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

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 intaccess filtering system
logged together with the login ID of the user, the time and date and the address of the web site. This

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 Colleh50 Tw 4.58 Td(t)-1.1 (i)3.p (r)-64de t on bee of ch.3 (3a-8(ar) on hol)-89 (i)3.1 (da)-243 (y)]TJ0 Tc 0 Tw 39.675 0 T ppane

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

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

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 Ars]TJ0 Tc4.5 e ar.Bf( )Tj0 g-0.002Td1vEMC /P 122(w) M.4 (m)-24.4 (al)3.1 (l)-8.9 (y)161 ( )-122(w)-Bm
llllled ef

yA-1.1 (ert3.1 (ed,)-1.1 (ng4.1 (ant s[i)ho")-8.4 (l.1 s)-de)-121 bl)3.2(oc)a1 (c)-ai ho-8.1 4l
Al D e aut[)-1361 (he8)-1.84(0 ne8 (ea,m)-24.)g aut nwolbe be dl.9 (y) been()-1-12(m)w23 6m 9.2(oc)- (dnt)-332(0H)]T21u

Policy Non-Compliance

- 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

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.

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