Criminal Law

• Criminal Law is Undertaken on behalf of the State
• The parties are described as Plaintiff(s)/Defendant(s)
• The Defendant does not have to prove Innocence
• The Plaintiff (who acts on behalf of society) must prove Guilt beyond all reasonable doubt

The Equality Act (2010)

The Equality Act 2010 legally protects people from discrimination in the workplace and in wider society. It replaced previous anti-discrimination laws with a single Act, making the law easier to understand and strengthening protection in some situations.

Civil Law

• Civil Law is between Individual Parties
• The parties are described as Plaintiff (s), or commonly Claimant, and Defendant (s)
• The Claimant will bring a case against the Defendant

English Legal System

Civil Law	Criminal Law
Law Set by legislation - form of public law	Non Criminal Disputes between parties - Form of private law
Passed by Government and enforced by State	-
Brought by state	Brought by Claimant
Regulates Society	Claimant Seeks remedy
Burden of proof - guilt must be proven beyond reasonable doubt	The outcome is usually in the form of financial compensation

The Computer Misuse Act 1990

The Computer Misuse Act protects personal data held by organisations from unauthorised access and modification).

The Computer Misuse Act 1990 (cont)

The act makes the following illegal:
1.Unauthorised access to computer material. This refers to entering a computer system without permission (hacking)
2.Unauthorised access to computer materials with intent to commit a further crime. This refers to entering a computer system to steal data or destroy a device or network (such as planting a virus)
3.Unauthorised modification of data. This refers to modifying or deleting data, and also covers the introduction of malware or spyware onto a computer (electronic vandalism and theft of information)
4.Making, supplying or obtaining anything which can be used in computer misuse offences

The Computer Misuse Act 1990 (cont)

These four clauses cover a range of offences including hacking, computer fraud, blackmail and viruses.
Failure to comply with the Computer Misuse Act can lead to fines and potentially imprisonment.

Offence/Penalty

Offence	Penalty
Unauthorised access to computer material	Up to 6 months in prison and/or a £5,000 fine
Unauthorised access to computer materials with intent to commit a further crime	Up to 5-year prison sentence and/or unlimited fine
Unauthorised modification of data	Up to a 5-year prison sentence and/or an unlimited fine
Making, supplying or obtaining anything which can be used in a computer misuse offences	Up to a 10-year prison sentence and/or an unlimited fine

Sponsored by **Readable.com**
Measure your website readability!
https://readable.com

Privacy Terminology

Pseudonymisation
The processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable person. Pseudonymised data is therefore re-identifiable and falls within the definition of personal data.
Profiling

Privacy Terminology (cont)

Any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a person, in particular to analyse or predict aspects concerning their performance at work or studies, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.
Restriction of processing
The marking of stored personal data with the aim of limiting their processing in the future.
Records of Processing Activities
Detailed records of the personal data processing activities that a Data Controller or Processor is required to maintain and make available under the GDPR.
Supervisory authority

Privacy Terminology (cont)

An independent public authority established by the UK or another state to regulate compliance with data protection law by Data Controllers and Processors and take enforcement action in the case of non-compliance. In the UK the supervisory authority is the Information Commissioner's Office (ICO).

The Defamation Act 1996

The Defamation Act 1996 was created with the purpose of protecting individuals or organisations from slander and libel. Defamation occurs when untrue, damaging information about someone is published to a third party. If the Act is violated, the courts may decide that the guilty party has to compensate the person who was defamed.

The communications act 2003

Communications Act 2003 Section 127(1) covers offensive and threatening messages sent over a "public" electronic communications network. Since 2010 it has increasingly been used to arrest and prosecute individuals for messages posted to sites such as Twitter and Facebook. Section 127(2) covers causing annoyance by sending messages known to be false, which is one of the laws that hoax-999 callers can be prosecuted under.

The Communications Act 2003 Examples

A workplace discusson is undertaken in a public offiece space between colleagues. The conversation is about a mutual aquanitance and body image. The conversation is overheard by another colleageu who shares the content on a social media site, naming all three people

An individual takes a consensual naked photo of a partner using a mobile phone, which immediately stores to a user's account. The individual then uses social media to distribute the image to a friend without gaining consent

Sponsored by **Readable.com**
Measure your website readability!
https://readable.com

The investigatory powers act (2016)

A Bill to make provision about the interception of communications, equipment interference and the acquisition and retention of communications data, bulk personal datasets and other information; to make provision about the treatment of material held as a result of such interception, equipment interference or acquisition or retention; to establish the Investigatory Powers Commissioner and other Judicial Commissioners and make provision about them and other oversight arrangements; to make further provision about investigatory powers and national security; to amend sections 3 and 5 of the Intelligence Services Act 1994; and for connected purposes..

