IT Acceptable Usage Policy

Version 7

LOCAL POLICY

Scope of Policy:	All Staff and Students
Policy Owner:	Head of IT
Date of Initial Approval:	25/05/2022
Approved By:	Strategic Leadership Team
Status:	Current
Most Recent Publication Date:	25/10/2024
Equality Screening Date:	27/01/2014
Policy Review Date:	30/06/2025

Published by Belfast Metropolitan College www.belfastmet.ac.uk. Belfast Metropolitan College ['Belfast Met'] is committed to providing publications that are accessible to all. To request additional copies of this publication in a different format please contact:

Corporate Development
Belfast Metropolitan College
Integrated Shared Services Centre
398 Springfield Road
Belfast BT12 7DU

This document is only valid on the day it was printed. The master and control version of this document will remain with Corporate Development. Amended and approved versions of the policy must be sent to Corporate Development once approved. Final versions will be posted on the intranet by Corporate Development.

Further Information
For further information about the content of this policy please contact:

Department of IT and Digital Services
Belfast Metropolitan College
Integrated Shared Services Centre
398 Springfield Road
Belfast BT12 7DU

Policy Compliance details: -

Compliance with Equality Legislation.

PLEASE NOTE: Policies must be equality screened before being submitted to SLT and Trade Unions: -

Equality Screening Date:	27/01/2014
Equality Screening Outcome:	Screened Out
Sector or Local Screening:	Local Screening
Consultation Date (if applicable):	Not Applicable
Equality Impact Assessment	Not Applicable
(EQIA) Date (if applicable):	Not Applicable
EQIA Key Outcomes:	Not Applicable

Document History

Version Number	Author	Updates/Amendments	Date
Final	C Daysh	New	Sept 2013
Final	C Daysh	Organisational and compliance changes	11/4/18
	Corporate Development	New legislation and formatting for new intranet	April 2019
Final	C Daysh	Review and annual update. Minor changes as follows:- Section 1 "telephone network" changed to "internet connection" New sentence – "Effective security involves the participation and support of every user. It is the responsibility of every user to know these guidelines, and to conduct their activities accordingly" Section 2 Additional wording – "in order to protect the college from illegal or damaging actions by individuals, either knowingly or unknowingly" Section 4.2 Legislation list updated to include latest legislation Section 4.5 Additional wording – "Users must not us another users account" Section 4.6 Additional wording - "and have the latest security patches installed" Section 4.8.1	May 2021

		Additional wording – "Passwords must be at least 20 characters in length"	
5	C Daysh	Section 4.7 Additional wording – "IT resources are intended to be used by the individual that has been provided them. No unauthorised persons should be permitted access to the IT resources, such as family members or friends." Section 4.9.2 Additional wording – "Send any college business related email, attachments or documentation to their own personal email account or personal/unapproved cloud storage or file sharing platform."	May 2022
6	Corporate Development on behalf of C Daysh	Legislative changes required due to Brexit - GDPR changed to UK GDPR Paragraph 6 - Related Policies section - referred to the Data Protection Policy 2018 and GDPR. This has been amended to reflect the title of the policy i.e. the Data Protection Policy.	August 2022
7	Kristian Kinnaird	Local Policy Section on Header Page Policy Owner changed from Head of IT to Head of IT & Digital Services to reflect new organisational change. Section 4.2 Legislative/Regulatory Context Change from "Computer Misuse Act 1990" to "Computer Misuse Act 1990 (to include additional addendums)"	July 2024

		Section 4.2 Legislative/Regulatory Context Added line Network & Information Systems (NIS) 2018 Section 4.6 Use of IT Resources "H" drive changed to "Shared" drive Section 4.9.2 Electronic Communications Unacceptable Use Line added "Take part in or aid and abet any criminal action including cyber-attacks on the College network and/or other external networks, in alignment with the regulations and legislation outlined in Section 4.2" Section 4.9.2 Electronic Communications Unacceptable Use Line added "Use technologies, such as AI, to leak/compromise sensitive data outside the boundaries of the College network." Corporate Development Contact Details updated	

Document History Table

Distribution

This document has been distributed as follows:

Name	Date (where applicable)
Trade Union	17 May 2022
Committee	N/K
Executive Leadership Team	N/A
Strategic Leadership Team	July 2018; 25 October 2021; 26 May 2022
Governing Body	September 2013
Published on intranet by Corporate Development	March 2019; November 2021; May 2022; Aug 2022; July 2024

Distribution Table

Contents

1 Policy Aim

Belfast Metropolitan College (the College) provides information technology (IT) resources that cover a range of facilities and services from the provision of Personal Computers (PCs), laptops, tablets and mobile phones to the use of information systems and software applications as well as access to its information; from the use of its internet connection to the buildings that accommodate them. These resources and support services allow users to conduct business on behalf of the College. Therefore, it is important that there are rules in place that define what is deemed acceptable in order to ensure that the College's IT resources are not misused in anyway. Acceptable use of the College's IT resources involves the participation and support of every College employee/worker, student, governor, business partner, contractor and/or service provider.

