

UNIVERSITY COLLEGE BIRMINGHAM

COMPUTER MISUSE POLICY

All access of computers and connected systems is governed by the Computer Misuse Act 1990. This act has created three criminal offences covering the usage of Computers:

1. Unauthorised access to computer material

It is illegal to access a computing system unless authorised to do so and as such it makes the activity of "*hacking*" a crime. It does not matter whether the hacker is remote, working from a distance over the remote area networks, or local, where persons such as staff or students who may have limited authorisation to use the computers knowingly exceed that authority. The hacking need not be directed at a particular computer, program or data.

For example, it is unlawful without proper authority:

- To use another person's ID and password in order to access a computer, use data or run a program;
- To alter, delete, copy, or move a program or data, or simply to output a program or data; or
- To lay a trap to obtain a password.

2. Unauthorised access to a computer system with intent to commit or facilitate the commission of a further offence

This covers the situation where unauthorised access is gained with intent to commit a further offence. For example, a person may gain unauthorised access to computer material in order to commit theft by re-directing funds from someone else's bank account.

3. Unauthorised modification of computer material

This offence includes the deliberate deletion or corruption of programs or data. It also includes the introduction of viruses etc., where these result in the modification or destruction of data.

Please note the University will take very seriously any attempts at "hacking" internal/external systems. Any such actions will be reported to the appropriate authorities immediately.