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, projectors, smartboards
- 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, in particular the College IT regulations and the College Internet policy statement.

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 2018, 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 and other authorised users of College IT facilities.

Responsibilities

The policy is maintained and regulated by the College's Estates, Facilities, and ICT department and jointly, with regard to employment issues, with Human Resources. 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 on 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 an authorisation by Estates and Infrastructure - ICT. Locations for MFDs are decided by Estates and Infrastructure following a consultation with the relevant Directors/Head of Units 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 a number of 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 will result in a staff disciplinary.

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, 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 Director of Estates, Facilities, and ICT. 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 situation
- 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 and IT guidance
- Mobile Devices Procedure
- Wireless Security Access Procedure and Agreement
- Laptop Trolley Procedure
- Printing guidance
- Safeguarding policy and procedure
- Staff code of conduct
- Student code of conduct

Review frequency:	3 years
Lead officer:	Director of Estates, Facilities, and ICT
Senior Manager Responsible:	Vice Principal, Corporate Services and External Relations
Approved by:	Business Services Committee
Date of Approval:	March 2022
Date for Review:	March 2025

IT Procedures

This document is an appendix to the College **IT Policy.**

Login IDs

As a user of the 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 (F), 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 Head of ICT Network & Engineering Services

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.

In particular, users:

- Must not transmit by email 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 they 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 web use and emails are logged by the network systems and 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 used by a member of staff.

Every attempt to access a web-site 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 a member of staff 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. Line 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 web site, such as those containing pornographic material, may not be accessed from college. A web access 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 web site. This log is monitored

in order to ensure that all users are complying with the JANET acceptable use policy, staff code of conduct, and student code of conduct. Repeated misuse identified by the filtering system will be reported to a senior manager.

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 email facilities
- Ensuring effective operation of email 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 and IT regulations 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 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 staff 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 member of staff, 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 disc.

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 HR 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
- JANET Acceptable Use Policy
- Staff code of conduct
- Student code of conduct
- Data retention policy

Lead officer: Head of ICT
Executive lead: Director of Estates & Infrastructure

IT Guidance

This IT Guidance supplements the **IT Policy** and guides its implementation.

Standards of acceptable use

The main purpose for the provision by the College of IT facilities is for use in connection with the teaching, learning, research, and approved business activities by the College.

IT facilities provided by the College should not be used for:

- Personal use, other than as specified below
- The transmission of unsolicited commercial or advertising material, chain letters, press releases, or other junk mail of any kind, to other users, user organisations, or organisations connected to other networks, other than where that material is embedded within, or is otherwise part of a service to which the member of the user organisation has chosen to subscribe
- The unauthorised transmission to a third party of confidential material concerning the activities of City of Bristol College
- The transmission of material such that this infringes the copyright of another person, including intellectual property rights
- The unauthorised provision of access to College services and facilities by third parties
- Activities that unreasonably waste staff effort or networked resources or activities that unreasonably serve to deny service to other users e.g. inappropriate use of all user email
- Activities that corrupt or destroy other users' data
- Activities that disrupt the work of other users
- The creation or transmission of any offensive, obscene or indecent images, data, or other material, or any data capable of being resolved into obscene or indecent images or material to a third party for whatever reason
- The creation or transmission of material which is designed or likely to cause annoyance, inconvenience or needless anxiety
- The creation or transmission of material that is abusive or threatening to others, or serves to harass or bully others
- The creation or transmission of material that either discriminate or encourages discrimination on racial or ethnic grounds, or on grounds of gender, sexual orientation, marital status, disability, political or religious beliefs
- The creation or transmission of defamatory material
- The creation or transmission of material that includes false claims of a deceptive nature
- So-called 'flaming' i.e. the use of impolite terms or language, including offensive or condescending terms
- Activities that violate the privacy of other users
- Criticising individuals, including copy distribution to other individuals
- The creation or transmission of anonymous messages i.e. without clear identification of the sender
- The creation or transmission of material which bring the College into disrepute

- Unauthorised access to other email accounts

Personal use

The main purpose for the provision by the College of IT facilities for email is for use in connection with teaching, learning and approved business activities of the College. The College permits the use of its IT facilities for email by staff, students, and other authorised users for personal use, subject to the following limitations:

- Access only in own time i.e. before work, lunch break, after work
- A level of use that is reasonable and not detrimental to the main purpose for which the facilities are provided
- Priority must be given to use of resources for the main purpose for which they are provided
- Personal use must not be of a commercial or profit-making nature, or for any other form of personal financial gain
- Personal use must not be connected with any use or application that conflicts with an employer's obligations to City of Bristol College as their employer
- Personal use must not be connected to any purpose or application that conflicts with the College's rules, regulations, policies and procedures
- Personal use must comply with the College's policies and regulations

Use of online information

The College network and the internet service offers staff some very powerful communication and information services. All staff are encouraged to make full use of these resources but their use must remain without certain limitations.

