



Acceptable Use of IT Policy

| | |
|----------------------------------|---|
| Document title: | Acceptable Use of IT Policy |
| Audience: | Students, Staff, Visitors and Contractors |
| Approved by: | Senior Leadership Team |
| Policy commencement date: | 01 March 2020 |
| Date of next review: | 01 February 2022 |
| Document author(s): | Head of IT |

This policy will be reviewed at least every two years by the Head of IT.

Table of contents

| | Page |
|---|------|
| 1. This policy and your responsibilities | 3 |
| 2. Your agreement and disciplinary action if you break it | 3 |
| 3. What the College does to protect you | 4 |
| 4. What you must do to protect yourself and others | 5 |
| 5. What you must not do | 9 |
| 6. Personal use of the College systems | 11 |
| 7. Review of this policy | 12 |
| 8. Documents related to this policy | 12 |

1. This Policy and your responsibilities

Who and what this policy applies to:

This policy applies to every learner who uses any of the IT Services provided by Bradford College. The policy applies whether you are on campus or working from home, a workplace or at distance. The policy applies to your use of College equipment and College services as well as your own equipment when you use it on College business.

Your responsibilities

You must read this policy and keep to the rules and guidelines set out within it. These exist to protect you and to ensure that you learn safely and get the most from College IT systems.

2. Your agreement and disciplinary action if you break it

Your agreement to stick to the rules in this policy

When you sign your Student Learner Agreement, you also sign your agreement to keep to the rules within this policy, which is available for you to read and print on the College web site.

Monitoring and disciplinary action

What you do on line when using the College network and what you access and store on the College network is monitored and logged. If you break the rules of this policy, you may face disciplinary action and potentially in the most serious circumstances Police investigation

Questions about this policy

Any questions about this policy should be directed to IT Services at this email address:

it.services@bradfordcollege.ac.uk

Reporting of issues

If you suspect that someone else is breaking these rules or at risk, you must share your concerns with your tutor (in confidence if necessary) who will make sure that this is investigated and support services are informed as required to support the user.

3. What the College does to protect you

We do lots to help you to stick to the rules and we do lots more in the background to protect you from threats that might arise online. Here are some of the things that we do:

Internet

Being a large college that caters for a wide range of learner ability, age and interest, we try to give access to as much of the Internet as appropriate whilst keeping our learners safe. To protect our learners, our IT security systems automatically block access to thousands of inappropriate web sites. Such web sites might promote racial discrimination or hatred, for example. If you need access to a blocked web site e.g. to research racial discrimination for a social sciences project, speak to your tutor who may be able to arrange access.

Personal Details

We do not publish your personal details and College staff must protect your privacy.

Secure Backed Up Storage

The College provides registered students with secure data storage by means of a Microsoft Office365 OneDrive account in the cloud. This conveniently allows you to access and share your own data from any device connected to the internet. However, even the most sophisticated IT systems are prone to occasional failure (which can make data temporarily unavailable or even permanently lost) so you should keep separate backups of important data such as your coursework. Remember to keep these backups secure (on a password protected device) and never store your data on a college device as it may be deleted.

College Email

The College provides registered students with an email account as part of MicrosoftOffice 365. You can forward your private email to this account and can use it for as long as you are with us. The College will use this account to update you with essential information.

Anti-virus software

Software that detects and deals with computer viruses is on every college computer and server. This anti-virus software is continually updated to ensure your protection.

College Computers

The software on college computers (including desktop computers, laptops and tablets) has been configured to prevent tampering. You must not attempt to install or permanently reconfigure software such as the operating system, security or application software.

4. What you must do to protect yourself and others

Connecting to the College network

Users of the College's network must not connect any equipment using an Ethernet cable. Users are permitted to connect their own devices to the College's wireless ('Wi-Fi') network only. Users are expected to ensure that any device attached to the College network has the latest security patches installed and up to date Antivirus software installed. The College reserve the right to scan devices automatically or manually and block access if these terms are not met.

Fair usage if a user is found to be consuming excessive bandwidth the access will be suspended pending investigation. Using college network to share content and copyright materials is not acceptable and would result in further action.

College access to the internet is provided by Janet, a high-speed network for the UK research and education community, so all users are also subject to the Janet Acceptable Use and Security Policy (<https://community.jisc.ac.uk/library/acceptable-use-policy>).

Phishing (Emails or websites trying to get bank account details)

Beware of links in E-mails and think before you click on them. They may look very real but are not really from BT, Microsoft, Banks. Do not put any details in to this kind of site.

Phone calls from these companies can also be fake and are trying to get hold of details or control of your device. Examples; you have won a lottery for which you have never brought a ticket, helping get money out of another country, payments for medical treatments, the purpose is to obtain bank details so your accounts can be emptied.

