The Computer Misuse Act, 1990 was passed to deal with the problem of hacking of computer systems. In the early days of hacking, the problem wasn’t taken very seriously – it was seen as mischievous behaviour, rather than as something which could cause serious loss or problems to companies, organisations and individuals. Before 1990, it was difficult to prosecute people for hacking – existing laws were not written with that in mind. However, it became increasingly clear that hacking should be against the law, and that the laws should be effective and enforceable. As a result, the Computer Misuse Act was passed in 1990.

The Act created three new offences:

• Unauthorised access to computer material

• Unauthorised access with intent to commit or facilitate commission of further offences

• Unauthorised modification of computer material.

Unauthorised access to computer material

This is the lowest level of offence. It includes, for example, finding or guessing someone’s password, then using that to get into a computer system and have a look at the data it contains. This is an offence even if no damage is done, and no files deleted or changed. The very act of accessing materials without authorisation is illegal. This offence carries a penalty of imprisonment up to six months and/or a fine.

Unauthorised access with intent to commit or facilitate commission of further offences

This builds on the previous offence. The key here is the addition of ‘intent to commit...further offences’. It therefore includes guessing or stealing a password, and using that to access, say another person’s on-line bank account and transferring their money to another account. For this offence the penalty is up to five years’ imprisonment and/or a fine.

Unauthorised modification of computer material

This could include deleting files, changing the desktop set-up or introducing viruses with the intent to impair the operation of a computer, or access to programs and data. The word ‘intent’ means it has to be done deliberately, rather than someone deleting files by mistake. This also includes using a centre’s computer to damage other computers outside the centre, even though the computer used to do this is itself not modified in any way. This offence carries a penalty of up to five years and/or a fine.
The Act clearly takes a very serious view of hacking – even where there is no intent to defraud or do damage. It is therefore important that centre users are made aware of the potential penalties, and equally importantly, why these offences are so serious. Most people would understand that using a computer to commit fraud is clearly wrong. However, some people would not see ‘victimless’ hacking, or playing around with computer settings, as serious. But the reality is that such activities can seriously affect the operation and work of the centre, resulting in unhappy and dissatisfied users, and probably creating a lot of additional work for the centre staff in repairing damage done to programs and data.

**How do you deal with misuse?**

Prevention is far better than cure. Reference to the offences under the Act should be included in your Acceptable Use Policy, preferably phrased in language which is easy to understand, and giving examples rather than using legalistic jargon. Your Acceptable Use Policy should be discussed with each user, rather than just handed out, so that people understand why it is important to follow the guidelines. The Acceptable Use activity will help to get all parties involved in the development of your policy.

**Viruses**, of course, are common now and usually introduced unwittingly rather than deliberately. Without effective monitoring and control of your centre’s computers, you would find it difficult to prove deliberate infection by a **virus** in any case. It’s therefore essential to have effective, up-to-date **software** protection against **viruses**. Visit the Firewalls, viruses and hacking section for more information.

If you feel there is deliberate misuse of computer systems, there are different options for dealing with this, ranging from internal to external. Depending on the seriousness of the offence, a centre is likely to have a range of internal sanctions, from first warnings to temporary bans from the centre, to permanent exclusion. Most offences are likely to be people simply playing around, to see what they can do. However, if something more serious is suspected – for example, using the centre’s computers to gain unauthorised access to other computers outside the centre, or to commit fraud – then it may be that the best option is to inform the police.

**Possible scenarios**

**Scenario One**
A student on holiday from college comes into the centre, starts playing around with the desktop settings, and installs some unauthorised **software** which she has downloaded from the **Internet**. Before leaving after that session, she changes everything back and removes the **software**. What do you do?

Before the student first used the machines, she should have been given the Acceptable Use Policy, and this should have been discussed with her. The fact that she has changed everything back to the way it was is irrelevant – an offence has been committed. More practically, downloading **software** from the **Internet** is a risky thing to do, and could easily have introduced a **virus** to the centre’s computers. As a centre you should consider the appropriate action here – this will probably be either a warning or temporary suspension.
Scenario Two
Someone has been using a computer for e commerce, to order some books. Rather carelessly, they had written down their credit card details on a piece of paper, and left it in the centre. Someone else finds it, and uses these details to make some orders of their own, changing only the delivery address. What do you do?

This is quite clearly illegal, and falls under the second category of offences. It is no different from breaking into someone’s house and stealing their property. There is a clear argument for reporting this to the police.