Effective security involves the participation and support of every user. It is the responsibility of every user to know these guidelines, and to conduct their activities accordingly.

2 Policy Objectives

The objective of this policy is to define the rules for users on the appropriate use of College IT resources to protect the college from illegal or damaging actions by individuals, either knowingly or unknowingly and to outline how the College will respond to any potential breaches of these rules.

3 Scope of Policy

This policy applies to all authorised Users of College IT resources (see definition below).

This policy applies to all areas of the College network, associated IT systems and information.

The College IT networks are connected to other educational institutions and to the rest of the world via JANET, the electronic communications network and associated electronic communications and networking services and facilities that support the requirements of the UK education and research communities. Acceptance of this College Policy is deemed to be acceptance of the JANET Acceptable Use Policy.

4 General Principles

4.1 Introduction

By using College IT resources, the user has personal responsibility for their appropriate use and agrees to comply with this policy and other applicable College policies and all relevant laws and regulations. This will help to ensure the security, confidentiality and safety of the College's IT resources.

4.2 Legislative/Regulatory Context

- Data Protection Act 2018 and UK General Data Protection Regulations
- Human Rights act 2000
- Criminal Justice Act 1988
- Computer Misuse Act 1990 (to include additional addendums)
- Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- Telecommunications Act 1984
- Protection of Children Act 1978
- Copyright, Design and Patents Act 1998
- Obscene Publications Act 1959 and 1964
- Defamation Act 1996
- Sex Discrimination Order 1976
- Disability Discrimination Act 1995 (as amended)
- Race Relations Order 1997
- s75 Northern Ireland Act 1998
- Network and Information Systems (NIS) 2018
- Sexual Orientation Regulations 2003/3006

4.3 Definitions

In this Policy, the following definitions apply:

- **IT** – Information Technology
- **IT resources** – encompasses all IT equipment (of any kind) that is:
    - Controlled or operated by the College or a third party on behalf of the College;
    - Connected to the College network(s);
    - Used at or for College activities;
    - Brought onto a College site.

- **User** - any person who operates, has access to or interfaces with IT. This includes College employees, workers and Governing Body members, students, contractors, sub-contractors, consultants, business partners, official visitors or customers of the College.
- **Electronic Communications** – Electronic communication systems, services and equipment owned, leased or managed by the College. This includes but is not limited to:
    - Email, instant messages and text messages;
    - Internet/Intranet access (including social networking services such as Facebook, Twitter; blog accounts; Bulletin boards; “Chat” Services), also refer to the College Social Media Policy and Guidelines;
    - Telephones (landlines and mobiles/smart phones) and Voicemail;
    - Laptops, Tablets, Personal Digital Assistants (PDAs);
    - Video conferencing;
    - Faxes, scanners and photocopiers (including multi-function devices).

4.4 General issues

The College strives to provide computer access for its staff, students and administrators to local, national and international sources of information and encourages an atmosphere that supports the sharing of knowledge, the sharing of resources, and assists the creative process of learning.

Users accessing the IT resources at the College must use the resources in an honest and responsible manner.

All users are responsible for the integrity of these IT resources. They must respect the rights of other computer users, respect the integrity of physical facilities and controls, and respect all licence and contractual agreements related to College IT systems. All users must act in accordance with these responsibilities, and the relevant local, national and international laws where applicable.

The College will deploy software to block access to inappropriate and illegal material on the Internet from all sites that it knows about. These sites constantly change and it cannot guarantee to block access to all such sites at any one time.

The College takes no responsibility for the accuracy of information obtained from the Internet. Any person accessing information through the use of College IT resources must determine for themselves whether the accessed information is appropriate for use.

The College will restrict or prohibit the use of its resources in response to violations of College policies or laws. When it has been determined that there has been a violation, the College will remove or limit access to IT resources and material posted on College-owned computers or networks.

Data transmitted or received using College IT systems may be stored by the College and may be used by the College in ensuring it can enforce relevant legislation.