Use of network tools etc.

The unauthorised use of network tools and changes to the College network is not allowed. If your course requires you to use network tools, monitor networked devices or install and configure servers and control systems then you should be provided with an isolated network to facilitate your learning without risking the availability and security of network resources for other users.

Help and guidance

At the start of your course of study you will be shown how to access the College systems and how to use them safely. You will also have opportunity to ask questions about this policy. Always seek help if you have questions or concerns about using the College's IT systems – IT Services and library staff have a lot of experience and are keen to help you.

Protect your personal details

Going online exposes you to thousands of people who want to trick you into giving them access to your personal details. Never give your personal details (including name, age, address, phone number, credit card or bank account details) or a photo of yourself (or anyone else) to any stranger on the Internet. Do not lend anyone your student card or divulge your network password, even to your best friend: this is a disciplinary offence.

Protect your money

You will almost certainly receive scam email messages, even though the College uses sophisticated security systems. Scam emails can look very convincing and often promise you money or goods in return for your personal details such as your email address or even your bank account details. Always delete these scam emails, and do not reply. If you are in doubt then ask someone else to take a look – but **do not** give out your personal details.

If you buy anything online, make sure that the seller advertises contact details including a phone number, and that it has good reviews. Any payment by credit card should take you to a secure site for entry of details. If you do not know what one of these looks like, then ask someone to check for you before you enter any personal details.

Protect your reputation on social networking sites

The College accepts that you may use social networking sites such as Facebook in your own time. Although we are not responsible for these sites and cannot control them, we strongly recommend that you take care when allowing others access to your Facebook or similar sites. Make sure your privacy settings are correctly configured to keep you safe. Think carefully before you post text and photos because even if you remove later they may have already been forwarded elsewhere, at which point you lose control of who sees them. Remember that what you might share with a close friend could be interpreted very differently by a stranger. Your reputation is precious and easily damaged – look after it.

Be careful what you say about others on social networking sites

Do not use your social network to spread lies about people, places or organisations. Publishing lies online - even amongst friends on social networking sites - can result in legal action being taken against you. Check the terms and conditions of social networking sites and use them for interacting with friends in your own time and not anti-social or illegal activity

College use of social networking sites

The College cannot be responsible for social networking sites outside its own network and provides a 'virtual learning environment' (Moodle) as a safe and secure alternative.

However, the College recognises that special features of some social networking sites might make your tutor invite you to join a social network site to communicate and collaborate with other students. You are strongly recommended to read and abide by all rules of such sites. Do not use these sites to vent negative feeling against other learners, staff or the College: what you say can be seen by others and you will be held accountable. Use the proper procedures if you want to complain about something.

Bradford College student Card

When you enrol at Bradford College you are given a student card that enables you to gain entry to college buildings and classrooms as well as access to resources such as the library and your printing account.

Do not lend your card to anyone. Your student card is for your use only and you may become liable for any issues that might arise should you let somebody else use it.

Protect your network username and password

When you enrol at Bradford College you are given a username and temporary password to enable you to connect to the College network. You are required to create a new password when you first login to the College IT systems and you must change the password every term.

It is very important that you protect your network password in order to maintain your privacy and to ensure that you are not accused of wrongdoing should somebody else break these rules whilst pretending to be you.

Here are a few do's and don'ts:

Do:

- Use your username and password when you log in to the College network. Never use somebody else's username and password. If the person before you have forgotten to log off, you must log them off the College network and log in as yourself.
- Always log off the network when you have finished work, otherwise you might be held responsible for what the next person does in your name.
- Change your password if you suspect that someone has learned it by watching you type it in.

Do not:

- Give your username and password to anyone else inside or outside the College.
- Write your username and password down. Just remember them – it's much safer.

Email – use it sensibly

Keep your email messages short and to the point. Get into the habit of using a greeting, adding a description to the 'Subject' field and finishing your message with your name and contact details. Do not use email to criticise others or to 'shout' at people (avoid using lots of capital letters for emphasis). Remember that email messages can be easily circulated to people you know (and those you do not know) and could even be quoted against you in court, so choose the words you use carefully.

Tell your tutor if you accidentally visit an unacceptable web sites mistake

Sometimes you might accidentally visit an inappropriate web site that should have been blocked by our automated security systems (occasionally these systems fail to identify an inappropriate web site, perhaps because it has just appeared or recently changed name). The College understands that mistakes happen, but you should still tell your tutor as soon as possible because otherwise the College's monitoring systems might prompt a formal investigation. Telling us also means that we can block such sites from other users.

