Castle College Nottingham – IT Acceptable Use Policy

The College seeks to promote and facilitate the proper and extensive use of computing/IT in the interests of learning and research. Whilst the traditions of academic freedom will be fully respected, this also requires responsible and legal use of the technologies and facilities made available to students and staff of the College.

This Acceptable Use Policy is intended to provide a framework for such use of Castle College's computing/IT resources. It applies to all computing and networking facilities provided by any department or section of the College. It should be interpreted such that it has the widest application, in particular references to IT Support should, where appropriate, be taken to include departmental or other system managers responsible for the provision of a computing service.

This policy also recognises and supports additional policies that are created for specific purposes (e.g. course specific guidelines, Staff E-mail, Internet and Telephone Usage policy by Human Resources). Interpretation of such policies must also take into account the requirements within this college-wide IT policy.

The Acceptable Use Policy is taken to include the JANET Acceptable Use Policy published by the United Kingdom Educational and Research Network Association (UKERNA), together with its associated Copyright Acknowledgement. Members of the College and all other users of the College's facilities are bound by the provisions of these policies in addition to this Acceptable Use Policy.

1) Purpose of Use

College computing resources are provided to facilitate a person's work as an employee or student of the College, specifically for educational, training, administrative or research purposes.
Use for other purposes, such as personal electronic mail or recreational use of the World Wide Web or Usenet News, is a withdrawable privilege not a right. Any such use must not interfere with the user's duties or studies or any other person's use of computer systems and must not, in any way, bring the College into disrepute.
Priority must always be granted to those needing facilities for academic work.
Commercial work for outside bodies, using centrally managed services requires explicit permission from the Head of ISLT; such use, whether or not authorised, may be liable to charge and improper use may lead to disciplinary action.

2) Authorisation

In order to use the computing facilities of Castle College a person must first be authorised. Registration of all monthly salaried employees and registered students is carried out automatically. Other members of the College should apply to IT Support for registration. Registration to use College IT services implies and is conditional upon acceptance of this Acceptable Use Policy.
The registration procedure grants authorisation to use the core facilities of the College IT system. Following registration, a username and password will be allocated. Registration for other services may be requested by application to IT Support.
All individually allocated usernames and passwords are for the exclusive use of the individual to whom they are allocated. The user is personally responsible and accountable for all activities carried out under their username. The password associated with a particular personal username must not be divulged to another person except, in exceptional circumstances, to senior members of IT staff (or with delegated authority of senior staff). Where IT staff have been made aware of passwords it is recommended they be changed as soon as possible. Attempts to access or use any username, which is not authorised to the user, are prohibited. No-one may use, or attempt to use, computing resources allocated to another person, except when authorised by the provider of those resources.
All users must correctly identify themselves at all times. A user must not masquerade as another, withhold his/her identity or tamper with audit trails. A user should take all reasonable precautions to protect their resources. In particular, passwords used must adhere to accepted good password practice. Advice on what constitutes a good password may be obtained from IT Support Intranet pages.

3) Privacy

It should be noted that systems staff, who have appropriate privileges, have the ability to access all files, including electronic mail files, stored on a computer which they manage. As College computers are the property of the College the College shall have the right to inspect or audit files, software and usage logs as appropriate and necessary to enforce this policy. This access will, however, be restricted and will respect the rights of privacy for users.
Software is used to monitor activity via web browsing and email. This information is logged and can be viewed only by senior systems staff for network management and policy enforcement purposes only.
Remote viewing and/or remote control software may be utilised to enforce this policy and maintain/manage the computer network.
Access to staff files is restricted to system administrators and will not be given to another member of staff unless authorised by the Head of ISLT, who will use his/her discretion in consultation with a senior officer of the College, if appropriate. In such circumstances the Head of Department or Section, or more senior line manager, will be informed, and will normally be consulted prior to action being taken. Such access will normally only be granted where a breach of the law or this policy is suspected.

Student privacy is seen by the College as a privilege and not a right, hence students should not expect to hold or pass information, which they would not wish to be seen by members of staff. Systems staff are authorised to release the contents of a student's files to any member of staff who has a work-based reason for requiring this access.
Files, which are left behind after a student or member of staff leaves the College, will be considered to be the property of the College.

