**You need to be familiar with the following ideas about *data* and computer misuse: that data stored electronically is easier to misuse; that *software* should not be copied without permission; the consequences of software *piracy*; 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*, Internet or *modem* 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*, *memory sticks* and *DVDs*. 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* 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* and *email* 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* are relatively simple *programs* 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 *hacking* into the bank's computer and wanting to increase the amount in your account.
3. Altering computer *data* without permission, eg writing a *virus* 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.

### Copyright law

This provides protection to the owners of the *copyright* and covers the copying of written, musical, or film works using computers. *FAST* is the industry body which is against software theft.

There have been cases where laws such as Copyright have been used to crack down on *file sharing* 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* have been closed down due to abuses, especially where children are vulnerable. Some have *moderators* 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*
- setting filters on email accounts
- reporting spammers to *ISPs*, 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* and sufficient security with passwords.