curriculum for excellence

N4 N5

Legal Implications

The Laws you need to know

- Data Protection Act
- Computer Misuse Act
- Copyright, Designs and Patents Act
- Communications Act
- Health and Safety Regulations

Data Protection Act

The 8 principles of the Data Protection Act:

1. Personal data should be fairly and lawfully processed.
2. Personal data should only be used or disclosed for the specified purposes.
3. Personal data should be adequate, relevant and not excessive.
4. Personal data should be accurate and kept up to date.
5. Information should not be kept any longer than necessary.
6. Data must be processed in accordance with the rights of the data subjects.
7. Security measures should prevent unauthorised access or alteration of the data.
8. Personal data should not be transferred to countries outside the EU except to countries with adequate data protection legislation.

Data Protection Act

The rights of the Data Subjects:-

- See data held on themselves, within 40 days, for payment of a fee.

- Have any errors in the data corrected.
- Compensation for distress caused if the Act has been broken.
- Prevent processing for direct marketing (junk mail) by writing to the data controller.

Data Protection Act

The responsibilities of Data Users:-

- Have to register with the Data Protection Registrar if they wished to hold personal information about data subjects.
- They must be willing to let data subjects see data held about them, but must amend any false data without charge.
- Data Users must also be willing to remove subjects' names and addresses from mailing lists if asked to.

Data Protection Act

Unconditional exemptions:-

- Data related to National Security.
- Data which by law has to be made public (e.g. voters' roll).
- Data held by the Police and National Health Service.

STRATHCLYDE POLICE

NHS SCOTLAND

Data Protection Act

Conditional exemptions:-

- mailing lists (names and addresses).
- data used for calculating and paying wages.
- information used for club memberships.
- data used by a data subject at home.

- Jail
- Fines of up to £500,000

Computer Misuse Act

The Computer Misuse Act makes it a criminal offence to:

- Gain unauthorised access to a computer system or ***hacking***
- Write and distribute viruses which can damage data on a computer

Both these types of crime are now widespread because so many computers may be accessed through networks such as the internet

- Up to five years in prison
- Unlimited fines

Copyright, Designs and Patents Act

This Act helps to protect copyright owners from having their work copied by others without payment.

It was created to ensure that copies must be bought and not simply passed on from one person to another.

It is illegal to copy software, for example, without the author's or the software company's permission.

- Up to ten years in prison (was 2 years until 2002)

- Unlimited fines

Communications Act

This is split into 2 separate laws we must understand:

- Electronic Communications Act
- Communications Act

Electronic Communications Act

There are 2 main parts to this act:

- Regulate the provision of cryptographic services in the UK
- Confirms the legal status of electronic signatures

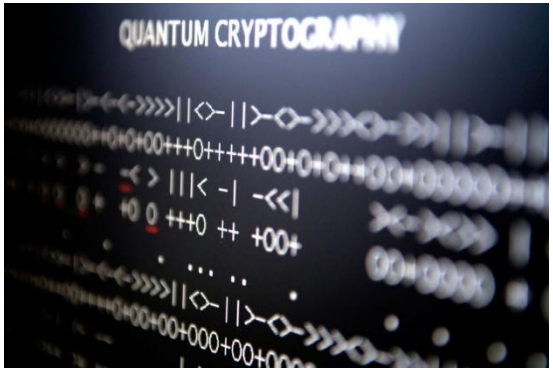
These are both important for electronic transactions

Electronic Communications Act

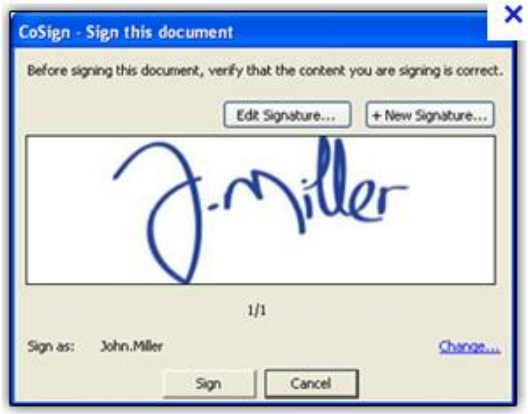
Cryptography is the process used to scramble ordinary text that is readable into cipher text which is unreadable by anyone other than the person holding the key to decrypt or unscramble the message.

Cryptography has been used by banks and government for many years. It is also an essential tool for any company wishing to trade electronically.

The Government has established a list of approved providers of cryptography services. The register is voluntary so there are no legal requirements for anyone offering cryptography services to be on the register. However, as it is essential the businesses can trust those providing cryptography services, it is more likely that they will use one who is on the approved register.



Electronic Communications Act



An electronic signature is a digital mark, code or other symbol that is associated with that person.

It can be used to sign an electronic document in place of a hand-written signature.

It can confirm the communication is authentic and has not been tampered with.

The owner of the electronic signature can be checked and verified in several ways, for example a certificate provided by a special provider.

Since 25th July 2000 the Act has recognised digital signatures as a legal method to identify an individual in the United Kingdom.

Communications Act

This Act gave OfCom (Office of Communication) its full power to across the television, radio, telecoms and postal sectors.

It has a duty to represent the interests of citizens and consumers by promoting competition and protecting the public from what might be considered harmful or offensive material.

Some of the main areas Ofcom presides over are licensing, research, codes and policies, complaints, competition and protecting the radio spectrum from abuse

Ofcom
OFFICE OF COMMUNICATIONS

Communications Act

The Act was also introduced to stop 'Wifi Leeching'.

A person who is guilty of an offence:-

(a) dishonestly obtains an electronic communications service, and

(b) does so with intent to avoid payment of a charge applicable to the provision of that service

It also contains a provision that could be interpreted as holding businesses such as coffee shops that provide free Wi-Fi to customers as responsible for unlawful downloads made over their networks.

The communications Act led to a trainee accountant being fined for posting a joke bomb threat on Twitter.

http://www.zdnet.com/court-allows-appeal-in-twitter-joke-trial-4010021365/

- 6 months to 5 years in prison
- Fined

Health and Safety Regulations

Requirement on employers:-

- Carry out a **risk assessment**.
- Employers with five or more employees need to record the significant findings of the risk assessment.
- Risk assessment should be straightforward in a simple workplace such as a typical office.
- Provide a safe and secure working environment.

Health and Safety Regulations

Can include:

- provide tiltable screens
- provide anti-glare screen filters
- provide adjustable chairs
- provide foot supports
- make sure lighting is suitable
- make sure workstations are not cramped
- plan work at a computer so that there are frequent breaks
- pay for appropriate eye and eyesight tests by an optician
- Fire escape routes
- Gritting paths in winter
- Secure fixtures and fittings

Note: These regulations **do not** apply to students in schools or colleges.

- Up to two years in prison
- Unlimited fines
- Up to 15 years disqualification as a company director

Also, if the breach results in severe injury or death then prosecution for more severe crimes is possible (e.g. manslaughter)