The Human Rights Act 1998

The Human Rights Act 1998 sets out the fundamental rights and freedoms that everyone in the UK is entitled to. It incorporates the rights set out in the European Convention on Human Rights (ECHR) into domestic British law. The Human Rights Act came into force in the UK in October 2000. The Act has three main effects:
1. You can seek justice in a British court
It incorporates the rights set out in the European Convention on Human Rights (ECHR) into domestic British law. This means that if your human rights have been breached, you can take your case to a British court rather than having to seek justice from the European Court of Human Rights in Strasbourg, France.
2. Public bodies must respect your rights

The Human Rights Act 1998 (cont)

It requires all public bodies (like courts, police, local authorities, hospitals and publicly funded schools) and other bodies carrying out public functions to respect and protect your human rights.
3. New laws are compatible with Convention rights
In practice it means that Parliament will nearly always make sure that new laws are compatible with the rights set out in the European Convention on Human Rights (although ultimately Parliament is sovereign and can pass laws which are incompatible). The courts will also, where possible, interpret laws in a way which is compatible with Convention rights.

The Copyright Designs and Patents Act (1988)

The Copyright Designs and Patents Act (1988) gives creators of digital media the rights to control how their work is used and distributed. Music, books, videos, games and software can all be covered by copyright law.

The Copyright Designs and Patents Act (1988) (cont)

Anything which you design or code is automatically copyrighted and may not be copied without your permission, as the digital creator.
- When you buy software, for example, copyright law forbids you from: Giving a copy to a friend
- Making a copy and then selling it
-Using the software on a network (unless the licence you signed allows it. For example, you may be allowed to install an app on 3 devices within a family)
-Renting the software without the permission of the copyright holder

The Intellectual Property Act (2014)

Intellectual property (IP) refers to the ownership of an idea or design by the person who came up with it. It is a term used in property law. It gives a person certain exclusive rights to a distinct type of creative design, meaning that nobody else can copy or reuse that creation without the owner's permission.

Sponsored by **Readable.com**
Measure your website readability!
https://readable.com

The Data Protection Act (1998)

The fundamental principles of DPA 1998 specify that personal data must:
•be processed fairly and lawfully.
•be obtained only for lawful purposes and not processed in any manner incompatible with those purposes.
•be adequate, relevant and not excessive.
•be accurate and current.
•not be retained for longer than necessary.
•be processed in accordance with the rights and freedoms of data subjects.
•be protected against unauthorized or unlawful processing and against accidental loss, destruction or damage.
•not be transferred to a country or territory outside the European Economic Area unless that country or territory protects the rights and freedoms of the data subjects.

Types of Data

Personal Data - This is Data that can identify you, either as a single element of data or as part of a dataset. Fully anonymised or data relating to a deceased person is not subject to GDPR.
Sensitive Data - This is data that if breached, could create a more significant risk to the individual, therefore it has more protection, includes most of the 'protected characteristics', biometric and genetic data.
Criminal Data - This is criminal conviction and offences data and cannot be held or processed without legal or official authority.

The Freedom of Information Act (2000)

The Freedom of Information Act 2000 provides public access to information held by public authorities.
It does this in two ways:

The Freedom of Information Act (2000) (cont)

•public authorities are obliged to publish certain information about their activities; and
•members of the public are entitled to request information from public authorities.
The Act covers any recorded information that is held by a public authority in England, Wales and Northern Ireland, and by UK-wide public authorities based in Scotland. Information held by Scottish public authorities is covered by Scotland's own Freedom of Information (Scotland) Act 2002.

The Freedom of Information Act (2000) (cont)

Public authorities include government departments, local authorities, the NHS, state schools and police forces. However, the Act does not necessarily cover every organisation that receives public money. For example, it does not cover some charities that receive grants and certain private sector organisations that perform public functions.

Sponsored by **Readable.com**
Measure your website readability!
https://readable.com