4) Behaviour

No person shall jeopardise the integrity, performance or reliability of computer equipment, software, data and other stored information. The integrity of the College's computer systems is jeopardised if users do not take adequate precautions against malicious software, such as computer virus programs. Reasonable care should also be taken to ensure that resource use does not result in a denial of service to others.
Conventional norms of behaviour apply to computer based information technology just as they would apply to more traditional media. Within the College setting this should also be taken to mean that the traditions of academic freedom will always be respected. The College, as expressed in its Equal Opportunities Policy, is committed to achieving an educational and working environment which provides equality of opportunity, and freedom from discrimination on the grounds of race, religion, sex, class, sexual orientation, age, disability or special need.
Distributing material, which is offensive, obscene or abusive, may be illegal and may also contravene College codes on harassment. Users of College computer systems must make themselves familiar with, and comply with, the College codes concerning all forms of harassment.
No user shall interfere or attempt to interfere in any way with information belonging to or material prepared by another user. Similarly no user shall make unauthorised copies of information belonging to another user. The same conventions of privacy should apply to electronically held information as to that held on traditional media such as paper.
For specific services the College may provide more detailed guidelines (e.g. Staff Email, Internet and Telephone Usage policy issued by Human Resources) in addition to the policies provided in this Acceptable Use Policy. Users of services external to the College are expected to abide by any rules and codes of conduct applying to such services.

5) Definitions of Acceptable & Unacceptable Usage

Unacceptable use of College computers and network resources may be summarised as:

- the retention or propagation of material that is offensive, obscene or indecent, except in the course of recognised research or teaching that is permitted under UK and international law; propagation will normally be considered to be a much more serious offence;
- causing annoyance, inconvenience or needless anxiety to others, as specified in the JANET Acceptable Use Policy;

- defamation (genuine scholarly criticism is permitted);
- intellectual property rights infringement, including copyright, trademark, patent, design and moral rights;
- unsolicited advertising, often referred to as "spamming";
- attempts to break into or damage computer systems or data held thereon;
- attempts to access or actions intended to facilitate access to computers or software applications for which the individual is not authorised
- unauthorised resale of College or JANET services or information

These restrictions should be taken to mean, for example, that the following activities will normally be considered to be a breach of this policy:

- the distribution or storage by any means of pirated software
- non-academic activities which generate heavy network traffic, especially those which interfere with others' legitimate use of IT services or which incur financial costs
- frivolous use of College owned Computer laboratories, especially where such activities interfere with others' legitimate use of IT services
- the deliberate viewing and/or printing of pornographic images
- the passing on of electronic chain mail
- the use of departmental academic mailing lists for non-academic purposes
- the purchase of blank CDs for the purpose of copying unlicensed copyright software
- the use of other people's web site material without the express permission of the copyright holder

This list is not exhaustive but is intended to be indicative of the activities that constitute a breach of this policy.

The installed machine on each network socket must be a workstation only and not provide any server-based services, including, but not limited to, Web, FTP, IRC, Streaming Media or email services.

Acceptable uses may include:

Personal email and recreational use of Internet services, as long as these are in keeping with the framework defined in this policy document and do not interfere with one's duties, studies or the work of others; and advertising via electronic notice boards, intended for this purpose, or via other College approved mechanisms. However such use must be regarded as a privilege and not as a right and may be withdrawn if abused or if the user is subject to a related disciplinary procedure.

6) Legal Constraints

Any software and/or hard copy of data or information which is not generated by the user personally and which may become available through the use of College computing or communications resources shall not be copied or used without permission of the College or the copyright owner. In particular, it is the responsibility of the user to check the terms and conditions of any licence for the

use of the software or information and to abide by them. Software and/or information provided by the College may only be used as part of the user's duties as an employee or student of the College or for educational purposes. The user agrees to abide by all the licensing agreements for software entered into by the College with other parties.

In the case of private work and other personal use of computing facilities, the College will not accept any liability for loss, damage, injury or expense that may result.

The user undertakes to comply with the provisions of the following Acts of Parliament (or any re-enactment thereof): Computer Misuse Act 1990, Criminal Justice and Public Order Act 1994, Copyright, Designs and Patents Act 1988, Trade Marks Act 1994, Data Protection Act 1984, Data Protection Act 1998; as well as all other relevant legislation and legal precedent. See below for a summary of the main points. Copies of these documents are available upon request. Further advice should be obtained through the Head of ISLT in the first instance.

