Acceptable Use Policy – Internet and Email - Students

Ref HR01

Acceptable Use Policy – Internet and Email - Students

Review Date: August 2016
INTRODUCTION

Information and communication technologies (ICT) are continually changing. Colleges have an important role to educate and train people in the proper use of these technologies.

North East Scotland College (the College) is committed to bringing the maximum benefits of ICT possible to its students, and to equipping them with the knowledge, skills and attitudes that will enable them to thrive in the digital age.

It must be borne in mind, however, that ICT exists within the College for the primary purpose of supporting the College’s role in providing education and training. ICT assists the College in discharging these functions and provides students with an opportunity to become familiar with ICT.

However, the College recognises that misuse of ICT by students can occur. This can be by, for example, accessing or transmitting offensive or unacceptable material or simply spending a disproportionate amount of time using ICT for personal or non-educational reasons.

This policy applies to all students of the College.

ACCEPTABLE USE

In accessing the College’s ICT facilities, all students will be deemed to have accepted the terms of this Acceptable Use Policy.

The primary role of electronic media, as with other resources within the College, is to support educational aims. ICT is provided to help the students learn more effectively and productively. College based ICT facilities must not be used for commercial purposes such as running a business or selling goods or services.

ICT must be used for the primary purpose of educational and College business use. Limited personal use of ICT will be acceptable as long as the facilities afforded to students are not abused. Personal use of electronic media is a privilege and not a right and must not be permitted to conflict with the educational aims of the College. Excessive personal use not only represents a waste of College resources but it also prevents other legitimate users from accessing facilities. We may withdraw permission for personal use at any time or restrict access at our discretion.
A number of key factors should be used to inform judgement on whether a particular use of College facilities is acceptable or unacceptable.

1. **Cost** - does the use involve significant extra costs to the College, and if so are these outweighed by any benefits?
2. **Time** - does this use impinge on study time?
3. **Acceptable content** - does it comply with this policy?
4. **Legal and ethical issues** - is the activity legal - is it ethical?
5. **Reputation** - Is it an activity that will bring the College into disrepute?
6. **Compliance** – Does it comply with our other policies including Equality & Diversity Policy, Anti-Harassment Policy, Data Protection Policy and Disciplinary Procedure?

The following are examples of acceptable use. However, in all cases, you should be aware that personal use of our systems may be monitored (please see below) and, where breaches of this policy are found, action may be taken under the Student Disciplinary Code (please see below).

We reserve the right to restrict or prevent access to certain telephone numbers or internet sites if we consider personal use to be excessive or inappropriate.

### 1. PERSONAL USE OF EMAIL

Personal use of email on College ICT systems is permitted provided that it does not impinge in any way on class time, or involve unacceptable content. Unauthorised encryption of email or other communications on College systems or equipment is not permitted at any time.

Students transmitting messages or communicating electronically on ICT facilities shall at all times use polite and appropriate language. Consideration must be given by students as to how the recipient of any message or email (or a third party obtaining sight of any message or email) will view the tone and language content of any such communication. All email should clearly identify the actual sender with no attempt made to masquerade or to misrepresent the identity of the actual sender.
2. **USE OF MAILING LISTS AND NEWSGROUPS**

Mailing lists, newsgroups and blogs are useful for the exchange of information and ideas. When using such systems, however, it must be borne in mind that they are essentially public spaces, and that contributing to them may have legal repercussions.

3. **PERSONAL USE OF THE WEB**

Provided that content is acceptable, and that use does not impinge on class time, a limited use of the internet will be regarded as acceptable.

When downloading files for personal use, students must ensure that they do not compromise the security or performance of either the machine which they are using or the College network as a whole. Specifically they must manage their personal files so as not to take up excessive space on the hard drive of the machine they are using or on College servers. This can be done by moving them to personal media such as a disc or USB drive.

The College cannot guarantee the security of any data stored on local machines. The College reserves the right to open any data or files stored on local hard disc or otherwise on the network. Students are responsible for their own back-ups in respect of any data or files that are important to them. The College takes no responsibility for any data loss or damage to any media used on College machines such as, for example, CD's, DVD's and USB drives.