When using the internet you must comply with the JANET acceptable use policy which can be found at www.ja.net

You should be aware of the need to protect College systems from virus infection. If you receive an email with an attached file, and you do not know where the email came from, you should delete it without opening the file.

You may use the internet for purposes not directly related to work but you must not do this during working time and you must comply with the JANET acceptable use policy.

Users should:

- Address colleagues in an acceptable manner using a salutation together with the name of the person to whom the message is directed, if the email is to a group of people then using the terminology of colleagues would be acceptable. The message should end with the senders contact details
- Keep all user emails for urgent College work
- Keep email messages brief and to the point
- Avoid unnecessary copying or forwarding of emails, and use of blind copies
- Check your mailbox at regular intervals to help ease congestion
- Always identify yourself when sending an email
- Use discussion groups/boards for expressing views/sale of personal items

Users should not:

- Send offensive email messages or pass on electronic chain letters
- Install any software on any College systems

- Copy or install any copyright protected software or data from any systems without permission
- Install or run games software, or download any programs from the internet
- Edit, move or delete any systems files or programs already installed on the system
- Attempt to penetrate the security of the system
- Have or publish any software that is obscene, libelous, sexist, incites racial hatred or in any way breaks any UK law relating to published material
- Express any 'political' opinions in any email

Clear desk

The Clear Desk guidelines are designed to assist in compliance with the General Data Protection Regulations 2018, and also the reduction of the amount of paper that is used in the College. As well as safeguarding personal data, it will reduce expenditure on costly toners and inks - particularly from colour printers. It will also reduce the amount of filing space that the College will require which will free up office space.

Many people use print offs as a form of backup against losing information from the computer systems. The ICT team backup systems and processes keep all the information required on a daily basis.

Tips for having a tidy desk

- Put a date and time in your diary to clear paperwork
- If in doubt - throw it out. If you are unsure of whether a piece of paper should be kept - it will probably be better to put it in the bin.
- Use the recycling or confidential waste bins for office paper no longer needed.
- Do not print off emails to read them. This just generates increased amounts of clutter
- Go through the things on your desk to make sure you need them and what isn't required throw away.
- Handle any piece of paper only once - act on it, file it, or put it in the bin
- Always clear your desktop before going home
- Consider scanning paper items and filing them in your PC
- Regard should be given to the appropriate disposal of confidential waste

Use of equipment

Users should not move equipment around or change the cabling in any way.

Users should not connect any equipment to the network unless you have obtained permission, in advance, from the Head of ICT Network & Engineering Services.

Copyright laws

It is illegal (for copyright protected software) to:

- Copy software

- Run pirated software
- Transmit software over a communications line, thereby creating a copy

Legal consequences of misuse of email facilities

In a growing number of cases involving the civil or criminal law, email messages (deleted or otherwise) are produced as evidence in a permanent written form.

There are a number of areas of law which apply to use of email and which could involve liability of users or the College.

These include the following:

- Intellectual property: Anyone who uses email to send or receive any materials that infringe the intellectual property rights of a third party may be liable to that third party if such use is not authorised by them
- Obscenity: a criminal offence is committed if a person publishes any material which is pornographic, excessively violent or which comes under the provisions of the Obscene Publications Act 1959. Similarly the Protection of Children Act 1978 makes it an offence to publish or distribute obscene material of a child
- Defamation: as a form of publication, the Internet is within the scope of legislation relating to libel where a statement or opinion is published which adversely affects the reputation of a person, group of people or an organisation. Legal responsibility for the transmission of any defamatory, obscene or rude remarks which discredit an identifiable individual or organisation will rest mainly with the sender of the email and may lead to substantial financial penalties being imposed
- Data Protection: processing information (including photographs) which contains personal data about individuals requires the consent of those individuals. Any use of personal data beyond that registered with the Information Commissioner will be illegal
- Discrimination: any material disseminated which is discriminatory or encourages discrimination may be unlawful under the Sex Discrimination Act 1975, the Race Relations Act 1976 or the Disability Discrimination Act 1995 where it involves discrimination on the grounds of sex, race or disability
- The above is only designed to be a brief outline of some of the legal consequences of misuse of email facilities.
- The Computer Misuse Act 1990 made it a criminal offence for anyone to modify computer held data or software without authority or to attempt to do so. There are three specific offences.
    - Unauthorised access to computer programmes or data (this could be access from outside the network or authorised users who deliberately exceed their authority
    - Unauthorised access with criminal intent (intention of using the information or date gained for a further offence)
    - Unauthorised modification of computer material (programmes and data). This covers deliberate introduction of a virus into a system

Linked policies

- IT Policy
- IT Procedure
- JANET Acceptable Use Policy

Lead officer: Head of ICT
Executive lead: Director of Estates & Infrastructure

Printing Guidance

Introduction

This document provides further guidance under the College **IT Policy** for anyone printing/using printing equipment that is the property of the College.

Printing facilities: the College has invested heavily in modern, efficient printing facilities using multi-functional devices (MFDs). There are four basic levels of provision:

- Large scale and highly specialist printing via external print partner
- General colour and black & white printing on A3 and A4
- Desk-top printing

Printing a single page will prove costly on any system but as the size of the print job increases, the inefficiencies and costs of using inappropriate facilities increase exponentially. The College will try to ensure that the most appropriate facilities are used in each case.

Business issues addressed by using MFDs

- **Efficiency** - costs: the cost of print consists of the ink/toner, the paper, the electricity and the depreciation and each of these (except paper) varies with the type of machine used and the annual amount of use. In general the larger the number of copies and the larger the machine used, the lower the cost per page. Further, the less a machine is used and the longer it sits in stand-by mode, the higher the electricity costs per page printed. It is universally accepted that printing through desk-top printers is considerably more expensive than printing through multi-functional printing devices. There are concerns about the time factor retrieving individual/small print tasks from multi-functional printing devices not located within a reasonable distance from the operator. Continued use of desk-top printers is recognised subject to the installation of any print management software that is adopted by the College on all desk-top printing devices and only after a comprehensive and rigorous review of the Faculties/Departments Print Strategy which reviews the continued use of individual desk-top printers and can be justified to external auditors when this guidance is reviewed in three years time and the outcome reported to the Audit Committee of the Board of Governors.
- **Environmental**: the carbon footprint of desk-top printers is an issue that the College must take seriously. Desk-top machines left in stand-by mode overnight and during the week-ends leave a massive carbon footprint and this is especially the case with older machines. Disposal of toners and cartridges is also an environmental cost and using larger machines and toners creates less waste than a multitude of smaller machines. Therefore in the exceptional case where desk-top printers are retained, Areas of Learning and Functional areas are required to ensure that procedures are in place to switch off desk-top printers at night and the week-ends and that toners are disposed of via the route identified by ICT.
- **Quality**: whilst the cost and time involved in colour printing are both higher than with black and white, colour does add an extra level of perceived quality, especially for materials aimed at external clients. Whilst it may not be strictly cost effective to have a relatively large number of colour machines, if we take into account the savings that can be achieved by removing most of the desktop printers, then the College will still be better off financially and will also leave a smaller carbon footprint.

Principles for printing

- All printing facilities should be accounted for under UNIFLOW and all costs recharged to Areas of Learning and Functional areas.
- The default printing option for everyone at the College should be mono double sided printing on their local multi-functional device.
- For jobs unsuitable for local printers users should employ the Job Ticket facility to forward print jobs in excess of 100 copies per activity to the external print partner.
- The "pop-up" which tells a user that their job has been sent to the printer and the cost should normally be enabled on all PCs although staff may request that it be removed from their account.
- Whilst desktop printers are not entirely banned, their use must be justified, and the purchase of toners and new machines must be authorised by ICT. E.G, Exam room printers.

Locations

- Multi-functional devices will normally be located in publicly accessible areas to take full advantage of the 'Follow Me' concept and maximise efficiently.
- Locations will be determined via print audits with the print solution vendor.
- Previous print audits have shown that Multi-functional devices located in staff rooms, or classrooms are used inefficiently and are not acceptable unless there are exceptional circumstances.
- Students will be offered a number of free print credits annually as agreed by Director of Estates & Infrastructure.

