Bury College Strategies, Policy, and Procedures

[redacted]

Document Information

IT Student Computer Use Policy

Directorate:	IT Services
Document Owner:	Mike Doherty
Document Type	Policy
Date:	May 2024
Version:	1.4
Review Period:	1 Year (or as required)
Reviewed by	Head of IT Services, Cyber Security Officer, AP - Personal Development, Student Information Manager, AP - Marketing Projects and Student Admin, AP - Academic and Technical
Date Approved:	8th May 2024
Approved by:	Leadership Team
Requires Publishing to the College Website	No
Equality Impact Assessed:	Yes

Version Control Tracking

Version	Date	Revision Description	Editor	Status
1.0	14/11/2019	IT Students to complete an additional form for acceptance of conditions for students who have additional privileges. Not to install or run any new software (this includes but not limited to remote viewing software and games)	FA/MD	Replaced
1.1	21/4/2021	Added liability section changed (h) bypass logins. Added 16 - tampering	MD	Replaced
1.2	26/4/2022	Annual review/update -Added section 6 - Investigations	FA/MD	Replaced
1.3	14/01/2023	Wording changes	MD/MW	Replaced
1.4	01/05/2024	Clauses 21 and 22 added.	MD/MW	Approved

Bury College Student Computer User Policy

Conditions for Use of any Computing Facility

The following conditions apply to any student using any College computer. In this context, computer shall refer to any standalone or networked computer (or virtual server for remote access) or any computing equipment (laptop/tablet) containing an electronic processor, or peripherals thereof.

1 A student shall only use computers for which access permission has been specifically granted (in some cases this may require another form to be completed and acceptance of further conditions). In particular, students are expected to use computer networks to connect only to their own user area. 'Hacking' around the network or attempting to circumvent restrictions including but not limited to network sniffing software, non-supported browsers, VPN services from a machine which is sited on or off College premises, will be treated as an abuse of the overall computer system.

a. This means that you will not use anyone's username and password other than your own. Using someone else's username and password automatically constitutes 'non-authorised' access, even if someone else gave you their username and password and gave permission for you to use them.

b. If you give your username and password to someone else, you are contributing to 'non-authorised' access, which is strictly prohibited and could result in disciplinary action.

2 A student shall observe the rules pertaining to Learning Resource Centres (LRC) and IT Computer rooms as displayed and shall be responsible for any damage caused as a result of disobeying the rules. In particular:

a. Personal stereo equipment and mobile telephones shall not be used in these areas at any time.
b. Eating, drinking, and smoking/vaping are not permitted at any time.
c. A student must vacate a room which is booked for a class of which he/she is not a member when asked to do so by a member of staff.
d. A student must always wear a valid College identity badge.

3 A student shall not misuse the electronic mail system (email) provided to them, in particular by sending abusive, offensive or disruptive messages or by attempting to bypass restrictions. 'Block' mailing (to many recipients) shall not be used. Electronic mail is not a secure medium and should never be used to communicate sensitive information. The College reserves the right to monitor e-mail usage and content.

4 A student shall only use a computer in conjunction with the course of study they are following at the College. In particular, no personal, commercial or bureau work on behalf of College or

non-College persons or companies, (whether for payment or not) may be done without written prior consent of a member of the Management Team.

5 All work done by the student with the assistance of College equipment shall remain the property of the College for the duration of the course and the College reserves the right to confiscate any unauthorised or inappropriate material.

6 All students are expected to follow the College's guidance and best practices on setting and using passwords associated with their College account(s). It is in the interest of both the student and the College that careful consideration is taken when setting, using and storing passwords.

7 Should the College suspect a student is accessing, viewing or downloading any material deemed to be of a suspicious nature or not in-line with their College studies, the College reserves the right to actively access files which are stored on College systems and cloud-based services provided by the College and also to remotely monitor College-owned devices without warning to carry out investigative reporting to gather evidence which could be used for disciplinary action and also shared with a third-party, this includes but not limited to law enforcement agencies where necessary.

