Computer Misuse Act

You need to be familiar with the following ideas about data: information without context, eg a list of students with numbers beside their names is data, when it’s made clear that those numbers represent their placing in a 100 metre race, the data becomes information and computer misuse: that data stored electronically is easier to misuse; that software: a general term used to describe an application or a program should not be copied without permission; the consequences of software piracy: acquiring, profiting from, using or making changes to copyrighted material without prior permission; that hacking can lead to corruption of data, either accidentally or on purpose.

Types of computer misuse

Misuse of computers and communications systems comes in several forms:

Hacking

Hacking is where an unauthorised person uses a network: a group of interconnected computers, Internet or modem: a piece of hardware that connects a computer to the Internet connection to gain access past security passwords or other security to see data stored on another computer. Hackers sometimes use software hacking tools and often target, for example, particular sites on the Internet.

Data misuse and unauthorised transfer or copying

Copying and illegal transfer of data is very quick and easy using online computers and large storage devices such as hard disks: a device used to store vast amounts of data, the data is stored on a disk, memory sticks: a thumb-
sized portable storage device used primarily for transferring files between computers] and DVDs [Digital Versatile Disc (DVD): used to store data, eg a movie]. Personal data, company research and written work, such as novels and textbooks, cannot be copied without the copyright holder's permission.

**Copying and distributing copyrighted software, music and film**

This includes copying music and movies with computer equipment and distributing it on the Internet without the copyright [copyright: gives the creator of an original piece of work control over its publication, distribution and adaptation] holder's permission. This is a widespread misuse of both computers and the Internet that breaks copyright regulations.

**Email and chat room abuses**

Internet services such as chat rooms [chat room: accessed on the Internet, users can meet to chat in real-time, messages are typed out but voice chat rooms exist too] and email [email: electronic mail - a message written or typed on a computer and sent electronically rather than by post] have been the subject of many well-publicised cases of impersonation and deception where people who are online pretend to have a different identity. Chat rooms have been used to spread rumours about well known personalities. A growing area of abuse of the Internet is email spam, where millions of emails are sent to advertise both legal and illegal products and services.

**Pornography**

A lot of indecent material and pornography is available through the Internet and can be stored in electronic form. There have been several cases of material, which is classified as illegal, or
which shows illegal acts, being found stored on computers followed by prosecutions for possession of the material.

**Identity and financial abuses**

This topic includes misuse of stolen or fictional credit card numbers to obtain goods or services on the Internet, and use of computers in financial frauds. These can range from complex well thought out deceptions to simple uses such as printing counterfeit money with colour printers.

**Viruses**

*Viruses* \textit{virus: ultramicroscopic non-cellular organism that replicates itself inside the cells of living hosts} are relatively simple \textit{programs} \textit{program: a list of instructions written in a programming language} written by people and designed to cause nuisance or damage to computers or their files.

**How to prevent computer misuse**

**The Computer Misuse Act (1990)**

This was passed by Parliament and made three new offences:

1. Accessing computer material without permission, eg looking at someone else's files.
2. Accessing computer material without permission with intent to commit further criminal offences, eg \textit{hacking} \textit{hacking: to gain unauthorised access to a computer} into the bank's computer and wanting to increase the amount in your account.
3. Altering computer \textit{data} \textit{data: information without context, eg a list of students with numbers beside their names is data, when it's made clear that those numbers represent their placing in a 100 metre race, the data becomes information} without permission, eg writing a \textit{virus} \textit{virus:ultramicroscopic non-cellular organism that}
replicates itself inside the cells of living hosts to destroy someone else's data, or actually changing the money in an account.

**The Data Protection Act**

This was introduced to regulate personal data. This helps to provide protection against the abuse of personal information. Find out more about the Data Protection Act.

**Copyright law**

This provides protection to the owners of the copyright: gives the creator of an original piece of work control over its publication, distribution and adaptation and covers the copying of written, musical, or film works using computers. **FAST** [Federation Against Software Theft (FAST): a not-for-profit organisation, formed in 1984 by the software industry with the aim of eradicating software theft in the UK] is the industry body which is against software theft. You can find out more about it in the Copyright section.

There have been cases where laws such as Copyright have been used to crack down on file sharing: the act of sharing files over the Internet websites or individuals who store and illegally distribute copyrighted material, eg music. There is a massive problem with many people around the world obtaining copyrighted material illegally.

**Close down chat rooms**

Some chat rooms: accessed on the Internet, users can meet to chat in real-time, messages are typed out but voice chat rooms exist too have been closed down due to abuses, especially where children are vulnerable. Some have moderators: an external assessor who will assess your project who help to prevent abuses. Advice about
sensible use is important; especially to never give personal contact details or arrange meetings without extreme caution.

**Reduce email spamming**

This may be reduced by:

- never replying to anonymous emails [email: electronic mail - a message written or typed on a computer and sent electronically rather than by post]
- setting filters on email accounts
- reporting spammers to ISPs [Internet Service Provider (ISP): Internet Service Provider - needed in order to access the Internet, they also provide services such as web space and email], who are beginning to get together to blacklist email abusers
- governments passing laws to punish persistent spammers with heavy fines

**Regular backups and security**

Just making something illegal or setting up regulations does not stop it happening. Responsible computer users need to take reasonable steps to keep their data safe. This includes regular backups [backup: to copy data onto a separate storage device in case the original device should fail, be damaged or the data stored on it get corrupted] and sufficient security with passwords.