CRAFT Training ICT Acceptable Use Policy

CRAFT Training provides access to networked computers to support candidates academic work. Our Acceptable Use Policy is an extension to the rules. It includes guidelines for the safe and responsible use of the network and the internet, and identifies those activities which constitute an abuse of our ICT facilities.

In summary, users of CRAFT Training's network are prohibited from:

- logging on to the network with another user's account
- creating or sending offensive or harassing materials to others
- altering the settings of CRAFT Training's computers or making other changes which render them unusable by others
- tampering physically with the equipment
- installing software without authorisation
- hacking into unauthorised areas of the network
- accessing inappropriate websites or trying to circumvent the filtering system
- attempting to spread viruses via the network
- any form of illegal activity, including software and media piracy

Disciplinary action will be taken against those found to be in breach of the Acceptable Use Policy.

FULL POLICY: Candidates

This policy is an extension of the CRAFT Training's Rules, covering specifically the use of the CRAFT Training network and any computer equipment connected to it.

For the purpose of this document, the term *mobile device* will include laptops and electronic notebooks, PC tablets, mobile phones, games consoles or any other portable web-enabled computing device.

Section A - Computer Facilities

1. Overview

Every candidate will log in as "TRAINEE". This provides access to the computer network and a range of standard applications (word processing, spreadsheet, database etc.) as well as online facilities such as the Internet and electronic mail.

CRAFT Training's ICT facilities are provided to support candidates study in all subjects, and priority will always be given to those using computers for academic and other training-related work.

Access to the computer network is a privilege and it is the responsibility of candidates to restrict themselves to usage which is ethical and appropriate. **Failure to comply with this policy will result in disciplinary action.**

Computer Services staff are authorised to monitor all user accounts to ensure the security of the network; records of usage, stored files and email messages that have been sent or received may be scrutinised at any time (a) during routine system maintenance or (b) if there is reason to suspect misuse of the network. All candidate machines are monitored by software and inappropriate activity is reported to the ICT Tutor.

2. Rules

a. General Conduct and Use

i. Candidates should conduct themselves in an orderly and quiet fashion, and must always show consideration for other users.
ii. No food or drink may be consumed.
iii. Any damage to computers, furniture or fitments should be reported to a member of the staff without delay. The same applies to any apparent malfunction of equipment.
iv. Only one candidate should be seated and working at a computer at any one time.
v. Chairs should be placed tidily in computer rooms before leaving.

b. Use of the Network

i. Never, under any circumstances, use another person's account or attempt to log on as a system administrator.
ii. Vandalism is defined as any malicious attempt to harm, modify, or destroy data of another user. The CRAFT Training's network or other networks connected to the Internet must not be vandalised. This includes the uploading or creating of computer viruses.
iii. Harassment is defined as the persistent annoyance of another user, or interference with another user's work. Harassment must never occur; this includes, but is not limited to, the sending of unwanted email.
iv. If a candidate identifies a security problem on CRAFT Training's system he/she must notify the Tutor immediately. He/she must not demonstrate the problem to other users.
v. Candidates must not attempt to gain access to the local drive of any machine or to create local accounts (administrative or otherwise).
vi. Only software that has been provided on the network may be run on CRAFT Training's computers; this includes programmes run from USB devices, which should only be used for the transfer of data.

vii. Candidates are not permitted to import or download applications or games. In many cases it is illegal to do so.

viii. You are reminded that it is a breach of CRAFT Training's Plagiarism Policy (and of the rules of examination boards) to pass off another's work as your own. This includes copying and pasting information accessed online without proper acknowledgement.

ix. Candidates must be aware of, and comply with, the restrictions placed on certain kinds of usage; notably the playing of games on particular machines and at particular times of the day, where priority is given to academic work.

Section B - Internet and Email

1. Rules

a. General Netiquette

Candidates must not:

i. Send electronic communications which are impolite, indecent, abusive, discriminatory, racist or in any way intended to make the recipient feel uncomfortable.

ii. Disclose to a third party the personal details of any other candidate.

iii. Access any inappropriate Internet site.

iv. Breach another person's copyright in any material.

v. Upload or download any unauthorised software or attempt to run that software. In particular hacking, encryption and other system tools are expressly forbidden.

vi. Purchase goods or services via the computer network.

vii. Use the computer network to gain unauthorised access to any other computer network.

viii. Attempt to spread computer viruses.

ix. Engage in activities that are prohibited under UK Law. Thus the transmission of material subject to copyright or protected by trade secret is forbidden, as of course is any threatening or obscene matter.

b. Personal Safety

Candidates need to be aware that thoughtless use of email and the Internet may jeopardise their personal safety either at CRAFT Training or outside CRAFT Training. Candidates should therefore:

i. Be aware that any person they "meet" or communicate with online may pretend to be someone else.

ii. Never arrange a meeting in person with anyone they have "met" or only communicated with online without prior parental approval.

iii. Not respond to messages or bulletin board items that are indecent, suggestive, belligerent, discriminatory, threatening, or which make the student feel uncomfortable or unsafe in any way.

iv. If such a message is encountered the candidate should report it to his/her tutor and parents or via an online reporting service such as ThinkUKnow (http://www.thinkuknow.co.uk). .

v. Remember that anything they read online may not be accurate.

vi. Ignore offers that involve either financial transactions or personal meetings.

vii. Not disclose any personal details online, such as their home address or telephone number.