

IT Policy

Policy Statement

The policy establishes a framework and describes the standards that users are expected to observe when accessing College IT facilities and ensures that users are aware of the legal and internal disciplinary consequences attached to inappropriate use of the facilities. College IT facilities include:

- all hardware, software and networks
- printers and printing facilities
- laptops and laptop trolleys
- classroom IT facilities, touchscreens
- telephones, smartphones, tablets
- email facilities
- access to college network using any device (e.g. PC, smartphone etc) whether owned by the College or not
- access to college network from any location (e.g. home, public location, College premises)

This policy should be read in conjunction with other College policies and procedures pertaining to acceptable standards of conduct and behaviour, e.g., rules for the conduct of employees, anti-bullying and harassment policy and procedures, disciplinary policy and procedures, general regulations for students and the IT procedure and guidelines.

Use of all IT facilities provided by City of Bristol College is subject to the relevant policies and regulations

Users should be aware that their usage of IT facilities for Internet, and email will be monitored and, in some cases, recorded in line with the Human Rights Act 1998, Anti-terrorism, Crime and Security Act 2001, General Data Protection Regulation 2018, Regulations of Investigatory Powers Act 2000, and the Telecommunications (Lawful Business Practice) Interception of Communications Regulations October 2000, Safeguarding Vulnerable Groups Act 2006, Equality Act 2010, Keeping Children safe in education guidance 2024, and the 'Prevent duty' (section 26) within the Counter Terrorism and Security Act 2015, staff code of conduct and student code of conduct. This policy complies with these regulations.

Associated with the provision of these services and facilities, City of Bristol College takes seriously its responsibility to provide an appropriate regulatory framework, including specific standards, procedures and guidance for the appropriate use of these College services and facilities. The IT Policy constitutes a component of this regulatory framework, as well as a component of the College's e-safety framework.

Scope

This policy applies to all members of staff, students, governors and other authorised users of College IT facilities.

Responsibilities

The policy is maintained and regulated by the College's Estates, Facilities, and ICT. The policy will be reviewed regularly to ensure that it reflects expected developments in the operational use of the system and best practice.

Managers have a responsibility to ensure that they fully understand the policy and effectively communicate this to staff. Managers judge the boundaries of acceptable use. All users, on joining the College, will be advised of where they can access a copy of this policy.

All users have a responsibility to ensure that they fully understand and comply with this policy.

Acceptable use

The Standards of Acceptable Use of College IT facilities are detailed in the **IT Guidance** document, and they reflect the values and current policies of the College. College management will be responsible for judging reasonable bounds within the Standards of Acceptable Use in line with the Guidance. The IT Guidance includes personal use of College IT facilities.

If users are in any doubt about what constitutes acceptable and appropriate use, they should seek the advice, in the case of members of staff, from their manager, and in the case of students, from their course tutor.

The College monitors the usage of its IT facilities, and any monitoring is carried out in line with current legislation.

Users should be aware that if found to be in breach of the acceptable standards that the disciplinary policy and procedure may be instigated. Some breaches, e.g. publication of certain materials, may amount to a criminal offence and the College reserves the right to involve the Police.

Printing

In general, multi-functional devices (MFDs) should be used for all printing. For large and/or specialist print jobs external printing may be used. Desktop printing and purchase of toners for desktop printers is available in special cases and requires authorisation by the College's IT Manager. Locations for MFDs are decided by Estates, Facilities, and ICT following a consultation with the relevant Directors/Head of Departments for those locations. Disabled access will be considered when authorising and locating printing facilities. Staff are expected to observe the **Printing Guidance**.

Students will be offered free print credits annually as agreed by Director of Estates, Facilities, and ICT.

Laptop trolleys

By borrowing a laptop trolley the member of staff is accepting to abide and observe the **Laptop Trolley Procedure** that includes standards of acceptable use. The first four instances of misuse of the laptop trolley facilities will result in warnings and sanctions as per the Laptop Trolley Procedure. Any further instances of misuse may result in staff disciplinary proceedings.

