Greater Brighton Metropolitan College

Acceptable Use of IT by Students Policy

Policy review area	Curriculum
Lead manager	Head of IT
Approval level	CMG
Start date	September 2021
Review cycle	1 year
Next review	August 2022

1. Purpose and Scope

1.1. The Greater Brighton Metropolitan College (the College) depends upon the integrity of its computer-based services and the availability of its Information and Communications Technology (ICT) systems for its academic activity and business functions. If any of these systems are unavailable or their information is compromised, then teaching, learning and business processes may well be disrupted.

1.2. To help protect against these risks the College has developed this Acceptable Use Policy (AUP), which seeks to ensure that all College systems and ICT equipment is as secure as is possible against loss caused by inadvertent or malicious actions and to safeguard these systems from unacceptable use.

1.3. Failure to comply with these terms and conditions may lead to removal of access to college IT systems.

1.4. This document sets out the rules for the use of College ICT facilities by College Students and will be regularly reviewed. Where the expressions PC or computer are used, the policy applies equally to the use of Apple Macs and Chromebooks.

1.5. This policy should be read in conjunction with the college Safeguarding & Prevent, Anti-Bullying and Student Management policies.

2. Security

2.1. Connections: College Students must not connect any personal device to the College network (excluding wireless) or ICT equipment. See Appendix 1 for exceptions.

2.2. College Students are not permitted to disconnect any IT equipment from the College network (excluding wireless). See Appendix 1 for exceptions.

2.3. Movement: No ICT equipment or facility may be relocated.

2.4. Leased Equipment: The College has a range of equipment on lease. This equipment must not be tampered with, marked or modified in any way. The cost of repairing or replacing any damaged or lost leased equipment will be charged to the student responsible for the damage or loss.

2.5. Computer Operating Systems: For licensing and security reasons the installation or modification or removal of a computer operating system is not permitted except by the IT Services Department or as part of supervised study i.e. on a computing course.

2.6. Computer Applications / Software: For licensing and security reasons the installation, modification or removal of computer software or applications is not permitted except by the IT Services Department.

2.7. Any personal CD, DVD, memory stick or portable media brought into the College must be free from any virus or other malware before using on any College system. If in doubt contact the Helpdesk and have the media checked before using. The cost of any corrective actions,

products or the use of third parties to repair any damage caused by the introduction of a virus, etc. may be charged to the student responsible for the introduction of the problem.

3. Access to computers

3.1. All activities relating to the use of the College's ICT equipment is traceable to an individual user. Log files may be examined on specific authority of the Executive Team, excepting operational issues that may arise and necessitate the examination of the logs for operational or technical reasons by IT Services.

3.2. All College ICT equipment must be in good working order and all reasonable efforts made to meet the manufacturer's guide. Any faults or problems should be immediately reported to the IT Services Helpdesk, Ext. 2580 or email itservices@gbmc.ac.uk or visit PT702 (Pelham Campus), WD248 (West Durrington Campus), or BWR05 (Broadwater Campus) during the published hours.

3.3. Care must be taken to protect College ICT equipment against accidental damage or theft to an appropriate level in relation to the value and importance of the items. It is the responsibility of all Students to report any of the above problems to the IT Services Helpdesk and to complete the appropriate forms and comply with any College policies regarding these matters such as Health and Safety.

3.4. It is in the best interests of every student that proper attention is given to all Health & Safety issues. Any dangerous equipment should be immediately isolated and the IT Services Helpdesk and / or Premises informed.

3.5. Access to all College Students-based ICT equipment is restricted to enrolled Students only. Student accounts are created for enrolled students via an automated hourly process.

3.6. Enrolled students are expected to be sufficiently familiar with the operation of any equipment they use to make its use safe and effective and to avoid interference with other users.

3.7. Use of the College's ICT facilities constitutes acceptance of this policy.

3.8. The granting of access rights to computer-based facilities will be by the provision of user accounts and passwords giving access to hardware, software and storage locations.

3.9. Usernames and passwords are for the use of the individual to whom they are issued and are for the purposes for which they are issued. Users must not use someone else's username and password nor allow their username and password to become known and used by any other person.

3.10. Passwords should not be easy to guess, must be a minimum of 8 characters in length with a least 1 capital letter, 1 number and 1 special character such as *, & or $. If it is suspected that a password is known by anyone other than the assigned owner of the username then the password must be changed immediately or the Helpdesk contacted for further assistance.

3.11. Forgotten passwords can be changed by a personal visit to IT Services or LRC's and presentation of Students ID. College staff are instructed not to change passwords for individuals they do not recognise or who have no proof of identity.

4. Use

4.1. For operational and/or technical reasons IT Services may access accounts at any time.

4.2. Student computer use is actively monitored for safeguarding and Prevent purposes. This may involve collection of data by Smoothwall Limited, Smoothwall Inc and Crisp Thinking.

4.3. Students will not create, display, produce, store, circulate, download or transmit in any form or medium socially unacceptable or offensive material that causes or may cause, sexual, racial, terrorist or extremist harassment.

4.4. Students will not create or transmit material which is designed or likely to cause annoyance, inconvenience or needless anxiety.

4.5. Students will not create or transmit defamatory material.

4.6. Students will not create or transmit material that infringes the copyright of another.

4.7. Students will not corrupt or destroy the data or work of other users.

4.8. Student files and folders are deleted when their course finishes - students are responsible for moving these to personal storage beforehand if necessary.