Users who do not comply with College policies will be denied access to College IT resources. Any potential breach of this policy will be referred to the relevant disciplinary policy and may result in disciplinary action.

Accepting a user account and / or using the College's computer resources shall constitute an agreement on behalf of the user to abide and be bound by the provisions of this policy.

Comments or questions regarding this document, or reports of security violations should be sent by email to: ITservicedesk@belfastmet.ac.uk.

4.5 Access to IT Resources

While the use of information and communication technologies is a required aspect of the College's academic programmes, access to the College IT systems remains a privilege and not a right. It is given to students and staff who act in a considerate and responsible manner and shall be withdrawn from those failing to maintain acceptable standards of use.

Users must not attempt to gain access to any IT resource that they are not authorised to access. This includes but is not limited to manual and electronic records/data, applications/programs, facilities and buildings.

Each user is responsible for the security of any College owned information resource in their possession (this includes but is not limited to computer equipment, network accounts, telephone/voicemail accounts and electronic and manual data, confidential or otherwise).

Each user is responsible for:

- All activities which originate from any of their accounts (i.e. network; email; telephone; voicemail; applications);
- All information sent from, intentionally requested, solicited or viewed from any of their accounts.

Users must not share their account passwords to other parties or allow use of their account to unauthorised persons. Users must not use or access another user's account.

Users must not attempt to exploit security weakness. This includes creating and/or running programs that are designed to identify security loopholes and/or decrypt intentionally secure data. This will not apply to authorised support staff in the performance of their duties.

All currently enrolled students can have access to IT resources but may be asked at any time to produce a valid student card. Failure to do so will result in the individual being denied access to resources.

When any user terminates his or her relationship with the College, their ID and password shall be removed to deny further access to College IT resources.

User accounts which have been inactive for a period of 6 months shall be removed from the system at the discretion of the Head of IT and the College may delete all data associated with that account.

The College will ensure that users have access to IT resources. Where identified by staff in Human Resources or Learner Services, additional hardware or software will be provided in certain circumstances e.g. to facilitate a disability or language barrier.

4.6 Use of IT Resources

The College believes that IT resources should be available on as wide a basis as possible, and should be used for the purpose of College business and related activities.

All users must respect the rights of other computer users, respect the integrity of physical facilities and controls, and respect all licence and contractual agreements related to College IT systems.

The use of IT resources must be in-line with the relevant policies that will be issued from time to time. This includes but is not limited to telephone, voicemail, email, internet and the corporate network.

Users are expected to practise sensible use to limit wastage of College IT resources or bandwidth. This includes avoiding unnecessary printing, and unnecessary Internet access, uploads or downloads.

Users must not use College IT resources to operate a business or participate in any pursuit geared to personal gain for themselves or an associate.

Users must not take part in or aid and abet any activity which may be criminal or may bring the College into disrepute, including (but not limited to) offences under the regulations/legislation stated at 4.2 above.

Users must not connect any equipment to the College's data or voice networks that has not been authorised by IT.

All computers connected to the College's networks, whether owned by the College or not, must have an approved, up to date virus-scanning software running in-line with the relevant policy and have the latest security patches installed.

All computers are locked so that no standard user is able to install unauthorised software. It is prohibited to run software, including apps and software utilities, without proper authorisation. All software must be legally obtained, tested and included in the assets registers.

Users will not, knowingly or carelessly, run or install on any computer (networked or otherwise) or give to another user, software intended to damage or place excessive load on the College's network. This includes, but is not limited to, programs known as computer viruses, malware, Trojan Horses, and worms.

Users must not violate the terms of any applicable software licensing agreements or copyright laws through inappropriate copying and/or distribution of computer software, music (MP3, etc.), movies, copyrighted text or images.

Users must report any security weaknesses or incidents of possible misuse of College information resources in-line with the relevant policy and procedures.

College information must only be used in the conduct of College business. Users must abide by applicable laws and policies with respect to accessing, using, or disclosing information.

Each data user is responsible for the consequences of any misuse.

Users will respect the confidentiality and privacy of individuals whose records they access in line with the General Data Protection Regulation. Personal data held by the College must only be used for the purposes specified in the College's Data Protection Policy.

The College cannot condone the removal of data from College systems for any purpose other than transfer to an appropriate body such as the Department for the Economy (the Department). In the case of the Department, measures have been put in place by the Department for the safe transfer of data. There are no accepted circumstances where personal data as defined in the Data Protection Act, or Confidential Business Data needs to be taken off the premises (or transferred between parts of the Business) using any medium such as USB, DVD or even on the hard drive of a laptop etc.

