

BEDFORD COLLEGE

ICT Acceptable Use Policy

Executive Summary

Bedford College provides access to networked and stand-alone computers to support students' learning and the efficient management of the organisation. Our Acceptable Use Policy is an extension to the College Code of Conduct. It includes guidelines for the safe and responsible use of the College network, IT systems and resources and the internet, and identifies those activities which constitute an abuse of our ICT facilities.

In summary, users of the College IT facilities are prohibited from:

- logging on to the college IT systems and network with another user's account
- creating or sending offensive or harassing materials to others, using any type of technological devices
- altering the settings of College computers or making other changes which render them unusable by others
- tampering physically with any computer equipment, including connecting personal devices
- installing software without authorisation
- hacking into unauthorised areas of the network or any other college IT system
- accessing inappropriate internet content and services or trying to circumvent the College filtering system
- attempting to spread viruses or any other malware via the network
- any form of illegal activity, including software and media piracy.

Disciplinary action, in accordance with College procedures, may be taken against those found to be in breach of the Acceptable Use Policy.

1. Policy Statement

Bedford College seeks to maintain a professional working environment for its students and staff, and provides ICT systems which facilitate effective working as a student or employee. The aim of this policy is to ensure that College ICT practices including use of e-mail and the internet are as safe, secure and efficient as possible.

The use and misuse of Information Communication Technology at Bedford College is covered by the Codes of Conduct for both staff and students. This policy is an extension of those Codes of Conduct, covering specifically the use of the Bedford College IT systems, network and any computer equipment connected to it. It applies to all Bedford College campuses.

What constitutes acceptable use of ICT is detailed at Annex A of this policy. It is the responsibility of all users to ensure that they take reasonable steps to comply with this policy, and failure to comply may result in disciplinary action.

2. Safeguarding

This policy supports the aim of the College to prioritise safeguarding and to provide a safe learning and working environment for students and staff, in line with the Every

Child Matters agenda and Ofsted outcomes for learners. In the context of ICT this includes taking measures to:

- identify and take action on any inappropriate use of College electronic media
- provide opportunities for staff and students to report any inappropriate use of electronic media e.g. cyber-bullying
- promote e-safety through the curriculum, tutorials and cross-College activity.

Guidance on staying safe online is included at Annex B.

3. Scope

Computer Facilities

Every student is issued with a username, password, moodle account and email address at the start of the academic year. This provides access to the student computer network and a range of standard applications (Word, Excel, Access etc.) as well as online facilities including the College VLE system and access to the internet and email. Access is provided for the duration of their course or until the end of the academic year, whichever is the shorter. College ICT facilities are provided to support students' learning and their sole use should always be for academic and other College-related work.

Every member of staff is issued with a username, password, moodle account and email address at the start of their employment. This provides access to the staff computer network and a range of standard applications (Word, Excel, Access etc.) as well as online facilities including the College VLE, student data systems and access to the internet and email. Additional user accounts and passwords may be issued to specific staff for the purpose of accessing IT systems that are particular to their role. Access is provided for the duration of their employment.

A public wireless network (free Wi-Fi) enables users to connect with their own mobile devices; this is only available in designated areas, including college residential areas. An account is required from IT Services to access this facility. While this network service may be used for recreational purposes or other uses that are not directly related to academic activities, internet access is filtered and this Acceptable Use Policy applies.

Internet, Email and Social Networking

The College's internet access is via an educational service provider (JANET), and all users are expected to comply with the JANET requirements relating to acceptable use. Access is filtered through the Barracuda systems which block access to web sites known to contain offensive or inappropriate material. The filter is continually updated, though there can be no absolute guarantee that unsuitable material is never available. Students and staff should alert IT Services to filtering issues (inappropriately blocked or unblocked sites).

Mobile Devices

The term *mobile device* in this policy includes laptops and electronic notebooks, PC tablets (including iPad), mobile phones (including iPhones & Windows Mobile devices), games consoles, media devices (including iPods and any other MP3 players) or any other portable web-enabled computing device.

Students and staff may connect mobile devices to the College's public network (BedfordCollege). This provides filtered access to the internet and the College's VLE (Moodle).