8 The College takes IT security very seriously to protect its network and IT systems particularly against external threats and as a result, students are required to set-up multi-factor authentication (MFA) when they start their studies to access College resources away from the College premises to protect their account. This will require the use of a personal device which includes but not limited to a mobile phone with the use of an authenticator app or SMS message. Where this is not possible due to no compatible device, the College will do all it can in a secure manner to facilitate external access, however students must accept that they may have to forfeit their external access. The College has no control over the devices used for MFA purposes and are solely used as a means of verifying identity.

9 No person or persons shall, by any wilful or deliberate act, jeopardise the integrity of the computing equipment, its systems software or other stored information. Neither shall they attempt to install any new software that has not been authorised by a member of the IT Services Team on any computer in the College. This also refers to music and video files unless directly required for your course study, in this case written permissions will be required from your tutor with consultation with the IT Services Team.

10 A student using a computer which is linked to the internet shall only access work which is appropriate to their course of study. At no time shall they access or reproduce any material which the College considers to be offensive or distasteful or which is classed as illegal. The College reserves the right to monitor internet and e-mail usage. Logs of access may be used in any disciplinary proceedings. The College employs a sophisticated web filtering and logging process for the College's internet activity. Any student found to be attempting to bypass this will immediately be in breach of this policy.

11 Every person authorised to use a computing resource is expected to treat the information which is available on the system as confidential. No part of this information shall be copied,

modified, or used without the permission of the appropriate person(s). In particular, this applies to software for which special copyright conditions apply.

12 The transmission, storage or display of offensive, defamatory or harassing material is strictly forbidden and enforceable law under the Criminal Justice and Public Order Act 1994.

13 Whilst every endeavour is made to ensure that the computer systems (hardware, communications, and software) are fully functional, no liability can be accepted by the College for the consequence of any errors or failures of the computer systems.

14 Whilst every endeavour is made to ensure the integrity and security of information held on computer media, no consequent liability can be accepted because of any such information being inadvertently lost or corrupted. It is recommended by the College, and it is the student's responsibility to keep a backup of College work and to store it appropriately using reliable media forms, this includes but not limited to cloud storage.

15 The College management is authorised to suspend any account involved in a suspected breach of these conditions, pending investigation. Reinstatement of any such account will require written approval from a senior member of the College staff.

16 Whilst the College appreciates that students may wish to bring personal devices into College, this is allowed assuming full compliance and respect to College policies. The use of students' own devices in classrooms and directed study/assessment activities is at the discretion of the tutor in charge, who accepts responsibility for enforcing College rules. The College takes no responsibility for the loss or damage to personal devices. No personally owned power supplies (chargers) for mobile devices are to be plugged into College socket outlets as all electrical items require a valid PAT test. In social areas around the College, USB socket outlets are available for charging compatible devices.

17 Students are NOT PERMITTED to connect privately owned laptops/tablets/smart phones/portable music players (this is not an exhaustive list) directly into the College network. This is not allowed due to network security reasons and students should use the Colleges Wi-Fi system which is intended for personal devices to access to the internet. The College subscribes to the 'eduroam' service which enables students to use WiFi at organisations where this service is supported such as hospitals and universities with their College credentials, therefore should a supported organisation need to investigate activity associated with a Bury College account which has been connected to their eduroam service, the College reserves the right to share details of the user as appropriate.

18 Any abuse/damage of the College's computing equipment or software, or to any of the rooms and their facilities and services which contain that equipment or software will be investigated as appropriate. The term 'damage' includes modifications to hardware or software which, whilst not permanently harming the hardware or software, incurs time and/or cost in restoring the system to its original state. Costs associated with repairing or replacing damaged equipment or software and/or in providing temporary replacements may be charged to the person(s) causing the damage. The costs will be determined by the College and may also result in disciplinary action and the ultimate penalty is expulsion from the College.

