DUNDRUM COLLEGE
OF FURTHER EDUCATION

Computer Ethics and Usage Policy

1. You are responsible for the correct use of our computer systems. That responsibility exists regardless of what security mechanisms are in place. All rules and policies of CFE Dundrum must be adhered to by all users of computing and information services at The College of Further Education Dundrum. All rights and privileges of all users should be protected.

The systems administrator at CFE Dundrum has the right to monitor the computer system. The systems administrator has the right to examine user files to diagnose system problems or investigate security breaches.

All usage of the CFE Dundrum's facilities must be consistent with the business of the college: Information placed on the system may relate only to educational, computer-oriented, cultural, charitable, social, or economic matters. Use of the system for any personal profit-oriented, commercial, or business purpose is strictly prohibited.

2. Broadband Usage

The college offers students full use of our high bandwidth Internet connection. We expect you to respect the needs of other Internet users and for this reason downloading of large movies or audio files is restricted. Please refrain from this activity. Installation or use of Kazaa or other P2P software is not allowed either on college machines or your own laptop/computer device.

3. The following are considered unacceptable uses of computer systems, and are strictly prohibited

Transmitting, accessing or storing information of an obscene, derogarotary or offensive manner
Any activity deemed illegal by the Irish authorities.
Computer damage or destruction.
Offenses against computer users including, but not limited to, harassment.
Unauthorized use of any system.
Modification or destruction of programs or data other than your own personal files.

Tampering or alteration of computer, computer systems, programs or files.
Unauthorized access or attempted unauthorized access to a computer or network.
Causing denial of computer services (ex: run a virus that renders a network unusable).
Preventing others from using computer services.
Causing deterioration of system performance (e.g. playing some networking games over a network for example Doom).
Computer trespass. This includes remote systems as well as secured areas of this system.

Computer invasion of privacy - unauthorized examination of files.
Computer caused physical injury.

Copying licensed software.

Posting confidential information such as Social Security Numbers or Phone numbers.
Cracking passwords.
Even if a file is readable, do not assume you may read it unless explicitly granted authority to do so.
Even if a file is updatable, do not modify it unless explicitly granted authority to do so.

4. You may not share your account.
You may not use any computer resource without prior permission.

If a CFE Dundrum systems administrator asks you to cease an activity on the computer, you must stop that activity immediately.

5. Password Policy
Your password is the only means you have of keeping your account and files secure. The algorithm that encrypts passwords has not been broken, however, it is possible for your password to be stolen when using the Internet so you are encouraged to change it often. More than 80% of computer break-ins are because passwords can be easily derived by hackers. The following are some guidelines we encourage you using when choosing a password:
Do keep your password secret and change it often.
Do not use an all numeric password, or a password shorter than eight characters.
Do use a password that mixes characters with numbers or punctuation marks.
Do use a password you will remember.

NB: Most problems reported to the networking team are of the nature of passwords i.e. people forget them!

6. Data policy

Users of these systems must not divulge system passwords or pass on data to any other person outside of the college.

7. Game Playing Policy
Game playing is allowed on student systems as long as:
It is authorised by a CFE Dundrum administrator (eg. During a rag day event).
It does not deteriorate system performance.
The computer is not needed for school work, research or any other legitimate purpose.

8. Hardware Policy
You may not move or take any hardware without explicit permission from the designated owner of that hardware.
You may not destroy or vandalize any hardware, cable or service provided by the campus.

9. Denial of Service

You may not disable the network by means of any computer program.
You may not disable the network by rendering any equipment unusable.

10. Security Policy

You are responsible for the security of your account. Please read the policy on passwords.
The following are symptoms of unauthorized trespass of your account. If you become aware of the following please contact your supervisor now.
New, unexplained files found in your directory.
Changes in file lengths or dates.
Unexplained data modification or deletion.
Unable to login to your account.