Disabilities

In deciding the location and scale of printing facilities it is important to consider any users with declared disabilities.

A3 printing should be available for those with restricted vision and printing facilities must be close to those with mobility issues. The College does not offer a braille printing service. Where this is necessary for blind staff and students they will normally have machines provided for them through government initiatives and the College will help them make use of such equipment.

In any case where there is a disability issue which might be affected by this printing policy due consideration will be taken of the staff and student needs.

Linked policies

- IT Policy

This guidance is produced by the College's ICT functional area and jointly, with the Finance functional area, and in regard to employment issues, with Human Resources.

Lead officer: Head of ICT
Executive lead: Director of Estates & Infrastructure

Wireless Security Access Procedure

Introduction

This document is an appendix to the College **IT Policy** and its purpose is to define standards, procedures, and restrictions for connecting to City of Bristol College's internal network(s) or related technology resources via any means involving wireless technology. This can include, but is not limited to, access from the following:

- External hosts via remote access technology (for example, using a wireless router at home to connect to the college network)
- Wireless gateways on college premises.
- Third-party wireless Internet service providers (also known as “hotspots”)

The procedure applies to any equipment used to access College resources, even if said equipment is not College-sanctioned, owned, or supplied. For example, use of a public library’s wireless network to access the College network would fall under the scope of this policy.

Any questions relating to this procedure should be directed to the ICT Helpdesk, via email: it.helpdesk@cityofbristol.ac.uk

Scope

This policy applies to all College employees, including full-time staff, part-time staff, students, contractors, freelancers, and other agents who utilise college-owned, personally-owned, or publicly-accessible computers to access College data and networks via wireless means.

This procedure is complementary to any previously-implemented policies dealing specifically with network access and remote access to the enterprise network.

Access and management

Wireless access to enterprise network resources is a privilege, not a right. Consequently, employment or enrolment at City of Bristol College does not automatically guarantee the granting of wireless access privileges.

The wireless access user agrees to and accepts that his or her access and/or connection to City of Bristol College's networks may be monitored to record dates, times, duration of access, data types and volumes, etc., in order to identify unusual usage patterns or other suspicious activity. As with in-house computers, this is done in order to identify accounts/computers that may have been compromised by external parties.

All wireless access points within the College’s firewall will be centrally managed by City of Bristol College's ICT department and will utilise encryption, strong authentication, and other security methods at the ICT department's discretion.

Although ICT is not able to manage public wireless resources, end-users are expected to adhere to the same security protocols while utilising this equipment. Failure to do so will result in immediate suspension of all network access privileges so as to protect the college's infrastructure.

All remote computer equipment and devices used for business interests, whether personal- or college-owned, must display reasonable physical security measures. Users are expected to secure their college-connected machines when they are physically at their machines, as well as when they step away. Computers will have installed whatever antivirus software deemed necessary by City of Bristol College's ICT department. Antivirus signature files must be updated in accordance with existing college policy.

Wireless networks at College premises

Wireless networks should not be considered a replacement for a wired network. They should be seen solely as extensions to the existing wired network, and are to be used for general purpose access in areas of transient use, such as common areas or meeting rooms. Wireless segments should not be used for work sessions involving any form of access to sensitive organisational or personal data without encryption.

Addition of new wireless access points within college premises will be managed at the sole discretion of ICT. Non-sanctioned installations of wireless equipment, or use of unauthorised equipment within the organisational campus, are strictly forbidden and will be removed.

Employees, contractors, and temporary staff will make no modifications of any kind to college-owned and installed wireless hardware or software without the express approval of City of Bristol College's ICT department.

Due to the potential for bandwidth conflicts within the college campus, use of unsanctioned equipment is strictly forbidden. If you have a need to use such equipment, please consult ICT before proceeding further.

Remote access to College network

It is the responsibility of any employee of City of Bristol College who is connecting to the organisational network via wireless means to ensure that all components of his/her wireless connection remain as secure as his or her network access within the office. It is imperative that any wireless connection used to conduct City of Bristol College business be utilised appropriately, responsibly, and ethically. Failure to do so will result in immediate suspension of that user's account.

