College Network Code of Conduct

Contents

The College has a Security Policy governing the use of the College’s electronic information systems (the **“network”**), and an Acceptable Use Policy (the **“AUP”**) which must be followed.

In addition, the College's ICT Policy Group has issued the following Code of Conduct as guidelines of expected behaviour and good practice when using the College’s network.

1. What you may use the College's network for

Computers are provided primarily for academic purposes or for College business. There is no objection to your making reasonable use for personal purposes such as electronic mail or preparing CVs, providing you observe the following code:

- Don't waste materials, or waste time on the computers to the detriment of others.
- Don't send offensive, or unsolicited junk, or nuisance mail, attachments or messages. Also remember mail might reach somebody for whom it was not intended.
- Your use must be lawful, honest and decent, and must have regard to the rights and sensitivities of other people. This means that any use that is or could be considered obscene or with the intent of annoying or offending somebody else is forbidden.
- Don't use the College network for commercial gain.
- The law requires that you don't hold any information in electronic form about living persons unless you are registered to do so. (see Section 9)

1. Respect the equipment

Please treat computer equipment with respect - it is there for your benefit.

- Please be considerate of other people - avoid excessive noise or other nuisance.
- No eating or drinking in whilst using computer equipment.
- Don't run your own software on College computers or load software on to the computer unless you have explicit permission to do so from the Computer Services Department.
- Don't delete, disable or tamper with any software provided by the College.
- Don't tamper with the hardware or any network or power connections.

2. Using the Network

- **Never** attempt to gain access to another account (username or file store) unless you have been given explicit permission to do so by the Computer Services & Systems Manager. If you do you are breaking the law.
- Do not connect your own equipment to the network, with the exception of the Student (Guest) wireless networks which is provided for this use.

3. Emails and the Internet

- E-mails should be drafted with care. Due to the informal nature of e-mail, it is easy to forget that it is a permanent form of written communication and the communication can be recovered even when it is deleted from your computer.
- Try not to create e-mail congestion by sending trivial messages or unnecessarily copying e-mails. Employees should regularly delete unnecessary e-mails to prevent over-burdening the system.
- Make hard copies of e-mails which you wish to keep for record purposes.
- You may want to obtain e-mail confirmation of receipt of important messages. You should be aware that this is not always possible and may depend on the external system receiving your message. If in doubt, telephone to confirm receipt of important messages.

4. Look After Your Usernames and Passwords

All learners and staff are entitled to use the computer network service. Once learners have enrolled they will receive a username and password as part of the LRC induction; staff will receive this as part of their staff induction.

- It's **your** responsibility to keep your logon details secure. **Never** allow anyone else access to it.
- **Keep your password secret**; don't use your name, your partner's name, your car registration or anything else that someone might guess. If you have to write it down, disguise it. Change your password regularly. If you think someone might have watched you typing it in, change it immediately.
- Don't leave a logged-in session unattended, even for a moment.
- Make sure you **log out** when you finish using the computer.
- **Never** use anyone else's account, with or without their permission.

5. Look After Your Equipment

It's **your** responsibility to keep equipment under your control free from viruses or anything else with the potential of causing damage. The College uses virus protection software centrally and on all its computers.

6. Look After Your Data

You, not the College, are ultimately responsible for the security of your data. If you hold important data on a multi-access computer, you should not rely entirely on the College's back-up procedures. Wherever possible, keep an independent copy of your data.

Power, disk and system failures usually take effect without warning; consider the consequences before you use the computers. The following good practice is recommended:

- Save your files at frequent intervals.
- Keep your own multiple back-up copies of anything that is important.
- Read the messages displayed at log-in on the Intranet or the Learning Zone; this facility is intended to warn you of any imminent service interruptions.

It is sometimes possible to retrieve files that have been deleted accidentally, but you shouldn't rely on this feature. When you leave the College your account and files will be deleted. Any usernames provided for use on a particular course will be deleted at the end of the course. It is your responsibility to take a copy of anything you need before you finish.

7. Observe Copyright Restrictions

Don't copy any software without permission. You should assume software is copyright unless you know otherwise.

Don't copy any data without permission. This includes copying text or graphics - whether by using a scanner or by typing it in. The usual exceptions to copyright arrangements which allow you to photocopy parts of an article or book **do not apply** to the use of computers.

8. Respect Personal Information

The college has a Data Protection Policy with which you should be familiar.

You are obliged by law to keep any personal data secure, whether it is your own or someone else's. This means you should not share personal data with anyone who doesn't need it, or send it by email without encrypting the information first. Do not store personal data outside of the college network.

As an example, do not take or transfer images of learners or staff without the express permission of the subject (or parents/carers as appropriate).

9. Rules and Discipline

You are bound by the college's Security Policy and Acceptable Use Policy. You will have received a copy when you joined the College and are reminded of them at each login to the College's network. You should ensure you are familiar with these Rules. You can obtain another copy from the Learning Zone, the Intranet or the Computer Services Department.

If you break the Rules:

- Your permission to use College computers may be withdrawn.
- You are also liable to disciplinary action under College procedures.

If you believe you have been treated unfairly you have the right of appeal to the College Principal (if a learner) or the Human Resources Manager (if not a learner).