4. **E-COMMERCE**

Making personal credit card purchases over the Internet will be acceptable, so long as the College is not being used in any way to imply the official status of the purchaser. However, using College web space to run a non-College business, for example, is clearly unacceptable.

5. **SOCIAL MEDIA**

While the bulk of current use of social media is recreational, these systems can have considerable potential in collaborative learning. However, engaging with social media on the College ICT systems too often, or purely for personal use, can be a waste of the College’s resources. This should be borne in mind when deciding what level of use of social media will likely be deemed acceptable.
6. COMPUTER GAMES

The use of computer games can form a part of some courses. In addition, there are educational resources which take the form of games. This type of use is clearly acceptable. However, extensive use of College facilities simply for game-playing ties up resources which could otherwise be put to better use, and brings limited educational gains. The use of College facilities for playing games, other than those of a specific educational benefit, will therefore be considered to be unacceptable use.

PROHIBITED USE OF OUR SYSTEMS

Misuse or excessive personal use of our ICT facilities will be dealt with under the Student Disciplinary Code. Misuse of the internet can in some circumstances be a criminal offence. Misuse of the e-mail system or inappropriate use of the internet by participating in terrorist activities, online gambling or chain letters or by creating, viewing, accessing, transmitting or downloading any of the following material will usually amount to a serious breach of the Student Disciplinary Code (this list is not exhaustive):

(a) pornographic material (that is, writing, pictures, films and video clips of a sexually explicit or arousing nature);

(b) offensive, obscene, or criminal material;

(c) material which is liable to cause embarrassment to us or to our stakeholders;

(d) information which may be, or could reasonably be expected to be, subject to provisions of counter-terrorism legislation;

(e) a false and defamatory statement about any person or organisation;

(f) material which is discriminatory, offensive, derogatory or may cause embarrassment to others (including material which breaches our Equality & Diversity Policy or our Anti-harassment and Bullying Policy);

(g) confidential information about us or any of our staff or students;

(h) any other statement which is likely to create any criminal or civil liability (for you or us); or
(i) material in breach of copyright.

Any such action will be treated very seriously and is likely to result in expulsion.

Where evidence of misuse is found we may undertake a more detailed investigation in accordance with the Student Disciplinary Code, involving the examination and disclosure of monitoring records to those nominated to undertake the investigation and any witnesses or supervisors involved in the Student Disciplinary Code.

Any information obtained may be handed to the police in connection with a criminal investigation.

CRIMINAL CONDUCT

A number of activities related to the use of the Internet or email are covered by law, by College policy or regulations and are otherwise clearly unacceptable. These will be regarded by the College as constituting misconduct and any student involved will be subject to disciplinary action up to expulsion. These include: terrorist activities, on-line stalking, grooming, internet luring, soliciting of children by computer, defamation, retention of offensive screen savers, fraud, software theft, damage to College systems, retention of other people’s personal details/information, drug-related activities, or any other illegal activity.

In addition, Section 26 of the Counter-Terrorism and Security Act 2015 places a duty on the College to have, in the exercise of its functions, due regard to the need to prevent people from being drawn into terrorism. This means that the College will place an appropriate amount of weight on the need to prevent people being drawn into terrorism in the application of this policy.

SECURITY

All students accessing College based ICT facilities must only do so using their own unique login name or password. This must be kept confidential and changed regularly. Under no circumstances may students use someone else’s login name or password.

MONITORING AND FILTERING THE USE OF COLLEGE ICT FACILITIES

In order to enforce this policy and ensure that ICT facilities are not being misused, the College will randomly monitor email and internet usage by students. Monitoring is only carried out to the extent
permitted or as required by law and as necessary and justifiable for business purposes.

