Codes of Practice for IT Users

(Students)

Code of Practice

Acceptable Use of Information Technology (IT) Facilities (Students)

If you use any College IT Facility you are automatically agreeing to comply with the terms of this Code of Practice.

1. Use of IT facilities, such as the network, computers, printers and the facilities associated with them e.g. software, data, email, internet, bulletin boards, data bases must be for College work, or other **authorised** use only. No 'private' work is permitted.

2. You are permitted to use the college IT equipment in accordance with any local conditions pertaining to that room or area. IT equipment not owned or installed by the college must not, under any circumstance, be connected to the college network.

3. All files created or stored by you on College IT facilities may, in the instance of suspected wrong doing, be subjected to inspection by College IT Technical Staff. Where evidence is found of misuse or of the illegal use of material they will be subject to removal and deletion.

4. You must comply with any local rules in force applicable to IT facilities provided by the College e.g. in Libraries and ILT Centres.

5. Specifically you must not:-

a) disclose to others your login name/password combination(s) or access, or attempt to access, computers at the College or elsewhere for which permission has not been granted

b) eat or drink in any IT facility

c) use or produce materials or resources to facilitate unauthorised corruption, changes, malfunction or access to any College or external IT facilities.

d) knowingly introduce a real, or hoax virus onto College IT systems

e) display, store, print or transmit images or text which could be considered offensive e.g. material of a sexual, pornographic, paedophilic, sexist, racist, libellous, threatening, defamatory or terrorist nature, or likely to bring the College into disrepute.

f) forge email signatures and/or headers, initiate and/or forward ‘chain’ or ‘junk’ or ‘harassing’ mail.

g) play unauthorised games, gamble or use unauthorised ‘chat-rooms’.

h) use, download, copy, store or supply copyright materials including software and retrieved data other than with the permission of the Copyright holder or under the terms of the license held by the College.

i) use a mobile phone to make voice calls in classrooms and other learning areas, e.g. Learning Centres. Mobile phones must be set to *silent* in all learning areas. The use of SMS/ MMS messaging in classrooms is prohibited without prior tutor authorisation.

6. The College cannot police the student use of external Web 2.0 and Social Networking web sites such as MySpace, Facebook and Blogger. However, if such sites are used inappropriately - e.g. to defame any member of staff or another student, or to access or publish offensive imagery – College disciplinary procedures may be invoked. Each college IT centre or room has its own rules regarding access to such sites – you need to ensure that you are aware of these local rules when using these centres.

7. When holding data on computers about living individuals, you must register that data and its uses, and treat it as required by the Data Protection Act 1998.

8. Whilst the College takes appropriate security measures against unauthorised access to, alteration, disclosure, destruction or accidental loss of personal and other data, it cannot and does not give any warranties or undertakings to you about security, confidentiality or integrity of data, personal or other. Make sure that you back-up your files!

Breaking these conditions may lead to College disciplinary procedures being invoked, with penalties which could include suspension from the use of College IT facilities for extended periods. Serious cases may lead to expulsion from the College and may involve civil or criminal action being taken against the user.