, erasure, restriction, objection, portability and other.

iii The University and its staff must be able to demonstrate compliance with, and accountability for, the requirements of data protection legislation at all times.

The Information Commissioner has the power to issue fines of up to 10 million Euros 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

Information Commissioner's Office (ICO) guidance: https://ico.org.uk/for-organisations/guide-to-data-protection/

## Freedom of Information Act 2000

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

https://ico.org.uk/for-organisations/guide-to-freedom-of-information/what-is-the-foi-act/

The Freedom of Information Act gives individuals a right of access to information held by the University, subject to a number of exemptions (https://ico.org.uk/for-organisations/guide-to-freedom-of-information/refusing-a-request/ ). 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

https://www.legislation.gov.uk/uksi/2003/2426/contents

The Privacy and Electronic Communications Regulations (PECR) sit alongside the Data Protection Act and the UK GDPR. They give people specific privacy rights in relation to electronic communications.

There are specific rules on:

- marketing calls, emails, texts and faxes;
- cookies (and similar technologies);
- keeping communications services secure; and
- customer privacy as regards traffic and location data, itemised billing, line identification, and directory listings.

The University has some guidance on direct marketing at:

https://www.bristol.ac.uk/secretary/data-protection/guidance/marketing/

The Information Commissioner also provides further information at:

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

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

https://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.

More information is available on ICO website: https://ico.org.uk/for-organisations/guide-to-pecr/ .

## Regulation of Investigatory Powers Act (RIPA) 2000

https://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: https://www.gov.uk/guidance/surveillance-and-counter-terrorism#ripa-what-it-is-and-how-to-apply.

## Copyright, Designs and Patents Act 1988

https://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:
https://www.gov.uk/government/organisations/copyright-tribunal

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

## Computer Misuse Act 1990

https://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 the following criminal offences for computer misuse:

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.

3ZA. Unauthorised acts causing, or creating risk of, serious damage.

3A. Making, supplying or obtaining articles for use in offence under sections 1, 3 and 3ZA.

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

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

## Human Rights Act 1998

https://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.

Human Rights Act is under review as was announced in December 2021:
https://www.gov.uk/government/news/plan-to-reform-human-rights-act

## Equality Act 2010

https://www.legislation.gov.uk/ukpga/2010/15/contents

https://www.gov.uk/guidance/equality-act-2010-guidance

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

https://www.legislation.gov.uk/ukpga/2006/11/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:
https://www.gov.uk/government/publications/the-terrorism-act-2006

## Limitation Act 1980

https://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

https://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

https://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 2017

https://www.legislation.gov.uk/ukpga/2017/30/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.

## Police and Justice Act 2006

https://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

https://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:
https://www.gov.uk/government/collections/counter-terrorism-and-security-bill .