Staff must

- book the trolley as described in the Procedure and return the trolley on time
- not book laptop trolleys on behalf of another member of staff
- check that all laptops are returned with the trolley and report any missing laptops immediately
- ensure laptops are charging after being returned, and that chargers and cables are stored tidily within the laptop trolley
- not take the trolley outside the building where it has been issued

Wireless Access Security

Wireless Access Security Procedures must be followed to protect the College's IT facilities and data from unauthorised use and/or malicious attack that could result in loss of information, damage to critical applications, loss of revenue, and damage to our public image. All users must adhere to college-defined procedures when:

- accessing College IT facilities and data via wireless means at any location, whether at college premises or elsewhere, and via any device, whether College owned or not
- connecting a college device to any wireless network

Employment or enrolment at City of Bristol College does not automatically guarantee the granting of wireless access privileges.

College wireless networks are an extension, not a replacement, of the wired network. They are to be used for general purpose access in areas of transient use, such as common areas or meeting rooms. Wireless access points within college premises are managed solely by ICT. Unauthorised installations or use of wireless equipment is strictly forbidden.

Wireless segments should not be used for access to sensitive College data.

Users accessing College resources through other than College networks are expected to adhere to the same security protocols as the College does. Failure to do so will result in immediate suspension of all College network access privileges.

College users using public hotspots for wireless Internet access must employ for their devices a college-approved personal firewall, VPN, and any other security measure deemed necessary by the ICT department. VPNs supplied by the wireless service provider should also be used, but only in conjunction with the College's additional security measures.

Hotspot and remote users must disconnect wireless cards when not in use. Users must ensure that their computers are not connected to any other network while connected to the College's network via remote access.

ICT reserves the right to turn off or remove without notice any access port or equipment from the College's network that puts the College systems, data, users or students at risk.

Please refer to the **Wireless Access Security Procedures** for detailed implementation.

Mobile devices

Mobile devices include, but are not limited to, mobile phones and tablets, and all accessories that were provided with the device. All employees who have been allocated mobile devices are responsible for taking the utmost care for them, complying with acceptable use and returning them safely.

Mobile devices will only be available to staff who have the authorisation of the appropriate Director and additional authorisation by the College's IT Manager. An employee will be eligible to have a mobile device if it is deemed necessary to their position, and they meet any one of the following criteria:

- If the employee's duties require them to spend a substantial amount of time out of the office on work related duties.
- Staff who are required to be contactable in an emergency
- Staff who are on call after normal business hours
- Staff who are identified by the Health and Safety team to be a 'lone worker'

In addition, pool mobile devices may be made available to college staff who *temporarily* meet these criteria.

Directors are responsible for ensuring an adequate provision in their budget to cover the cost of all mobile devices issued within their area.

Please refer to the **Mobile Devices Procedure** for detailed implementation.

Linked Policies, Procedures and Guidance

- IT Procedure
- IT Guidance
- Mobile Device Procedure
- Wireless Security Access Procedure
- Laptop Trolley Procedure
- Printing Guidance
- Safeguarding Policy and Procedure
- Code of Conduct (Staff)
- College Code of Conduct (Students)

Version:	
Approved by:	SLT
Date of approval:	June 2025
Date for Review:	June 2028
Lead Officer:	ICT Manager
Senior Manager responsible:	Director of Estates, Facilities, and ICT

IT Procedure

This document is an appendix to the College IT Policy. It applies to all employees, students, governors, and other authorised users of the College network.

Login IDs

As a user of the College's network, you will be issued with a login ID and a password. This will allow you to gain access to network files, secure storage space on the network, other network resources such as printers, and cloud-based services. Your login ID will allow you to access your own private file area on the network, as well as shared file areas.

You should keep your login ID and password secure, and you must not disclose them to anyone else.

You must not:

- Use any other person's login ID or password
- Attempt to log into the network with any login ID other than the one that has been issued to you

The only exceptions to this are where other IDs have been issued for a specific purpose that has been agreed, in advance, by the IT Manager.

Preventing the spread of malicious software (viruses)

Users of College IT facilities must take all reasonable steps to prevent the receipt and transmission by email, or other electronic methods of malicious software e.g. computer viruses.

