

IT Acceptable Use Policy

1 – SCOPE

1.1 – The College's Internet access is provided by the United Kingdom Education & Research Networking Association (UKERNA). UKERNA have developed and now operate the Joint Academic Network (JANET) under a Service Level Agreement from the Joint Information Systems Committee (JISC) of the UK Higher and Further Education Funding Councils.

1.2 – UKERNA requires the College to agree to abide by and adhere to various terms and conditions when using the service. The most important obligations placed on College staff and students using the JANET system are as follows:

"The User Organisation (the College) will ensure that all use of JANET by its members, staff, students and anyone else to whom JANET is made available by the User Organisation conforms to the current version of the JANET Acceptable Use Policy and its Security Policy."

1.3 – Failure to comply with these Terms and Conditions may lead to the loss of the service, i.e., the link to the Internet. It is essential that all users of Internet and Internet email are made aware of the contents of these policies and adhere to them.

1.4 – JISC & UKERNA also recommend that every HE & FE College instigates its own Acceptable Use of IT Policy (AUP) to make all users aware of the Terms and Conditions laid down by UKERNA as to the AUP of JANET and to protect itself and its staff by making them aware of all relevant legislation.

1.5 – This code applies to all users of College computer facilities, i.e., all staff (academic and support) and all students.

2 – AIMS

2.1 – To ensure security of College IT Systems.

2.2 – To safeguard The College's business.

2.3 – To inform all users (staff and students) of all relevant legislation relating to IT.

2.4 – To provide an appropriate teaching and learning environment for all College IT Users.

2.5 – To ensure all users of College IT Systems are aware of the Terms and Conditions laid down by UKERNA

3 – INTERNET AND INTERNET EMAIL USAGE

3.1 – Use of the Internet for College work purposes is encouraged and permitted within the following guidelines:

- It complies with the JANET AUP It does not contravene any applicable legislation.

3.2 – Reasonable private and personal use of the Internet is encouraged and permitted for College staff within the guidelines as in 3.1 above and also:

- It is carried out in the user's own time.

3.3 – The College undertakes to provide an internet email account for all staff and students as "username"@coll.ac.uk

3.4 – There may be certain periods when private use of the internet will not be permitted, for example during enrolment and on-line examinations.

3.5 – Copyright applies to all text, pictures, video and sound, including those sent by e-mail or on the Internet. Files containing such copyright protected material may be downloaded, but not forwarded or transmitted to third parties without the permission of the author of the material or an acknowledgement of the original source of the material, as appropriate.

3.6 – Copyrighted software must not be downloaded. Such copyrighted software will include screen-savers.

3.7 – Users should not import non-text files or unknown messages on The College's system without having them scanned for viruses. College systems automatically scan for known viruses. If a virus is detected, contact MITS immediately.

4 – MONITORING AND INTERCEPTION OF DATA

4.1 – The College reserves the right to monitor the usage of all College IT facilities in order to:

- ensure the security of its systems
- to safeguard those systems from virus infection and spam invasion.

- to monitor and prevent access to inappropriate internet sites in order to provide as secure an environment for students as possible.
- to ensure compliance with the [JANET AUP](#) and [Security Policy](#)

4.2 – In order to comply with current legislation, [Regulation of Investigatory Powers Act 2000, the Telecommunications (Lawful Business Practice)(Interception of Communications) Regulations and Data Protection Code of Practice] , it is necessary for The College to obtain the express permission of all users to enable the monitoring of these systems. College staff will supply their express permission by signing the user application form. Students will give their consent by connecting online to validate their network login.

5 – GENERAL USAGE

5.1 – College staff and students are responsible for safeguarding their password(s) for the system(s). For security reasons, individual password(s) must not be printed, stored on-line or given to others.

5.2 – A User's ability to connect to other computer systems through the network does not imply a right to connect to those systems unless authorised to do so.

5.3 – Advertising – Users of College IT resources are not permitted to create, place or distribute any advertisement which is of a commercial nature.