Employees using wireless access methods will, without exception, use secure remote access procedures. This will be enforced through public/private key encrypted strong passwords in accordance with City of Bristol College's password policy, and other encryption methods. Employees agree to never disclose their login passwords to anyone, particularly to family members if business work is conducted from home.

Employees, contractors, and temporary staff with wireless access privileges must ensure that their computers are not connected to any other network while connected to City of Bristol College's network via remote access.

Public wireless networks

College users using public hotspots for wireless Internet access must employ for their devices a college-approved personal firewall, encryption, 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 City of Bristol Colleges additional security measures. ICT will support its sanctioned hardware and software, but is not accountable for conflicts or problems whose root cause is attributable to a third-party product.

Hotspot and remote users must disconnect wireless cards when not in use in order to mitigate attacks by hackers, war-drivers, and eavesdroppers.

Users are advised that their login passwords should be changed regularly, and we recommend that passwords are changed after using public wireless networks.

Incidents

The wireless access user agrees to immediately report to his/her manager and City of Bristol College's ICT department any incident or suspected incidents of unauthorised access and/or disclosure of college resources, databases, networks, and any other related components of the organisation's technology infrastructure.

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

Policy Non-Compliance

Failure to comply with the Wireless Security Access Policy, Procedure and Agreement may result in the suspension of remote access privileges, disciplinary action, and possibly termination of employment.

Lead officer: Head of ICT
Executive lead: Director of Estates & Infrastructure

Laptop Trolley Procedure

COVID secure guidance for using laptop trolleys

Laptop trolleys and the laptops they contain are shared devices. Therefore, in order to use these safely, these guidelines must be followed.

Moving/returning trolleys

Using cleaning wipes located in each room, clean laptop trolley handles, lock, and charging plugs prior to moving, and after returning trolley to charging location.

Using laptops

Again, using cleaning wipes located in each room, clean laptop charger plug, exterior surface of laptop and gently wipe keyboards prior to, and after use.
We do not recommend cleaning of screens as the wipes will leave residue, and make screens difficult to read. Laptop users should avoid touching the screens if they haven't been cleaned.

Introduction

This document is an appendix to the College **IT Policy** and sets the procedures, standards of acceptable use and restrictions for the use of laptop trolleys provided by the College. This procedure also describes the consequences attached to inappropriate use of the facilities.

This procedure applies to all laptop trolleys available as bookable resources via the laptop booking system.

Scope

This procedure applies to all members of staff, students and other authorised users of College laptop trolleys.

Responsibilities

The procedure is maintained and regulated by the College's ICT functional area and jointly, with regard to employment issues, with Human Resources. The procedure 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 procedure and effectively communicate this to staff.

All users have a responsibility to ensure that they fully understand and comply with the acceptable standards outlined in this procedure.

Standards of acceptable use

The laptop trolleys are for use in connection with the teaching, learning, research, and approved business activities by the College. By borrowing a laptop trolley the member of staff is accepting to abide and observe these standards of acceptable use.

The following applies when borrowing laptop trolleys provided by the College:

- The majority of laptop trolleys contain 10 laptops, for loan to teaching staff for use in classrooms. They are for **student use** only.
- Only whole trolleys can be issued. Individual laptops should not be loaned. If you receive any requests for individual laptops please refer them to the nearest study centre.
- Only one trolley per classroom should be booked. If you require more than one trolley for your class, you should either book an IT computer suite, or split the class activities so that one group can be using the laptops, whilst the other group carries out another activity.
- The majority of laptop trolleys have a Salto lock; if the lock is faulty in any way please report this to the BFM Helpdesk.
- The Laptop Trolley Risk Assessment should be made available at the trolley point and must be adhered to at all times (document available on staff intranet)
- Staff must check laptops are returned with the trolley and report any missing laptops immediately.
- Staff must ensure all laptops are charging after being returned.
- Staff must ensure chargers, and cables are stored tidily within the laptop trolley.
- The laptops can be issued to a tutor for a session of no more than 3 hours. This covers a morning or afternoon session. They must then be returned to the trolley point for re-charging. Charging time is **up to 1½ hours** so please take this into consideration when making bookings.
- Laptop trolleys cannot be block booked for an all-day session. If a lecturer has borrowed a trolley in the morning, they may only borrow it again in the afternoon if there are no other bookings.
- Trolleys **must not** be taken outside the building where they have been issued, for health and safety reasons.
- In the event of a laptop developing a fault, it should be removed, stored in a secure place at the trolley point or office and the fault reported to the IT Helpdesk by the relevant member of staff. If there is no secure place to leave the laptop, please leave it in the trolley. The designated laminated sheet with the job request number should be placed on the empty trolley shelf, to denote that it is under repair or on top of the reported laptop as applicable (Job logged template for faculty laptops document available on staff intranet)
- Staff are responsible for the security and safety of any laptops and trolley borrowed by them for the duration of the loan.
- Staff must not book laptop trolleys on behalf of another member of staff.
- Staff may ask students to assist in the collection and return of a laptop trolley, but staff must accompany students. Students cannot be sent unaccompanied to collect or return a laptop trolley. However, if a member of staff is unable to so as a result of a disability, then reasonable adjustments can be made for the collection and return of the trolley, e.g. another member of staff could be requested to fulfil this duty. Disability is a protected characteristic of the Equality Act 2010.
- Laptop trolleys for use in classrooms can be booked up to two weeks in advance via the laptop booking system. The laptops are only for use in the classroom which you have booked them for.
- Staff are responsible for reporting any incidents or inconsiderate use of laptop trolleys to ICT immediately. Failure to report such incidents will likely result in an incident being logged against your name.
- Fully charged laptops have up to 3 hours of battery life. They should only be used on battery whilst in the classroom. Chargers and cables must not be removed from the trolley.
- Before shutting down the laptop, students should save their work to their area on the network (F drive). Any work saved to directly to the laptop (for example to the Desktop) will not be backed up and as such will not be retrievable.

Inconsiderate user related incidents

- Trolleys returned in a mess, chargers not plugged in, laptops piled on top of each other, wires not tucked in, etc.
- Laptops not returned to the correct trolley
- Trolley missing
    - Is not returned at all and left in a random room
    - Not returned on time
    - Staff have taken a trolley without booking it
- Trolley is booked by someone else so if trolley not returned on time, results in time wasted trying to track down the wrong person when trolleys are returned late.

Monitoring procedure

Laptop trolleys are the property of the College. In order to ensure best utilisation of this equipment, its use will be logged and monitored. This will be periodically reviewed, and if necessary equipment redeployed to areas within the College where it can be best utilised.

ICT will maintain a laptop trolley incident database to record incidents relating to laptop trolleys, which includes breaches of the standards outlined above.

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 above, ICT will log this as an incident in the laptop trolley incident database. Warnings will be issued to staff as a result.

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 management team and the College ICT Unit.

Indications of non-compliance with the provisions of the laptop trolley facilities will be investigated in accordance with the provisions of the College's disciplinary procedures as applicable to staff and students.

Consequences of misuse of laptop trolley facilities

There are a number of actions that will be taken as a result of the misuse of College laptop trolley facilities.

These include the following:

- **1st instance:** Incident recorded in database, and warning email sent to member of staff reminding them to be considerate to other users of the facilities.
- **2nd instance:** A stronger warning email from Head of Estates & Infrastructure, or Head of ICT Network & Engineering Services (copy also goes to their Curriculum Leader / Director of Learning)
- **3rd instance:** Email to their Curriculum Leader / Director of Learning requesting them to meet with their member of staff regarding acceptable use of the facilities.
- **4th instance:** Remove member of staff from the laptop booking system and Salto locks for the laptop trolleys, email to Curriculum Leader / Director of Learning, and copy to member of staff.

Any further breaches of the acceptable use of the laptop trolley facilities will result in staff disciplinary procedures. E.g. if member of staff then takes trolley without booking it.

Linked Policies and documents

- HR Policy
- IT Policy
- Laptop Trolley Risk Assessment
- Job logged template for faculty laptops

Lead officer: Head of ICT
Executive lead: Director of Estates & Infrastructure

Mobile Device Procedures

Introduction

This document is an appendix to the College **IT Policy** and sets the procedures and restrictions for the use of College mobile devices.

The aim of this procedure is to protect the College's investment in mobile device hardware, software and the College's own technology-based resources (such as College data, networks, databases, etc.) 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. Therefore, all users utilising College technology resources must adhere to College-defined processes for doing so.

Definitions

Mobile Device – includes, but is not limited to, laptops, mobile phones and tablets, and all accessories that were provided with the device, such as chargers, headphones etc.