If you need to access web sites that are normally blocked

Some coursework may require research into subjects that are normally blocked as unacceptable. For example, you might need to research the use of illegal drugs for a Social Work course. In such cases, your tutor must contact IT Services beforehand to request a temporary exception to the rules. If you are at all uncomfortable about the areas that you need to access and how these might be at odds with this policy, please seek assurance from your tutor.

5. What you must not do

For clarity, this guidance is sub-divided into unacceptable 'content' (things you must not look at, download, publish, or communicate) and unacceptable 'activities' (things you must not do).

Unacceptable Content

You must not seek, view, download, publish, transmit or communicate content that is

- illegal
- threatening
- offensive
- abusive
- libellous (untrue or unfair comments about someone which will harm their reputation)
- harassing
- pornographic
- sexist
- racist
- unlicensed for use within Bradford College

and/or which relates to:

- terrorism and extremism
- cults
- dating
- controlled drugs
- bullying
- gambling
- criminal activity (including software hacking)
- social chat, jokes or chain mail that is not related to your course social groups
- promotion of any kind of discrimination
- personal business (such as any private work that you do)
- encouraging violence, or unlawful conduct

Unacceptable Activities

You must not:

- do anything which may bring the College into disrepute
- commit illegal activity or activity which breaches any college policy
- provide access to facilities or information to those who are not entitled to have it
- use college facilities to bully, harass, intimidate or otherwise cause alarm or distress to others
- attempt to undermine the security of the College's facilities, including hacking or undertaking any unauthorised penetration testing or vulnerability scanning of any college systems
- pretend to be other users by using their network username and password
- try to access the network anonymously (so you cannot be identified)
- write or introduce viruses or other programs designed to cause harm

- introduce unauthorised equipment e.g. modems, other active equipment, monitors etc. which could adversely affect network performance and put sensitive data at risk
- waste resources or introduce insecurities
- tamper with workstation addresses, settings or software
- use college IT facilities purely for private, social or personal business use within timetabled study time
- use college IT systems to advertise material that may provoke or offend others, such as extremism or hate crime
- use college systems to attack other systems, sites, organisations or individuals
- use college systems to transmit details about other people that you do not have permission to pass on
- use college systems to re-publish material that is copyright (owned by others)
- send e-mail messages or phone messages which are abusive, harassing or include unacceptable content, swearing and threatening language
- download software without college permission or introduce software for which you hold a personal home license without first checking suitability with IT Services and if the software may be legally used on business premises
- download or use games or access games over the network, other than software installed and/or approved for learning purposes
- download copyrighted information for storage, re-transmission or re-use including copyright images, text, data, music and video
- create, store or transmit defamatory or obscene material (where there be genuine need to access such material e.g. during a criminal investigation, prior permission for controlled access must be obtained from the Director of Learning Resources)
- advertise the email address or location of any other person without their permission
- create and transmit bulk e-mail messages that could be construed as 'spam' email
- subscribe any other person to any online facilities without that person's consent
- publish 'example' or 'fictitious' material about courses or the College that may be confused with genuine college-published materials
- fail to comply with a request from an authorised person for you to change your password
- fail to report any breach, or suspected breach of information security
- fail to comply with a request from an authorised person to stop any activity which is detrimental to the operation of the College's facilities.

6. Personal use of College systems

Personal Use of IT Facilities

The College accepts limited personal use of its IT facilities outside timetabled class time. This might include research, personal finance, family appointments/communication, social networking etc. so long as:

- it does not interfere with your study or anyone else's study
- it does not contravene any college policies
- it is not excessive in its use of college resources

Those who use college IT facilities to make purchases, pay bills or conduct online banking or similar activities do so at their own risk. The College cannot be held responsible for any direct or indirect losses sustained by those using its IT facilities for personal transactions.

Personal Mobiles and devices

Phones, tablets, smartphones and any other personal devices should only be used in personal time and not during timetabled class time unless permitted by your tutor. In exceptional circumstances, such as home emergencies, you should check with your tutor who can make allowances.

The College is not responsible for third party mobile networks on which devices such as mobile phones and smartphones operate and cannot intercept or block calls. Do not use your mobile phone, smartphone and/or tablet to abuse others or to send anything anonymously. If you receive messages or voice mail or anything else that upsets you, ask your tutor or any member of staff for support - there are trained staff within college who will offer you support and keep you safe. Whilst the College is not responsible for activity that occurs on third party networks, it will report serious incidents to relevant telecommunications providers.

7. Review of this policy

This policy will be reviewed annually by the Head of IT and approved by the College Senior Leadership Team.

8. Documents related to this policy

- Student Learner Agreement
- Anti-Bullying and Harassment Policy
- Prevent Strategy
- Safeguarding Policy and Procedures
- Equality and Diversity Policy