Users must ensure that all work-related information (data; documents; email; locally developed applications) is stored on their own network drive (shared drive or College provided “OneDrive”) or on departmental or other shared drives (e.g. College SharePoint sites). These drives reside on central servers, which are routinely backed up.

Users must comply with all security and control procedures for personal and administrative data to which they have been authorised to view, create, modify, delete, copy, download or transfer.

Users are expected to assist in the maintenance of data quality in line with the relevant policy.

4.7 Care of IT Resources

All College IT resources should be cared for in a responsible manner. All food, drink, chewing gum etc. must be kept away from IT equipment.

Any damage, loss or theft of College IT resources must be reported immediately to either IT Service Desk or a security representative.

Users must not cause College IT resources to become unusable or inaccessible to other Users through abuse or misuse.

Users must not remove material (e.g. files, printouts) belonging to other Users and must leave all support materials provided by the College (e.g. manuals, removable media, etc.) in the facility.

Users must not attempt to modify College IT resources without specific written authorisation.

Users must not intentionally jeopardise the security of any College IT resources.

IT resources are intended to be used by the individual that has been provided them. No unauthorised persons should be permitted access to the IT resources, such as family members or friends.

4.8 IT Passwords

4.8.1 Password Selection

- Passwords should consist of a memorable phrase or collection of words;
- Passwords must be at least 20 characters in length;
- Must be a minimum of five words;
- Must only be used in on the college systems and not on personal, home or external systems;
- Should avoid replacing the letter 'O' with a zero (or replacing the letter 'I' with the number one) or any other techniques as hackers can exploit these rules.

4.8.2 Password Control

- Passwords must never be shared if they relate to a personal user id;
- Must not be entered into macros, software or script files;
- Must not be transmitted or stored in clear text;
- Must only be reinstated via a formal process if forgotten;
- Must be issued as pre-expired to force change on first use;
- Must not be easily guessable.

4.8.3 Password Changes

- To assist users in remembering their passwords, not writing them down and not reusing old passwords; the college will not be enforcing frequent password changes;
- Passwords should only be changed in the following circumstances;
    - When it is suspected that the password has been compromised e.g. known by someone else apart from the owner;
    - The password has been forgotten;
    - The user's account has been hacked;
    - Upon instruction from the College.

4.8.4 User Responsibilities

- Do not share passwords;

- Do not re-use passwords or write them down;
- Avoid creating passwords that are easily guessable;
- Change passwords on indication or suspicion of compromise;
- Use different password for privileged and non-privileged accounts.

4.9 Electronic Communications

4.9.1 Electronic Communications Acceptable Use

Use of the College's electronic communication systems, services and equipment are subject to the following conditions:

- Electronic communication systems services and equipment are provided primarily for teaching and conducting College business;
- Electronic communication records pertaining to the administrative business of the College are considered College records whether or not the College owns the electronic communication equipment or system used to create, send, forward, reply to, transmit, store, hold, copy, download, display, view, read, print, or record them, and are subject to the College's Records Management policy;
- Information relating to the College's students, staff, customers and some of its business operations are confidential. All such information must only be used for the purpose(s) intended and not disclosed to any unauthorised third party (this may sometimes include other employees/workers of the College);
- Confidential information should never be transmitted without appropriate protection; Consideration must be given to the nature of the content or the method of communication used and the appropriate standards of security must be exercised in line with the information handling procedures;
- Use may be made of electronic communication systems, services and equipment for incidental personal purposes provided that:
    - The systems are not used for private business or other commercial purposes;
    - Use of the equipment or system does not interfere with the normal performance of the user's duties and there is no breach of the prohibitions identified in this policy;
- Any abuse of the electronic communication equipment or systems is reported immediately, once users become aware of it taking place;
- Use does not violate other College policies, procedures or guidelines.

