

Legislation

Legislation

- What legislation impacts on information security?
- How do we lawfully collect, store, and manage information?
- What laws are in place to protect software?
- How can organizations protect themselves, and their customers, within the confines of the law?



Acts and Regulations

Computer Misuse
Act 1990

Freedom of
Information Act
2000

Regulation of
Investigatory
Powers Act 2000

Data Protection
Act
1998

Privacy and Electronic
Communications
Regulations 2003-2011

Copyright, Designs and
Patents Act 1988

Malicious
Communications Act
1988

Human Rights Act
1998

Equality Act 2010

Terrorism Act 2006

Official Secrets Act
1989

Limitation Act 1980

Digital Economy Act 2010

Police and Justice Act
2006

Computer Misuse Act 1990

A person is guilty of an offence if:

- a) He causes a computer to perform any function with intent to secure access to any program or data held in any computer, *or to enable any such access to be secured*.
- b) The access he intends to secure, *or to enable to be secured*, is unauthorized; and
- c) He knows at the time when he causes the computer to perform the function that that is the case.

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



Data Protection Act 1998

- Personal data shall be:
 - processed fairly and lawfully, and obtained only for the specified purpose.
 - adequate, relevant and not excessive.
 - accurate, and where necessary, kept up to date
 - kept only as long as is required for its purpose.
- Individuals can:
 - View the data that an organisation holds on them.
 - Request that incorrect information be corrected, which if ignored, court order can have data corrected or destroyed.

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

Data Protection Act 1998

Police checks on partners | x
m.bbc.co.uk/news/uk-wales-21451611

Police checks on partners broke data laws

By Alun Jones
BBC Newyddion Ar-lein

14 February 2013 | Wales

Police officers and staff in Wales have broken the Data Protection Act 62 times in the past two years.


Four people were sacked and 14 resigned as a result of the breaches.

They were caught carrying out the breaches for non-policing purposes, BBC Wales has discovered under the Freedom of Information Act.

They included checks on partners, relatives and associates, altering their own records, and passing data to third parties.

A spokesperson for the Information Commissioner's Office, which is responsible for the enforcement of the Data Protection Act 1998, said officers and civilian staff had access to "highly sensitive personal information".

"It is important that they do not abuse this access and only use the information for their policing duties," the spokesperson added.



Four police workers were sacked and 14 resigned as a result of the breaches

Top Stories


Outcry as IS 'wrecks' Assyrian site
Archaeologists and officials express outrage about the reported bulldozing of the ancient Assyrian city of Nimrud in Iraq by Islamic State (IS) militants.
31 minutes ago

Pair jailed for Ayesha Ali killing
18 minutes ago

Migrant population 'up 565,000'
4 minutes ago

Features


Special delivery
The man who posted himself to the other side of the world



M&S breached Data Protection | x
www.computing.co.uk/ctg/news/...

M&S breached Data Protection Act

25 Jan 2008
6 Comments



Marks and Spencer has breached the [Data Protection Act](#) in not encrypting employee data held on a laptop, according to the [Information Commissioner's Office \(ICO\)](#).

The system contained pension details for 26,000 employees and was stolen from the home of a contractor.

The personal details of 26,000 Marks and Spencer's employees were stolen last May

Further reading

- > [M&S online sales brighten Christmas gloom](#)
- > [M&S signs £19m Computacenter deal](#)
- > [M&S employee details at risk](#)

Protecting such information is crucial, according to ICO assistant commissioner Mick Gorrill.

"It is essential that before a company allows personal information to leave its premises on a laptop there are adequate security procedures in place to protect personal information such as password protection and encryption," he said.

The ICO has issued Marks and Spencer with an enforcement notice ordering the company to ensure all laptop hard drives are fully encrypted by April.

Failure to comply is a criminal offence and can result in further action against the company.

General Data Protection Regulation (GDPR) – May 2018

- A major change to how EU organisations (including UK) should manage data – agreed in 2016, with 2 year period to comply (25th May 2018).
- Some key points:
 - **Increased Territorial Scope** – *it applies to all companies processing the personal data of data subjects residing in the Union, regardless of the company's location*
 - **Penalties** – *4% of annual global turnover or €20M (whichever is greater) for most serious infringements.*
 - **Consent** – *companies will no longer be able to use long illegible terms and conditions full of legalese, as the request for consent must be given in an intelligible and easily accessible form*
 - **Breach notification** - *to notify users within 72 hours of discovery*
 - **Privacy by design** - *the inclusion of data protection from the onset of the designing of systems, rather than an addition*

General Data Protection Regulation (GDPR) – May 2018

- Key data subject rights
 - **Right to access** - *whether or not personal data concerning them is being processed, where and for what purpose. Further, the controller shall provide a copy of the personal data, free of charge, in an electronic format. This change is a dramatic shift to data transparency and empowerment of data subjects.*
 - **Right to be forgotten** - *entitles the data subject to have the data controller erase his/her personal data, cease further dissemination of the data, and potentially have third parties halt processing of the data*
 - **Right for data portability** - *the right for a data subject to receive the personal data concerning them, which they have previously provided in a 'commonly use and machine readable format'*
 - **Rights in relation to automated decision making**

<https://www.eugdpr.org/key-changes.html>

<https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/>

<https://gdpr-info.eu/art-22-gdpr/>

Data Protection Impact Assessment (DPIA)

- The GDPR mandates a DPIA be conducted where data processing “is likely to result in a high risk to the rights and freedoms of natural persons”. The three primary conditions identified in the GDPR are:
 - A systematic and extensive evaluation of personal aspects relating to natural persons, which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person.
 - Processing on a large scale of special categories of data or of personal data relating to criminal convictions and offences.
 - Systematic monitoring of a publicly accessible area on a large scale.