We reserve the right to retrieve the contents of e-mail messages or check internet usage (including pages visited and searches made) as reasonably necessary in the interests of the College, including for the following purposes (this list is not exhaustive):

(a) to monitor whether the use of the e-mail system or the internet is legitimate and in accordance with this policy;

(b) to find lost messages or to retrieve messages lost due to computer failure;

(c) to assist in the investigation of alleged wrongdoing; or

(d) to comply with any legal obligation.

The College currently employs filtering software to limit access to websites that contain inappropriate, offensive or illegal content. Such content includes (but is not limited to) obscene or pornographic, sexist, racist, discriminatory or other offensive material. Inappropriate sites includes (but is not limited to) those with content relating to gambling, alcohol and tobacco, illegal drugs, violence and terrorist activities.

If access to these sites is attempted then an ‘Access Denied/Site Blocked’ dialogue box will be displayed. Attempted visits to these sites will be monitored by the College’s IT Department.

If a student finds that a website is blocked which they have a genuine educational reason for using, they should submit a request to the [IT Department] for potential access. Such requests must be approved by the [individual’s supervisor], and either the [Head of IT] or the [Head of HR].

OTHER ISSUES RELATING TO THE USE OF THE INTERNET AND EMAIL

1. COPYRIGHT

Copyright issues as they relate to the Internet are in flux. Copyright as it applies to the Internet should be seen as being more stringent than that applying to other media. There are no special arrangements relating to the Internet which extend students’ copying rights beyond those allowed by general copyright law. Nor do general copyright agreements entered
Acceptable Use Policy – Internet and Email - Students

into by the College currently extend to materials on the Internet. It is safest to assume that, unless otherwise stated on the web pages concerned, copies (whether paper-based or electronic) cannot be made. If you wish to make use of pages that will involve any kind of copying, the best approach is to email the copyright holder and ask for permission. However, when using internet pages it is good practice to use a link to the site rather than attempting to copy pages. Clarification on copyright issues can be sought from the Records Manager.

Importantly, students making use of ICT facilities must respect copyright and not plagiarise the work of others. Please see the Copyright Policy for Students.

2. COPYING OF COLLEGE SOFTWARE

Where this is not specifically allowed by agreements pertaining to the software, or entered into specifically by the College, this is illegal. Any copying of College software must be authorised, in advance, by the Head of ITTS.

3. ENCRYPTION

Encryption software allows messages sent between computers to be encoded in such a way that they cannot be read by third parties. In some cases, for example, when securely sending credit card details, this happens automatically. In others, such as the sending of email, the sender actively invokes it. Email should only be encrypted using College-approved software, and where this is required for purposes of confidentiality. College email systems must not be used for the sending of confidential private messages, and non-approved encryption software must not be used in order to achieve confidentiality.

4. SAFE SURFING

Internet systems are very effective at hiding the true identities of users from each other. This accounts for some of their appeal, allowing as they do the adoption of different personae and the ability to communicate openly in relative anonymity. This and other characteristics of the Internet do, however, open the way for various kinds of abuse. We therefore recommend that Students are live to these issues when using the internet to ensure that they engage in ‘safe surfing’.
5. **NETIQUETTE**

In brief, netiquette is good manners for the Internet. Students must observe netiquette as appropriate to the systems they are using and to avoid causing offence to other users.

6. **VIRUSES**

Viruses can be transferred between computers either over the Internet or by using USB drives or other media between machines. Students should adopt sensible practices both when using College machines and those they have access to at home to ensure no viruses are transferred.
USE OF USER-OWNED DEVICES WITH COLLEGE NETWORKS

The College recognises that students may wish to use their own personal ICT equipment while in the College, and may also wish to connect it to the College network. At present laptops, tablets and smart phones are likely to be the most common devices.

This is a trend which the College views as positive and which it seeks to encourage through the use of support Bring Your Own Device (BYOD). At the same time this brings with it certain risks, including security risks, which must be effectively managed.

In order to do this, and to comply with current legislation, anyone wishing to use their personal device must sign and return the declaration at the end of the Policy and the following will apply:

1. At all times when any device is connected to College networks or power supplies it must be used only in accordance with all College Policies and regulations, and the instructions of College staff.

