

Acceptable Use Policy – Internet and Email



ABERDEEN COLLEGE®



HR01

Acceptable Use Policy – Internet and Email

Review Date: December 2012

Acceptable Use Policy – Internet and Email

Introduction

Information and communication technologies (ICT) such as the Internet are radically changing the world in which we live and work. Colleges have an important role to educate and train people in the proper use of them.

Aberdeen College is committed to bringing the maximum benefits of ICT possible to its students and staff, 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 information technology.

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

In order to ensure that the educational objectives of the College are being fulfilled, and that ICT facilities are not being misused, the College reserves the right to monitor the use of e-mail and internet activity in terms of this policy.

Acceptable Use

All staff and students accessing ICT facilities will only do so using their own unique login name or password. Under no circumstances may they use someone else's login name or password. Access to ICT facilities is subject to all staff and students expressly accepting the terms of this Acceptable Use Policy each and every time they log in. The College reserves the right to update this Policy at any time.

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 and help staff work more effectively and productively. College ICT facilities must not be used for commercial purposes such as running a business or selling goods or services.

Acceptable Use Policy – Internet and Email

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 staff and students are not abused. Personal use of electronic media 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.

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 students' study time or staff work time?
3. Acceptable content - does it comply with College policy?
4. Legal and ethical issues - is the activity legal - is it ethical?
5. Is it an activity that will bring the College into disrepute?

The following are examples of acceptable use.

1. **Personal use of e-mail**

Personal use of e-mail provided that it does not impinge in any way on class time or study time in the case of students, and on hours of work in the case of staff, or involve unacceptable content, is an acceptable use of the College facilities. Unauthorised encryption of e-mail or other communications on College systems or equipment is not permitted.

It is not acceptable to use the College e-mail system to send jokes the content of which is sexist, racist or in any other way contravenes the College's Equal Opportunities Policy. This is because what may appear amusing to one person may be viewed as offensive or distasteful to others. It is also unacceptable to send e-mail messages of a sexual or offensive nature or to forward any e-mails of this nature following receipt. Random monitoring of activity will be carried out to ensure that unacceptable use is not being made of College computing facilities.

Staff and students transmitting messages or communicating electronically on ICT facilities shall at all times use polite and appropriate language consistent with their role within the College. Consideration must be given by staff and students as to how the recipient of any message or email (or a third

Acceptable Use Policy – Internet and Email

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. Further, neither students nor staff shall use the ICT facilities to make appointments to meet people they have made contact with via the internet.

The misuse of the College email system will be regarded as a disciplinary matter and disciplinary action up to and including dismissal may be taken against staff who have been found to have misused this facility.

2. Use of mailing lists and newsgroups

Mailing lists, newsgroups and web logs provide useful fora for the exchange of information and ideas between people involved in related fields of activity or interest. They can also contribute to professional development. When using such systems, however, it must be borne in mind that they are essentially public spaces, and that contributing to them may be seen as equivalent to publishing under the law. They may also be seen as reflecting on the College itself. Postings must, therefore, not be made which:

- might be, or might be construed to be defamatory;
- involve breach of copyright;
- express negative opinions about the College and its staff or might be construed as such;
- might, through the nature of their content, reflect negatively on the College.

When using these systems, staff should use a signature file or other disclaimer, indicating that any views expressed are their own, and not the official view of the College. It should be recognised, however, that the use of a College e-mail address, and the fact that a contributor is a College employee, implies a degree of official status. The use of such a signature file does not, therefore, release an employee from the obligations outlined above.

3. Personal use of the Web

Provided that content is acceptable, and that use does not impinge on study or work time a limited use of the internet will be regarded as acceptable. Staff may, therefore, use the Web during lunch or coffee breaks. Staff and students may not, however, access web sites which may be regarded as offensive or unsuitable. By way of example, unsuitable sites include any sites which show images of nudity, images of a

Acceptable Use Policy – Internet and Email

sexual nature or contain explicit dialogue. Internet sites which promote racism, sexism, religious intolerance, homophobia, or political violence may not be accessed. Anyone found accessing, downloading, distributing, reading or retaining for a screen saver, material from any such site will be subject to the College's Disciplinary Procedure.

When downloading files for personal use, staff and students must 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 pen drive.

The College cannot guarantee the security of any data stored by any such local machines and the College reserves the right to open any data or files stored on local hard disc or otherwise on the network. Staff and 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 responsibility for damage to any media used on College machines such as, for example, floppy discs, zip discs and CD ROMs.