<https://www.itgovernance.co.uk/data-protection-impact-assessment-dpia>

CIA Principle

- Confidentiality
 - Data should only be viewed by those who are authorized to do so.
- Integrity
 - Data should be accurately recorded, and maintained in its original representation.
- Availability
 - Data should be readily accessible for the authorized users.

Think about how CIA relates to the Computer Misuse Act and the Data Protection Act.

Intellectual Property Rights

- IP is a mechanism designed to protect our creative ideas – may be arts, written, musical.
 - Extends to algorithms and software.
- IP includes copyright, patents, industrial design rights, and trademarks.

Intellectual Property Rights

- Patents
 - Granted by government to an inventor, giving rights to exclude others from making, using, selling, offering to sell, and importing an invention for a limited period of time, in exchange for the public disclosure of the invention. An invention is a solution to a specific technological problem, which may be a product or a process.

Intellectual Property Rights

- Copyright
 - A copyright gives the creator of an original work exclusive rights to it, usually for a limited time. Copyright may apply to a wide range of creative, intellectual, or artistic forms, or “works”. Copyright does not cover ideas and information themselves, only the form or manner in which they are expressed.

Intellectual Property Rights

- Industrial design rights
 - An industrial design right protects the visual design of objects that are not purely utilitarian. An industrial design consists of the creation of a shape, configuration or composition of pattern or colour, or combination of pattern and colour in three-dimensional form containing aesthetic value. An industrial design can be a two- or three-dimensional pattern used to produce a product, industrial commodity or handicraft.

Intellectual Property Rights

- Trademarks
 - A trademark is a recognizable sign, design or expression which distinguishes products or services of a particular trader from the similar products or services of other traders.

Copyright Law

- Copyright, Designs and Patents Act 1988
- Federation Against Software Theft (FAST) 1984
 - Prevention of software piracy
- <https://www.gov.uk/intellectual-property/law-practice>

End User License Agreements (EULA)

- Used for proprietary (closed-source) software.
- Contract between licensor and the purchases, establishing the purchaser's rights to use the software.
 - Typically will state that the software can not be copied, modified, or redistributed by the purchaser.
 - May also state how personal data will be used by the software.

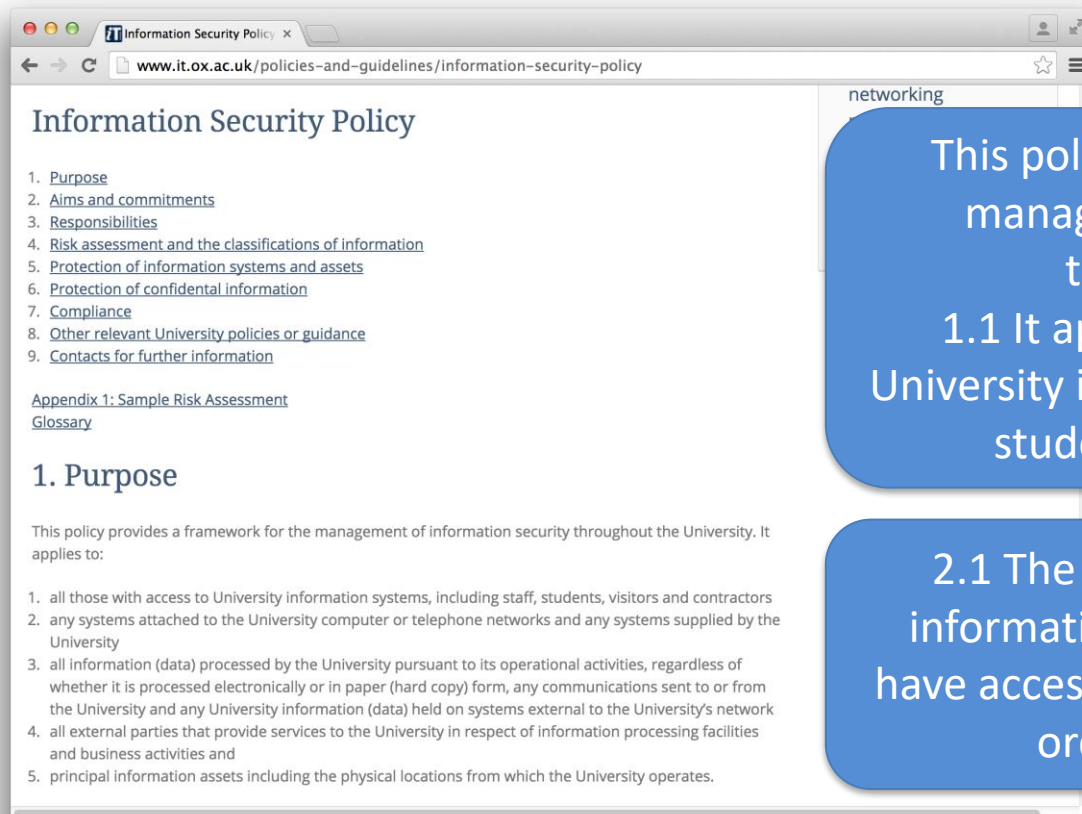
Open Source Software Licensing – (Free Software Foundation)

