
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 data 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