Director – Director/Assistant Principal/Head of Unit/Executive Director

Responsibilities

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. This includes all accessories that were provided with the device including but not limited to chargers, headphones etc.

Directors and ICT are responsible for authorising allocation and acceptable use of the devices.

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

Eligibility criteria

Mobile devices will only be available to staff who have the authorisation of the appropriate Director and additional authorisation by ICT. 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 situation
- 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. Pool devices will be made available through College Study Centres.

Should a user's role/title change whilst in possession of a device, the user must follow the "Requesting Mobile Devices" procedure if they wish to retain the device. Should their Director decide their new role complies with the above criteria, information must be provided to by the Director to Finance on the budget for the device to be charged against, to enable accurate billing.

Should a user's Director and/or ICT decide their role no longer requires the device, this must be returned to the IT Helpdesk for reallocation.

Requesting mobile devices

A **Mobile Device Request Form** must be completed in all cases. These are available from the IT Helpdesk. The Director must provide their approval by sending this to ICT with written consent. All sections must be completed including budget code.

The purchase of mobile devices must be in compliance with the College's Financial Regulations. All costs for the purchase and use of mobile devices will be charged to the appropriate departmental budget.

Replacement devices

If a device is lost or stolen, it should be reported immediately to the IT helpdesk and an incident report form must be completed. Any damage, loss or theft may result in the user being liable for the cost of a replacement; however any replacement device will remain the property of the College, as agreed in the **Mobile Device Acceptance form**.

If a device is damaged or faulty, then this should be returned to the IT helpdesk. If the device cannot be repaired, ICT will require a request for a replacement from the user's director.

If the device is damaged, lost or stolen as a result of unacceptable carelessness, as decided by ICT, the user is liable for the cost of a replacement. ICT will consult with relevant Directors and may delegate the decision of the cause of the damage, loss or theft to them but retain final say on the matter.

Return of devices

When the user no longer meets the eligibility criteria or their employment terminates, the employee must return any College devices to ICT, unless ICT have approved a transfer to a new user. Any accessories supplied by the College for use with the device must also be returned.

Devices issued to an individual must not be passed to any other employee without the prior consent the relevant director and ICT. Any devices passed internally without prior consent from ICT may be disabled remotely. Where ICT have consented to internal reallocation of a handset, information must be provided to Finance on the new user of the handset to enable accurate billing and account management.

Conditions of use

The mobile device user must use their device appropriately and responsibly, ensuring use is limited to work-based activity. College mobile device users are required to sign and agree to the **Mobile Device Acceptance form** on collection of the device.

All College mobile devices must have the College Mobile Device Management software installed and configured on them. This is to ensure that the College can comply with the General Data Protection Regulation 2018, and specifically to ensure that the College data is held securely. This management system also provides facilities to recover lost or stolen devices and remotely manage them.

In accordance with the IT Policy, the College will monitor the usage of mobile devices in line with current legislation. If it determined that devices are not being utilised, the College has the right to reallocate them. Reasonable and minimal personal use is acceptable where necessary, however ICT retain the right to question any activity they deem

inappropriate, excessive or for personal use. ICT retain the right to question any activity they deem inappropriate, excessive or for personal use.

In accordance with the Health and Safety Policy and guidance, mobile devices must be used legally and responsibly when undergoing tasks such as driving, operating heavy machinery and any other activity where full concentration is required.

Restrictions

For international travel, authorisation from an Executive Director to enable roaming must be provided to ICT. International Pool Mobiles are available from the IT Helpdesk for overseas trips.

Any users using mobile devices in restricted security locations must comply with those locations security procedures at all times. This may include, but is not limited to, relinquishing mobile devices to be collected on exit and disabling camera functions.

Fair usage limits have been applied to users, and all users share a common amount of free minutes, texts, and data. The service is not unlimited. If limits are reached, ICT may disable the device until a user explains why limits have been exceeded. This is not to stop people working but to minimise outside usage which is not business related.

Non-compliance

Failure to comply with the procedure and linked policies may result in the suspension of mobile devices, disciplinary action, and could result in termination of employment.

Linked policies

- IT Policy
- IT Policy: Wireless Security Access Procedures
- Health and Safety policy
- Financial regulations

Lead officer: Head of ICT

Executive lead: Director of Estates & Infrastructure