4. Monitoring

It is the responsibility of the Director of Information & Learning Technologies to monitor compliance with this policy and those administering the College network have measures in place for ensuring the security of user data:

- Students and staff can assume that files and information, stored on the college network, are protected from viruses and from interference by others. They should not, however, assume that their activities are completely private.
- IT Services staff are authorised to monitor all user accounts to ensure the security of the network; system log files, records of usage, stored files and email messages that have been sent or received may be scrutinised at any time, either during routine system maintenance or if there is reason to suspect misuse of the network.
- All student machines are monitored by software and inappropriate activity is reported to the Director of ILT
- All use of the Moodle chat facility is recorded and regularly checked. Action is taken against students using the facility inappropriately, including banning the student from using the facility and referral to Student Services in cases of cyber-bullying
- Use of the 'Bullying Alert' button on moodle is monitored by Student Services
- The College's internet connection is filtered, and access to inappropriate sites is denied.

5. Communication

The requirements of this policy are communicated through student and staff induction, as well as via electronic media such as moodle and the staff intranet.

6. Supporting Documents

- Disciplinary Procedures and Code of Conduct (staff and student)
- Anti-bullying Policy
- Safeguarding Children and Vulnerable Adults
- Professional Boundaries Policy
- The Safe Use of New Technology (Ofsted)

7. Useful links

- [Data Protection Act \(1998\)](#)
- [Computer Misuse Act \(1990\)](#)
- [Criminal Justice and Police Act \(2001\)](#)
- [Criminal Justice and Public Order Act \(1994\)](#)
- [Copyright, Designs and Patents Act \(1988\)](#)
- [Malicious Communication Act \(1988\)](#)
- <http://www.thinkuknow.co.uk>
- <http://www.excellencegateway.org.uk/>
- <http://www.jiscinfonet.ac.uk/infokits/social-software/acceptable-use>

Definitions of Acceptable Use

The list of unacceptable activities in this section is not necessarily exhaustive. Any activity which may reasonably be regarded as unlawful or as negatively affecting the College's reputation is not permitted.

Section A - Computer Facilities

General Conduct and Use

1. Students must show ID cards to access IT Support and the IT open access facilities
2. No food or drink may be consumed in any ICT classroom or IT open access facility
3. Any damage to computers or any apparent malfunction of equipment must be reported to IT Services as soon as possible.

Use of the Network

1. When logging on to the network (including logging on to college network services from home), a student or member of staff must always use their own user identification and password. Any attempt to impersonate another user will be treated as a serious disciplinary offence, as will any attempt to interfere with data stored on the network by another user. These activities are illegal under UK law:
2. A student or member of staff must never, under any circumstances, use another person's account or attempt to log on as a system administrator.
3. The college definition of vandalism includes any malicious attempt to harm, modify, or destroy data of another user. The Bedford College IT systems, network or other networks connected to the Internet must not be vandalised. This includes the uploading or creating of computer viruses or any other form of malware.
4. Harassment in this context is defined as the persistent annoyance of another user, or interference with another user's work. Harassment is a breach of the Acceptable Use Policy and includes, but is not limited to:
 - the sending of annoying, obscene, malicious or indecent emails, telephone calls, SMS or text messages
 - Spamming using Moodle Chat
 - Placing malicious or offensive materials on any electronic materials.
5. If a student or member of staff identifies a security vulnerability on the Bedford College system they must notify IT Services immediately. They must not demonstrate the vulnerability to other users.
6. Students and staff must not divulge their passwords for any College system to other member of staff, students or users of computers outside the College. Any student or member of staff who suspects that this has happened accidentally should change their password immediately.
7. Before leaving a computer or any password protected college IT system, students and staff must log off the network and check that the logging out procedure is complete.
8. Students and staff must not attempt to gain access to the local drive of any machine or to create local accounts (administrative or otherwise).
9. Students and staff must not attempt to share drives, folders or files across the network other than when enabled by IT Services.
10. Only software provided on the network may be run on College computers. This includes programmes run from USB devices unless previously agreed with IT Services and is limited to the transfer of data only. Students and staff are not permitted to import or download applications or games, and it may be illegal to do so.
11. It is a breach of the College Code of Conduct (and examination board regulations) to pass off another's work as your own (plagiarism). This includes copying and pasting

information accessed online without proper acknowledgement. Further guidance on plagiarism is available from the Learning Resources Service.