Computer Misuse Act 1990

This Act makes it an offence :-

- to erase or amend data or programs without authority
- to obtain unauthorised access to a computer
- to "eavesdrop" on a computer
- to make unauthorised use of computer time or facilities
- maliciously to corrupt or erase data or programs
- to deny access to authorised users.

Criminal Justice & Public Order Act 1994

This defines a criminal offence of intentional harassment, which covers all forms of harassment, including sexual. A person is guilty of an offence if, with intent to cause a person harassment, alarm or distress, s/he:-

- uses threatening, abusive or insulting words or behaviour, or disorderly behaviour; or
- displays any writing, sign or other visible representation which is threatening, abusive or insulting, thereby causing that or another person harassment, alarm or distress.

Copyright, Designs and Patents Act 1988

This Act, together with a number of Statutory Instruments that have amended and extended it, controls copyright law. It makes it an offence to copy all, or a substantial part, which can be a quite small portion, of a copyright work. There are, however, certain limited user permissions, such as fair dealing, which means under certain circumstances permission is not needed to copy small amounts for

research or private study. The Act also provides for Moral Rights, whereby authors can sue if their name is not included in a work they wrote, or if the work has been amended in such a way to impugn their reputation. Copyright covers materials in print and electronic form, and includes words, images, sound, moving images, TV broadcasts and many other media.

Trade Marks Act 1994

This Act provides protection for Registered Trade Marks, which can be any symbol (words or images) or even shapes of objects that are associated with a particular set of goods or services. Anyone who uses a Registered Trade Mark without permission can be sued. They can also be sued if they use a Mark that is confusingly similar to an existing Mark.

Data Protection Acts 1984 and 1998

The 1984 Act requires that any person or organisation processing information about individuals in machine-readable form must register with the Data Protection Registrar and must abide by a number of principles. It also gives individuals the right to inspect information held about them, to demand amendments to records if they are inaccurate, and to sue if they suffer financial damage as a result of incorrect information.

7) College Discipline

Staff or students who break this Acceptable Use Policy will find themselves subject to the College's disciplinary procedures and may be subject to criminal proceedings. The College reserves its right to take legal action against individuals who cause it to be involved in legal proceedings as a result of their violation of licensing agreements and/or other contraventions of this policy.

8) Policy Supervision and Advice

The responsibility for the supervision of this Acceptable Use Policy is delegated to IT Support. A senior member of IT Support, normally the System Support Manager or their nominee, will be designated as the person responsible for the day to day management of the policy's enforcement. He/she will liaise with the Head of ISLT and other College Managers as required. Procedural guidelines will be published from time to time as a separate document.

Any suspected breach of this policy should be reported to a member of IT Support staff. The responsible senior member will then take the appropriate action in conjunction with other relevant sections of the College. Should evidence be found that supports a suspected breach of this policy this will in most cases trigger a formal investigation into events surrounding the incident – the outcome of which may result in actions under our disciplinary procedure. IT Support staff will also take action when infringements are detected in the course of their normal duties. Actions will include, where relevant, immediate removal from online information

systems of material that is believed to infringe the law. The College reserves the right to audit and/or suspend without notice any account pending any enquiry.

A variety of software products are in use to support enforcement of this policy. These include, but are not restricted to; Internet browser filters and loggers, email filters and loggers, software auditing, hardware auditing, file detection and central logging, network 'sniffers', image signature checkers against Scotland Yard databases of pornography and paedophilia, and automated screen capture. Where activity triggers these products we reserve the right to view the activity (via remote access or screen capture) in order to enforce this policy – or in the case of false triggers so that the process may be enhanced and made more accurate. Where this involves work or information covered by your right of privacy we will respect that privacy at all times.

This policy is not exhaustive and inevitably new social and technical developments will lead to further uses which are not fully covered. In the first instance students should address questions concerning what is acceptable to their supervisor; staff should initially contact their Head of Department/Faculty or the Head of ISLT. Where there is any doubt the matter should be raised with the System Support Manager, IT, who will ensure that all such questions are dealt with at the appropriate level within the College.

THE LATEST VERSION CAN BE FOUND ON THE COLLEGE INTRANET AT;
http://intranet.broxtowe.ac.uk/structure/departments/islt/docs/AcceptableUsePolicy.doc

This policy is also available in larger print. Please ask your Manager/Tutor to obtain a copy from the IT Department.