19 Students will not tamper with other students work or try to access their computer whilst they are logged on. Tampering or writing inappropriate messages in other students work, will alert the monitoring system and students who do this will be subject to disciplinary and this might be deemed as bullying and harassment.

20 The College is involved in the Governments National Strategy ‘Prevent’ to safeguard our students with regards to extremism and radicalisation. To support the Prevent initiative, the College will monitor the use of the College network, email, and internet activity for all students.

21 Any student who is issued with a College laptop, tablet or other mobile device must understand that it is to be used for College purposes only and it remains the property of the College at all times when allocated to the student. Under no circumstances must any of these devices whilst allocated to an individual be tampered with, modified, or repaired by the allocated individual or by a third-party. This includes but not limited to, removal of any internal storage devices, repairs to broken/faulty screens and use of non-OEM power supplies.

22 Students who have extra permissions for courses, including but not limited to, IT and Computing, shall follow all the points in this policy and should a student with these extra permissions be found to have abused these privileges in order to bypass, tamper or harm the College computers or network in any way, their IT access will be revoked pending investigation which could ultimately result in the removal of their permissions, permanent IT access blocked or expulsion from the College depending on the severity of the issue.

Summary

The conditions may be summarised as:

a) Only use computers which you are permitted to use.

b) Only use your own username and password to access the College computer network.

c) Only use the computer facilities including internet access and e-mail for work associated with your studies.

d) Do not misuse computer resources - other students need to use these resources.

e) Do not give your username and password to someone else, you are contributing to ‘non-authorised’ access, which is prohibited.

f) Do not steal or interfere with the software loaded on any computer or network.

g) Do not bring unauthorised software into College: this includes video and mp3 files.

h) Do not attempt to gain unauthorised access to computer systems or bypass login procedures.

i) Do not behave in an anti-social manner to other users.

j) Do not access, download, transmit, display or store any material which could be considered offensive, defamatory, harassing or is classed as illegal

k) Do not disclose your password to any other computer user

l) Follow the Colleges best practices on setting, using and storing passwords.

m) Do not write, store, or send any material in any e-mail account that you access from College that may go against this policy. This will include subscribing to chat/e-mail forwarding services that are deemed inappropriate.

n) If when using College computer facilities, you receive any material which could be considered offensive, defamatory, harassing, or classed as illegal, you must contact a member of the IT Services Team who can be contacted via Reception.

o) Take a backup of work at regular intervals using reliable media forms.

p) The use of students' own devices in classroom and directed study/assessment activities is at the discretion of the tutor in charge.

q) Students are NOT PERMITTED to connect privately owned laptops/tablets/smartphones/portable music players (this is not an exhaustive list) directly into the College network. Students should use the College WiFi system.

r) Abuse/damage of the College's computing equipment - replacement costs may be charged to the person or persons causing the damage.

s) If you suspect a student is not abiding by the Student Computer User Policy then you must contact a member of the IT Services Team who can be contacted via Reception. You must discuss your concerns only with the member of the IT Services Team, not other staff and not with other students.

Liability for Misuse and Disciplinary Action

Users and the College are potentially at risk for a range of civil and criminal liability arising from misuse of the Colleges computing facilities. Legal liability can arise from:

- defamation under the Defamation Act 2013
- copyright infringement under the Copyright, Designs and Patent Act 1988
- breach of confidence
- negligent virus transmission
- breach of the Computer Misuse Act 1990 and the Police and Justice Act 2006
- breach of the Obscene Publications Acts of 1959 and 1964, the Protection of Children Act 1978, the Criminal Justice and Immigration Act 2008 and the Telecommunications Act 1984 and the Communications Act 2003

- computer hacking
- harassment and discrimination under the Equality Act 2010, the Racial and Religious Hatred Act 2006 and the Malicious Communications Act 1988
- the Data Protection Act 2018 and the Human Rights Act 1998
- the Investigatory Powers Act 2016, the Privacy and Electronic Communications Regulations 2003, the Terrorism Act 2006, the Serious Organised Crime and Police Act 2005 and the Counter-Terrorism and Security Act 2015.