12. Students and staff must be aware of, and comply with, the restrictions placed on certain kinds of usage, in particular the playing of games on any machine on the College network.

Section B – Internet, Email and Social Networking

General Netiquette

Students and members of staff must not:

1. Send electronic communications which are annoying, obscene, malicious, indecent, abusive, discriminatory, racist or in any way intended to make the recipient feel uncomfortable.
2. Disclose to a third party the personal details of any other student. (Including sharing photos of other students without permission).
3. Access any inappropriate internet site. If any student or staff member finds that they have accidentally accessed an inappropriate site it is their responsibility to leave that site immediately.
4. Breach another person's copyright in any material.
5. Upload or download any unauthorised software or attempt to run that software. In particular, hacking, encryption and other system tools are expressly forbidden.
6. Use the College computer network to gain unauthorised access to any other computer network.
7. Spread or attempt to spread computer viruses. Attachments from email providers other than the College system are blocked to prevent the spread of viruses and spyware.
8. Engage in activities that are prohibited under UK Law. Thus the transmission of material subject to copyright or protected by trade secret is forbidden, as is any threatening or obscene material.

Section C – Mobile devices

The following apply to all mobile devices:

1. Unless authorised by IT Services, students and staff may only connect their own devices to the College's *public* network.
2. Under no circumstances should computers, printers or other devices be disconnected from the College network to make way for a student's or staff's own computer or mobile device.
3. No mobile device may be plugged directly into any network port, switch, hub or router.
4. The sharing of local drives, folders or files across the network is strictly forbidden.
5. No servers of any description should be attached to the network, without prior permission from IT Services.
6. Students and staff must ensure that their own devices are properly protected from viruses before connecting to the College public network.
7. Students and staff are responsible for the material that exists on or is accessed via their mobile device. IT Services are empowered to scrutinise, and if necessary retain for further investigation, any device which is or has been attached to the network.
8. The College does not accept responsibility for any damage, howsoever caused, to students' and staff's own mobile devices or their contents (files, folders etc.).
9. All rules of usage for internet access and computer usage apply to mobile devices.
10. It is the responsibility of the owner to ensure that they have a licence for all software installed on their mobile device.
11. No software may be run on a mobile device during lessons which is not appropriate to that lesson.

Section D – Free Wi-Fi (Public Network)

Students and staff using the College's public network (the Free Wi-Fi system) are subject to all provisions of this Acceptable Use Policy.

While students and staff are welcome to use their own mobile devices using the Free Wi-Fi, they should only be connected to the College's public network. To do this, the devices must have up-to-date anti-virus and firewall software. In order to gain access to this system please contact IT Services. Any problems, in particular by users of operating systems other than Microsoft Windows, should be referred to IT Services.

Staying Safe Online

Student and staff need to be aware that thoughtless use of email and the internet may jeopardise their personal safety either at College or outside College. Students and staff should therefore:

1. Be aware that any person they “meet” or communicate with online may pretend to be someone else.
2. Never arrange a meeting in person with anyone they have “met” or only communicated with online. If necessary to meet someone you have communicated with online ensure you take a trusted adult with you and let someone else know where you are going and when you should be back.
3. Not respond to messages or bulletin board items that are indecent, suggestive, malicious, discriminatory, threatening, or which make the student feel uncomfortable or unsafe in any way.
4. Report any such messages to their tutor/manager by using the ‘Bullying Alert’ button on moodle or via an online reporting service such as ThinkUKnow (<http://www.thinkuknow.co.uk>).
5. Remember that anything they read online may not be accurate.
6. Ignore offers that involve either financial transactions or personal meetings, these are likely to be scams.
7. Not disclose any personal details online, such as their home address or telephone number.
8. Not disclose personal details, such as your location or intended plans to be at a particular place as others can view this and make unwanted contact.
9. Remember that student s and staff are easily identified by College photos. Once a photo is online it can then be copied and re-used by anyone who has access to the initial image.
10. Not use or upload photos of any other students or staff without their prior permission.

Roy Currie
Director of Information & Learning Technologies

December 2010