- GPL – GNU General Public License
 - Most widely used free software license.
 - End-user can study, share and modify software.
 - ***Copyleft*** – same rights must be offered for future use.
- LGPL – GNU Lesser General Public License
 - Same as GPL, but is not copyleft.
 - Means code library could be used in another project, and would not require an open-source license (i.e. proprietary).

Information Security Policy

- Documentation of how an organisation will address information security.
 - Should be suitable for employees, stakeholders, contractors, customers.
- Policy should be in line with legislation, and with the business objectives.
- Policy should explain how information (data) will be utilized, stored, managed, and secured.
- Ensures confidentiality, integrity, availability of data.

Security Management in Practice



This policy provides a framework for the management of information security throughout the University.

1.1 It applies to all those with access to University information systems, including staff, students, visitors and contractors.

2.1 The University recognizes the role of information security in ensuring that users have access to the information they require in order to carry out their work.

2.2 Any reduction in the confidentiality, integrity or availability of information could prevent the University from functioning effectively and efficiently.

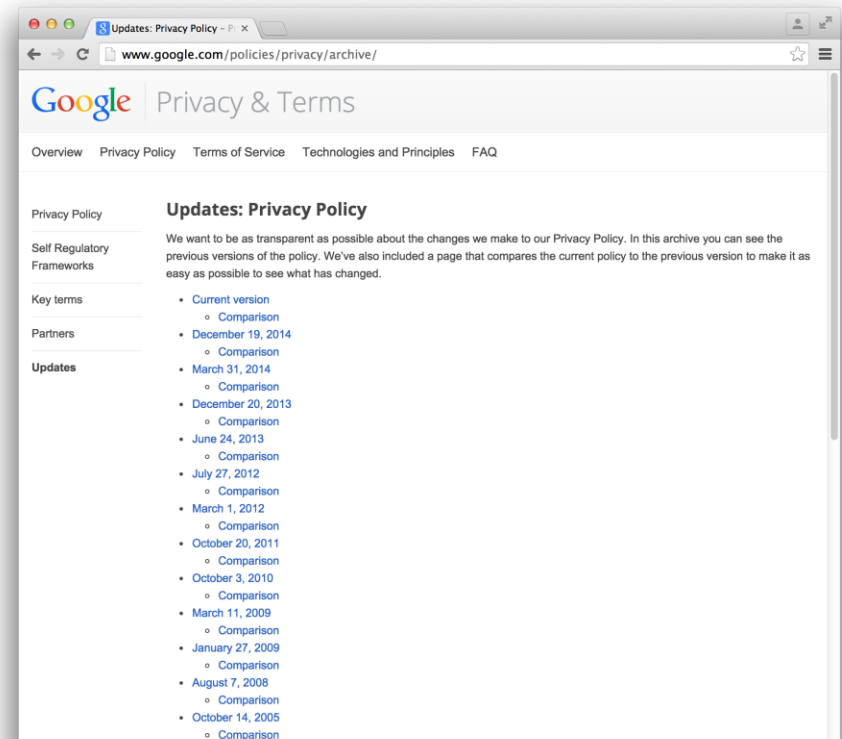
<http://www.it.ox.ac.uk/policies-and-guidelines/information-security-policy>

Privacy Policy

- More focus towards how the information of the individual (customer, employee) is managed.
 - What data will be collected
 - Why it is collected
 - How it is used
 - How it can be accessed and updated.

Privacy Policy

- Google maintain archive of previous policies, and comparisons.
- Earliest: June 9th 1999
- 17 versions to date (as of February 25th 2015)
- Changes reflect how their business has evolved, and how they use personal data.
- <http://www.google.com/policies/privacy/archive/>



Privacy Policy

- Examine the different policies and the comparisons.
- Examine the Google Timeline
<https://www.google.co.uk/about/company/timeline/>
 - E.g. Gmail 2004, Google Maps 2005, Youtube 2006, Android 2007)
- How do the changes of the business reflect in the privacy policy?



Recap

- Computer Misuse Act, Data Protection Act.
- General Data Protection Regulation
- Intellectual Property Rights.
 - Copyright, Designs and Patent Act.
- Software Licensing (EULA, Open-Source)
- Privacy Policy