You:

- Must not transmit by email or any other means, any file attachments which they know to be infected with a virus
- Must ensure that an effective anti-virus system is operating on any computing device which you use to access College IT facilities
- Must not open email file attachments received from unsolicited or un-trusted sources

Monitoring procedure

Internet and email facilities are the property of the College. All internet use and emails are logged by the College's network systems and are monitored.

The College will maintain appropriate monitoring arrangements in relation to all internet, email and related services and facilities that it provides, and the College will apply these monitoring arrangements to all users. This applies to both College owned and personal devices using College network services. Please note that this also applies to college owned devices when using networks not owned by the College. E.G, A home Internet connection.

Every attempt to access a website is logged and activities monitored. The log records the name of the login user, the time and date and the address of the web site. The amount of time spent by that person on the internet is logged and the precise time of the day when access is open. The log records the type of site, e.g. chat, gambling, entertainment, business, etc. and the sites visited. Managers will be informed periodically if personal internet use, in work time, is abused or is excessive in work time and this may lead to disciplinary action.

Certain types of website, such as those containing pornographic material, may not be accessed from college. A content filtering system is in place that denies access to such sites. All attempts to access these banned sites are logged together with the login ID of the user, the time and date and the address of the website. This log is monitored to ensure that all users are complying with the legislation, staff code of conduct, and student code of conduct. Repeated misuse identified by the content filtering system will be reported to the relevant person.

These arrangements may include checking the contents of, and in some instances recording, email messages for the purpose of:

- Establishing the existence of facts relevant to the business
- Ascertaining or demonstrating standards which ought to be achieved by those using the facilities
- Preventing or detecting crime
- Investigating or detecting unauthorised use of facilities
- Ensuring effective operation of facilities
- Determining if communications are relevant to the business, e.g. where an employee is off sick or on holiday

The College may, at its discretion, apply automatic message monitoring, filtering and rejection systems as appropriate, and deny transmission of messages with content that is unacceptable in the terms of this policy.

These monitoring arrangements will operate on a continual and continuing basis, with the express aim of monitoring compliance with the provisions of the College's IT policy, procedure, and guidance and for the purposes outlined above as permitted by The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000.

Procedure in the event of a breach of the standards of acceptable use

In circumstances where it is assessed that there has been a breach of the standards of acceptable use, as described in the IT Guidance, the College will, as a first action, act promptly to prevent continuance or repetition of the breach, for example to withdraw any unacceptable materials.

This action will be taken in accordance with the normal managerial arrangements and will typically involve liaison between the appropriate member(s) of the College Leadership Team/Safeguarding team and the College ICT team.

Indications of non-compliance with the provisions of the IT Policy will be investigated in accordance with the provisions of the College's disciplinary procedures as applicable to employees and students.

Procedure for access to ex-employee email accounts

In some circumstances it will be necessary to access the email account of a former employee, e.g. to gain access to work related information that the user has stored on their email account and not copied to their manager/team/colleagues prior to leaving.

In all termination letters a member of staff will be asked to clear their email accounts of personal emails so that only business emails remain on the account. Information is archived in accordance with the College data retention policy following the end of employment and then removed from the system, if an individual is aware that business information they hold on their account will be required by the College at some future date it should be stored on the network, and not in the email system...

If a member of staff is absent from work for any reason (sickness leave, annual leave) where their permission cannot be obtained the College will arrange for the relevant manager with prior permission from a member of the People Services team to access the relevant email account and open the relevant file. Any file that has a personal file name attached to it will not be opened.

Linked policies

- IT Policy
- IT Guidance
- Mobile Device Procedure
- Wireless Security Access Procedure
- Laptop Trolley Procedure
- Printing Guidance
- Safeguarding Policy and Procedure
- Code of Conduct (Staff)
- College Code of Conduct (Students)

Version:	
Approved by:	SLT
Date of approval:	June 2025
Date for Review:	June 2028
Lead Officer:	ICT Manager
Senior Manager responsible:	Director of Estates, Facilities, and ICT