4.9. Students will not use the College systems in a way that denies these services to others – for example deliberate or reckless overloading of access links or email servers or hack or attempt to hack into corporate systems.

4.10. Students must take precautions against the introduction of viruses, malware or other harmful programs or products either through downloading from the Internet or from other media. Any that are suspected or found should be immediately reported to the IT Services Helpdesk.

4.11. Students must log out at the end of each session. Failure to do so could leave a user's account open for use or misuse by others and risk corruption to user files.

4.12. Users who have logged on to a personal computer must not leave that computer unattended or potentially usable by another person other than the registered account owner. Computers may be left with an activated password protected screen saver or other keyboard locking and screen blanking process for short time periods only. If the computer is to be left unattended for any time longer than 5 minutes, then the computer should be logged out. No computer should be left unattended with any unsaved files left open, failure to save and close files when leaving the computer may lead to the loss or corruption of the data.

4.13. The use of the College's Internet facility is restricted to sites that are not blocked by the College Internet Filter Tool. Access to Blocked sites is only permissible if authorised by the Head of Department. To request access to a blocked site please speak to the course tutor.

4.14. Personal use of the Internet during non-work time, for example during lunchtime, is only permitted if:

4.14.1. The use does not cause disruption to the performance of the Internet for business purposes i.e. when access to the Internet is slow

4.14.2. It is not used for purposes that are socially unacceptable or offensive

5. E-mail

5.1. The Student email system should only be used for College related matters.

5.2. The use of the College email system is logged; these log files may be examined by IT Services for operational reasons at any time.

5.3. All College email accounts including their contents and any associated files remain the property of the College.

6. Social Media.

6.1. Students should ensure that their privacy settings on Social Media are adjusted to control and restrict who can access the information they post and the activities they undertake. Students are responsible for adjusting the privacy settings for their Social Media accounts – please note that default privacy settings may lead to information being available to others outside an individual's circle of contacts. Information available on Social Media can be used by the College in accordance with its policies and procedures, or in legal proceedings.

7. Prevent

7.1. Use of the internet should be in accordance with the college's Safeguarding and Prevent Policy which is available on the college website.

7.2. Systems are in place to block access to, and log blocked attempts to access, extremist materials in accordance with our Prevent Strategy

7.3. For further help or advice, please contact the College Safeguarding Team

8. Printing

8.1. Students are not permitted to load paper into the printers unless under supervision of staff.

8.2. College printing equipment should only use manufacturers' recommended toner, ink or paper.

8.3. Printer usage is charged and recorded.

9. Retention of data / files

9.1. Student data and software will be subject to reorganisation, removal or archiving at certain times. When possible, IT Services will give adequate notice to those users affected.

9.2. At the end of their course, Students are responsible for moving any files and documents they wish to keep from College storage (network or Google Drive) to their own, personal storage.

9.3. All students have a responsibility to ensure they perform their own housekeeping upon their file space, both regarding data files stored on disks and email messages.

9.4. Care should be taken to prevent the build-up of unnecessary files on the systems.

9.5. IT Services may delete jobs which remain in an electronic print queue after a reasonable period.

10. Viewing log files

10.1. For security, maintenance, fault finding and volume purposes, the College reserves the right to:

10.1.1. View computer log files such as email logs

10.1.2. View electronic records such as logon/logoff times

10.1.3. View electronically stored data

11. Disclaimer

11.1. The College accepts no responsibility for:

11.1.1. The malfunctioning of any ICT facility or part thereof

11.1.2. The loss of any data or software or the failure of any security mechanism.

11.1.3. Any loss alleged to have been caused whether by defect in the resources or by act or neglect of the College, its employees or agents.

11.1.4. Any loss to a user consequent upon failure to log out at the end of a session. Any loss to a user as a result of leaving a logged-in computer unattended.

12. Non-institutional Use

12.1.1. Commercial: The use of ICT facilities for commercial purposes whether for gain or not, is not permitted unless for and on behalf of and under arrangements with the College. Such use is not permitted without the explicit written prior permission of the Principal.

12.1.2. Placement: The use of ICT facilities to the substantial advantage of the employers of placement students must have the explicit written prior permission of the designated authority and may be subject to charge.

12.1.3. External: Use of ICT facilities by persons other than Students or students must have the explicit written permission of the designated authority and may be subject to charge.

Appendix 1

Acceptable devices

USB Memory Keys connected to USB extension leads only	Anyone
USB Digital Camera connected to USB extension leads only	Anyone
Speakers or Headphones and Microphone connected into extension leads only	Anyone

Appendix 2

Related and connected laws in the United Kingdom

- The General Data Protection Regulation (Regulation (EU) 2016/679 of the
- European Parliament and of the Council of 27 April 2016)
- Data Protection Act 2018
- Privacy and Electronic Communications Regulations 2003
- Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- The Common Law Duty of Confidentiality
- Data Protection Policy GRP101
- Computer Misuse Act 1990
- Digital Economy Act 2017
- The Freedom of Information Act 2000
- Environmental Information Regulations 2004
- Network and Information Systems Regulations 2018
- Data Retention and Investigatory Powers Act 2014
- Human Rights Act 1998