The College will report any use of its ICT facilities for illegal purposes to the police

4. **E-commerce**

Making personal credit card purchases over the Internet during breaks 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. **Chatting**

While the bulk of current use of chat systems is recreational, these systems can have considerable potential in collaborative learning and working. At the same time the recreational use of these systems can be very time-consuming and, therefore, wasteful of College resources. However, many "chat rooms" are of a sexual nature, or are used for the exchange of material of a sexual nature. The best approach to the use of appropriate chat systems is probably to integrate them in a controlled way into courses. Where recreational use of chat is excessive, is in conflict with other use of resources or is impinging on work and study time it will be regarded as

Acceptable Use Policy – Internet and Email

unacceptable. Also, where content is inappropriate, this will clearly be an unacceptable use of College facilities.

6. Computer Games

The use of computer games forms a part of some courses. In addition, there are educational resources which take the form of games. This type of use is clearly acceptable. Like chat rooms, 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 should, therefore, be considered as unacceptable use.

The playing of computer games by staff at any time (including lunch breaks) is an unacceptable use of College equipment. The use of facilities for this purpose in open areas of the College, such as the IT Centre, libraries, offices and reception areas, sets a poor example to students and gives a poor impression of the College to members of the public and visitors.

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 staff copying rights beyond those allowed by general copyright law. Nor do general copyright agreements entered 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 e-mail the copyright holder and ask for permission. Clarification on copyright issues can be sought from the Head of Online Learning and Information Services.

Students and staff making use of ICT facilities must respect copyright and not plagiarise the work of others. Please see College Copyright Policy.

Acceptable Use Policy – Internet and Email

2. **Monitoring the Use of Computer Facilities**

The introduction of ICT increases the potential for efficiency and productivity. However, many staff use such office-based communications for personal reasons and mistakenly consider this to be a right.

In order to enforce this policy and ensure that ICT facilities are not being misused, the College will randomly monitor e-mail and internet usage by staff and students.

Misuse of College computing facilities, including unacceptable use as defined in this policy and the accessing of inappropriate material, will be seen as constituting misconduct. Disciplinary action up to and including dismissal may be taken against an employee who is found to have been misusing College computing facilities in terms of this policy.

3. **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 College Systems Manager.

4. **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 e-mail, the sender actively invokes it. E-mail should only be encrypted using College-approved software, and where this is required for purposes of confidentiality. College e-mail 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.

5. **Safe Surfing**

Current 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. While the risks of using the Internet should not be overplayed, teaching staff must ensure that students are aware of the dangers, and are equipped with strategies for avoiding them (e.g. not handing out personal details to strangers on the Internet).

Acceptable Use Policy – Internet and Email

6. Netiquette

The details of netiquette can be abstruse. In brief, netiquette is good manners for the Internet. Staff and students must be encouraged to observe netiquette as appropriate to the systems they are using and to avoid causing offence to other users.

7. Viruses

Viruses can be transferred between computers either over the Internet or by using floppy disks or other media between machines. All staff should ensure that their machines are properly protected from virus infection and that they take action to ensure that viruses are not passed from home or other machines to those in the College. Teaching staff should also encourage students to adopt sensible practices both when using College machines and those they have access to either at home or at work.

8. Use in public view

Aberdeen College is a publicly-funded organisation and members of the public have a legitimate interest in the ways in which those funds are used. Adherence to the provisions of this policy will ensure that misuse of public funds with regard to the use of the Internet and e-mail does not occur. For this reason, recreational or personal use of computers should not take place *at any time* on machines that are in public view.

Other Issues

A number of activities related to the use of the Internet or e-mail are covered by law, by College policy or regulations or are otherwise clearly unacceptable. These will be regarded by the College as constituting misconduct and any staff involved will be subject to disciplinary action up to and including dismissal. These include: 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.

Status:
Date of version:
Responsibility for Policy:
Responsibility for Review:
Date of equality impact assessment:
Review date:

**Approved by HR Committee
December 2010
Vice Principal (HR)
Vice Principal (HR)
June 2008
December 2012**

Appendix 1

Use of user-owned devices with College networks

Aberdeen College recognises that both staff and 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. It is also recognised that this is a developing trend and that as ICT becomes more portable, and more fully a part of our everyday lives, it will become quite normal for a range of devices to connect to the College network as and when needed. At present laptop computers are likely to be the most common devices, but in future this may include mobile phones, PDAs, MP3 players and other small devices.

This is a trend which the College views as positive and which it seeks to encourage. 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, 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, including acceptable use policies, 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 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,

Acceptable Use Policy – Internet and Email

for example, that proper virus protection is installed and used on the device.

5. All devices are connected to College power supplies or networks entirely at the user's own risk. The College will not be responsible for any damage to the device and/or loss of or damage to or corruption of data held on the device which results from such connection.
6. 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 in any other way. Specifically they should not seek to "hack" into the network in any way whether for malicious or other intent.
7. 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).