4.9.2 Electronic Communications Unacceptable Use

Electronic communication equipment and systems **must not** be used to:

- Take part in or aid and abet any criminal action including (but not limited to) offences under the regulations/legislation detailed in 4.2 above;
- Take part in or aid and abet any criminal action including cyber-attacks on the College network and/or other external networks, in alignment with the regulations and legislation outlined in Section 4.2
- Transmit or forward on, download, retrieve browse or store any messages, attachments, images or pages that contain offensive, libellous, defamatory or obscene material including but not limited to, pornographic, racist, homophobic, disablist, terrorist, anarchic, insulting and sexist material;

- Download, store, transmit browse, post, tweet or forward on messages, images or pages that are intended to harass, intimidate, persecute, terrorise or bully other users because of their gender, age, race, sexual orientation, religious belief, disability, political opinion, marital status, caring responsibility or other similar categories of difference (this includes the use of 'jokes');
- Introduce or transmit pirated or unauthorised commercial software or deliberately spread computer viruses, malware, worms or Trojan horses or programmes that create trap doors or sustain high volume network traffic that substantially hinders others in their use of the network, deliberately corrupt, modify or erase data or programmes intentionally interfering with the normal operation of the College's network;
- Use the facilities in such a manner that would inhibit, distract or have a detrimental effect on the provision of services;
- Introduce copyright material without the owner's permission onto the College's network;
- Use technologies, such as AI, to leak/compromise sensitive data outside the boundaries of the College network;
- Transmit or upload personal, sensitive personal or confidential information without the appropriate safeguards, such as encryption;
- Overload or disable the network or electronic communications equipment and systems or attempt to disable or circumvent any security mechanisms intended to protect the security and privacy of those systems or any associated information, records or messages;
- Employ a false identity or hide the identity of the sender or tampering with the communications of others;
- Abuse the services and computer facilities in such a way that wastes resources (including employee time), denial of service, global mailings etc. not taking appropriate care in terms of limiting file sizes and maintaining archives of messages sent and received, that will have a detrimental impact on the performance of the College's network;
- Access, receive, transmit or circulate inappropriate or non-business related material to others including (but not limited to) chain letters, business opportunities, jokes, electronic greeting cards, executable files, Items for sale, entertainment software, gambling or betting, financial markets, sport scores, social networking or any other bulletins that are not business related;
- Operate a business or participate in any pursuit geared to personal gain for themselves or an acquaintance;
- Enter into any contractual arrangement using a College electronic identity and/or address as any part of a personal contract with a third party or purchase goods and services i.e. internet shopping;
- Promote personal views that are detrimental to the College or commonly regarded public decency or participate in discussions that are politically sensitive or controversial or give advice on information that they know to be contrary to the College's policies and interests;
- Send out global messages without authorisation.
- Send any college business related email, attachments or documentation to their own personal email account or personal/unapproved cloud storage or file sharing platform.

Exceptions to the above will apply to employees who, as part of their job function, have to access material that may contravene the unacceptable uses listed in this policy. All such employees will need authorisation from their line manager in order to gain access to such material. Users are required to ask their line manager to submit any such requests to the IT Service desk.

4.9.3 Electronic Communications Monitoring

The College will monitor and audit its business communications and may access the content (with the written authorisation of a College Head of Department) in order to:

- Provide evidence of business transactions;
- Ensure the accessibility of business records;
- Ensure that the College's business processes, policies and procedures and contracts with staff are adhered to;
- Comply with its legal obligations;
- Observe standards of service, conduct, staff performance and for staff training purposes;
- Prevent and/or detect unauthorised use, abuse or any criminal activities taking place using the College's network, electronic communication equipment and systems; and
- Maintain the effective operation of the College's electronic communication equipment and systems and to carry out system maintenance, problem resolution and capacity planning.

The College does not monitor the content of electronic communications as a matter of course.

However, if misuse is suspected which contravenes this policy or the College deems it to represent a threat to the security of College information systems, the College reserves the right to inspect the content of any electronic messages without authorisation from or notification to the sender and/or the recipient.

5 Policy Breach

If any user is found to have breached this policy or any related policy, they will be dealt with in accordance with the College's relevant disciplinary procedure. This form of action may lead to termination of employment for employees; termination of a contract in the case of service providers, consultants or temporary staff and expulsion in the case of a student.

It is a condition of computer systems usage that all users abide by the terms and conditions of this Policy. The use of IT resources and electronic communication equipment must always be consistent with the College's statutory obligation in which to maintain the highest ethical standards.

If a breach of this policy has the potential to be of a criminal nature, the College reserves the right to refer the matter to the relevant authority.

If users do not understand the implications of this policy or how it may apply to them, they can seek advice from their line manager, Human Resources or the IT Helpdesk.

6 Related Policies

This policy should be read in conjunction with the following:

- JANET Acceptable Use Policy (AUP)
- Data Protection Policy
- Staff/Student Disciplinary Policies
- Equal Opportunities Policies – Staff/Student
- Staff/Student Code of Conduct