Misuse of the College computing facilities (including failing to comply with this Policy) may expose both Users personally and/or the College to court proceedings attracting both criminal and civil liability. Users will be held responsible for any claims brought against the College for any legal action to which the College is, or might be, exposed as a result of User's misuse of the Colleges computing facilities including reimbursing the College for any financial liability which the College suffers as a result of Users actions or omissions.

The College considers failure or refusal to comply with this policy to be a serious disciplinary offence which may lead to disciplinary action taken including withdrawal of services and/or expulsion with or without notice.

Formal declaration by the student

I abide by the conditions and spirit of College membership as expressed in the above policy. I accept that any breach of this policy may result in the College's disciplinary procedure being applied.

Please Note: Student signature on the Bury College Enrolment Form automatically constitutes agreement to abide by the conditions of this policy.

Preliminary Equality Impact Assessment

Screening for effects on equality	
Name of policy being assessed.	**Student Computer User Policy 2022-2023**
Policy Holder and/or person with authority to make changes to policy:	Mike Doherty
Position:	Head of IT Services
Directorate:	IT Services
New/Revised/Reviewed Policy:	Revised
What is the aim, objective or purpose of the policy, procedure, strategy or decision?	
The aim of the policy is to ensure the successful management and conditions for use of any Bury College IT Computing Facility by students "including but not limited to" Computers (PCs), Laptops, tablets etc. In this context computer shall refer to any stand alone or networked computer (or virtual server for remote access) or any computing equipment (laptop/tablet) containing an electronic processor, or peripherals thereof.	
Who was consulted when the policy was first written?	
IT services and Leadership Team (for approval).	
Who does the policy affect?	

This policy applies to: All students of Bury College with access to the College network or IT facilities.
Who implements the policy, and what steps will be taken to ensure the effective implementation of the policy?
IT Services are responsible for reviewing and implementation the policy which will be accessible on SharePoint for staff to access and cascade policy information to their students. The revised policy will be reviewed by IT services and adopted by the Leadership team.
What pre-existing evidence is available to facilitate the screening of the policy?
For example: • IT Services • IT Audits • Published research/Expert opinion sought (JISC) • Leadership Team

What impact is the policy likely to have on the following characteristics?

Protected characteristic*	**Positive impact**	**Negative impact**	**Neutral impact**	**Unclear**	**Further comments**
Age (or age group)	□	□	√	□	
Disability	□	□	√	□	DDA will be considered
Gender reassignment	□	□	√	□	
Pregnancy and maternity	□	□	√	□	
Race (including ethnicity and nationality)	□	□	√	□	
Religion or belief	□	□	√	□	
Sex	□	□	√	□	
Sexual orientation	□	□	√	□	
Looked after learners	□	□	√	□	
Social-economic	□	□	√	□	
Carers	□	□	□	□	N/A
Ex-offenders	□	□	√	□	

***Protected Characteristics as identified by the Equality Act 2010.**

If any answers are 'negative' can any adverse impact be justified on the basis of a legal requirement? **Yes** ☐ **No** ☐

If 'yes', please explain:

Please detail any suggested actions identified to improve positive impact or remove negative impact of this policy.

Issue identified	**Suggestion action to address this issue**

Should a Full Equality Impact Assessment be carried out?

Yes ☐ **No** √

If 'yes', is the priority High or Low?

Yes ☐ **No** ☐

Please explain the justification of Full Equality Impact Assessment Decision

How will this policy be approved? *Leadership Team*

This Preliminary Impact Assessment was checked and signed off by the policy holder:

Name & Signature	*M Doherty*
Date	**May 2024**

Once completed please return (a) a signed hard copy of the form and (b) an electronic version (to be published on the intranet) to …………………………………