2. Where a device is to be connected to College power supplies, whether for use or for recharging, the device must be EITHER i) less than 3 years old OR ii) PAT tested. Users should only connect to College power supplies which are indicated by the College as being available for this when this can be done in a way which is compatible with the health and safety of all, and does not create any kind of hazard. Care must be taken, for example, to ensure that there are no trailing cables which might create a trip hazard. Where PAT testing is required, it is the responsibility of the owner of the equipment.

3. No device should be connected to the College network, whether wirelessly or in any other way, with any malicious intent, or for any purpose incompatible with the College’s role as a publicly funded provider of education and training (it should not be for any commercial purpose, for example, or with the aim of deliberately damaging the network).

4. The user of any personal device must take all reasonable steps to ensure that the use of their device does not compromise or damage the College network in any way. They must ensure, for example, that proper virus protection is installed and used on the device.
5. The user must at all times use their best efforts to physically secure the personal device against loss, theft or use by persons who the College has not authorised to use the device and protect the device with a pin or password. If the security of the device is compromised this should be reported to the College immediately.

6. All devices are connected to College power supplies or networks entirely at the user’s own risk. In agreeing to the terms of the College ‘Declaration and Agreement – Acceptable Use’ users agree that the College will not be responsible for any loss, damage to the device, or damage to or corruption of data held on the device and/or liability arising out of its use which results from such connection.

7. Users should make use of the normal facilities provided by the College for access to the College network by user-owned devices. They should not seek to access the network, circumvent security processes or bypass network access controls that are in place. Specifically they should not seek to “hack” into the network in any way whether for malicious or other intent, attempt to bypass Internet access controls or hide activities e.g. by the use of proxy services.

8. Where damage to the College network, power supply, or other infrastructure occurs through negligence or malice on the part of the device user, or through failure to comply with College policy and regulations, the user will be held liable for the damage caused. Such a situation would arise, for example, where damage results relating to: a device which is more than 3 years old and has not been PAT tested; malicious infection of the College network with a virus; accidental infection of the College network with a virus where appropriate measures have not been taken to prevent this; damage caused through unauthorised access to the College network i.e. hacking (this list is not exhaustive).

9. Use of the College network to facilitate threatening, intimidating, abusive behaviour towards another person, even via privately owned devices, shall be deemed to be a breach of the Acceptable use Policy and the Bullying Policy. In such cases appropriate action will be taken in accordance with the Student Disciplinary Code.

10. The College reserves the right to refuse or remove permission for your device to connect with College systems.
11. All materials, data, communications and information created on, transmitted to, received or printed from, or stored or recorded on a personal device during the course of business or on our behalf is our property, regardless of who owns the device.

12. We reserve the right to monitor, intercept, review and erase, without further notice, all content on the personal device that has been created for us or on our behalf, as well as inspect the device. Users must co-operate with the College to enable such inspection, access and review, including providing any passwords or pin necessary to access the personal device or relevant applications. A failure to co-operate with the College in this way may result in disciplinary action being taken, up to and including expulsion.

13. It is possible that personal data may be inadvertently monitored, intercepted, reviewed or erased. Therefore, you should have no expectation of privacy in any data held on the personal device if used for business purposes. Students are advised not to use our ICT systems for any matter that they intend to keep private or confidential.

14. Monitoring, intercepting, reviewing or erasing of content will only be carried out to the extent permitted by law, for legitimate business purposes, including, without limitation, in order to prevent misuse of the personal device and protect College data; ensure compliance with our rules, standards of conduct and policies in force from time to time (including the Acceptable Use Policy); and ensure that students do not use our facilities or systems for any unlawful purposes or activities that may damage our business or reputation.

15. By agreeing to the terms of the College’s ‘Declaration and Agreement – Acceptable Use’, you confirm your agreement (without further notice or permission) to such monitoring and to our right to copy, erase or remotely wipe the entire personal device (including any personal data stored on the device).