BMet
Inspiring futures, realising dreams.

Acceptable use of IT and Social Media Usage Policy

POLICY OWNER:	Data and IT
AUTHOR:	Rachel Jones
DATE OF REVIEW:	April 2021
DATE OF APPROVAL:	
FOR APPROVAL BY:	SLT
NEXT REVIEW DATE:	April 2022

1. POLICY STATEMENT

1.1 Our IT and communications systems are intended to promote effective and safe communication and working practices within the College. This policy outlines the standards you must observe when using these systems, the circumstances in which we will monitor your use, and the action we will take in respect of breaches of these standards. The policy also addresses our expectationsconcerning the use of Social Media.

1.2 This policy covers all employees, officers, consultants, contractors, casual workers, agency workers, students and anyone who has access to our IT and communication systems.

1.3 Misuse of IT and communications systems, or prohibited use of social media can damage the college and our reputation. Breach of this policy may be dealt with under our Disciplinary Procedure and, in serious cases, may be treated as gross misconduct leading to student expulsion or summary dismissal.

1.4 This policy does not form part of any employee's contract of employment or student learning agreement and we may amend it at any time.

2. RESPONSIBILITIES AND OBLIGATIONS

2.1 The Senior Leadership Team has overall responsibility for the effective operation of this policyand for ensuring compliance with the relevant statutory framework. Day-to-day responsibility for operating the policy and ensuring its maintenance and review has been delegated to the Director of IT and Data.

2.2 Managers have a specific responsibility to ensure the fair application of this policy and all members of staff are responsible for supporting colleagues and ensuring its success.

2.3 The IT Department will deal with requests for permission or assistance under any provisions of this policy, and may specify certain standards of equipment or procedures to ensure security and compatibility.

2.4 All staff have the responsibility to comply with this policy and ensure that they do not compromise the security of college systems.

PROCEDURE/COMPLIANCE OBLIGATIONS

3. EQUIPMENT SECURITY AND PASSWORDS

3.1 You are responsible for the security of the equipment allocated to or used by you, and must not allow it to be used by anyone other than in accordance with this policy.

You are responsible for the security of any computer terminal used by you. You should lock your terminal or log off when leaving it unattended, to prevent unauthorised users accessing the system in your absence. Anyone who is not authorised to access our network should only be allowed to use terminals under supervision.

You should not allow family members or anyone else to use college equipment when working at home.

3.2 Desktop PCs and cabling for telephones or computer equipment should not be moved or tampered with without first consulting the IT Department. Students should be directed to contact the LRC counter for assistance.

3.3 For staff upon termination of employment (for any reason) you must provide details of your passwords to HR and return any equipment, key fobs or cards.

3.4 If the College has issued you with a laptop, tablet, smartphone or other mobile device, you must ensure that it is kept secure at all times, especially when travelling. Passwords must be used to secure access to data kept on such equipment to ensure that confidential data is protected in the event of loss or theft. You should also be aware that when using equipment away from the workplace, documents may be read by third parties, for example, passengers on public transport.

3.5 College equipment should not be used by any other person except the person issues the laptop. This includes other family members. Passwords and access to the laptop should not be shared with anyone except the member of staff or student.

4. PASSWORDS

4.1 You should use passwords on all IT equipment, particularly items that you take out of the College. You must keep your passwords confidential and change them regularly. You must not use another person's username and password ormake available or allow anyone else to log on using your username and password.

4.2 All staff will be required to use Multi-factor authentication (MFA), either by downloading an app to a mobile phone (this can be a personal mobile phone) or the college will provide staff with a dongle, that will have to be carried with them at all times. There will be a charge for replacement dongles, if lost.

4.3 College password for employees must now be at least 10 characters long and must contain a combination of the following details:

- A mixture of capital and lower case letters
- Include at least 1 number
- Include at least 1 special character

4.4 Passwords for employees will no longer be required to be changed every 90 days, and must comply with the criteria above. This will only be implemented where MFA and long strong passwords have been implemented.

4.5 You must not share your password with anyone. The college will never ask for your password and you should never enter it on any sites. Use a password that you only use for work.

4.6 Students will continue to use passwords with regular change requests. However Multi Factor Authentication will be trialled with some students during 21/22. The long term vision and to ensure security is that all staff and students will using MFA.

5. SYSTEMS AND DATA SECURITY

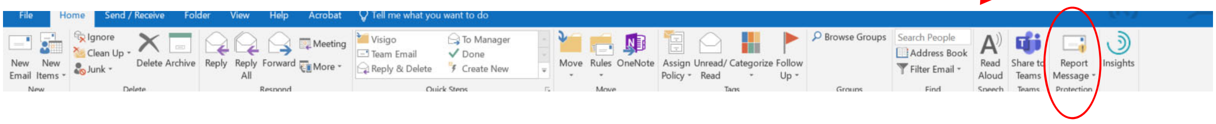
5.1 You should not delete, destroy or modify existing systems, programs, information or data (except as authorised in the proper performance of your duties or study).

5.2 You must not download or install software from external sources without authorisation except when necessary for College use. This includes software programs, instant messaging programs, screensavers, photos, video clips and music files. Incoming files and data should always be virus-checked by the IT Department before they are downloaded. If in doubt, students should contact the LRC counter and staff should seek advice from the IT Department.

5.3 You must not attach any device or equipment to our systems without authorisation from the IT Department. This includes any USB flash drive, MP3 player, tablet, smartphone or other similar device, whether connected via the USB port, Bluetooth, infra-red connection or in any other way.

5.4 We monitor all emails passing through our system for viruses. You should exercise particular caution when opening unsolicited emails from unknown sources or an email which appears suspicious (for example, if it contains a file whose name ends in .exe). Be particularly careful of e mails that you were not expecting, and if in doubt don’t click on the mail and seek advice from IT.

You can now inform IT and Microsoft using the new tool on your email desktop, which is quicker and more direct than contacting the IT helpdesk, as this uses AI to start to block emails automatically for other users. An example can be seen below:-



Inform the IT Department immediately if you suspect your computer may have a virus. We reserve the right to delete or block access to emails or attachments in the interests of security. We also reserve the right not to transmit any email message.

5.5 You should not attempt to gain access to restricted areas of the network, or to any password-protected information, except as authorised in the proper performance of your study/duties.

5.6 You must be particularly vigilant if you use College IT equipment outside college premises and take such precautions as we may require from time to time against importing viruses or compromising system security. The system contains information which is confidential and/or subject to data protection legislation. Such information must be treated with extreme care and in accordance with our Data Protection Policy.

6. DATA TRANSFER

6.1 If you have responsibility for transferring bulk data sets (for example spreadsheets containing multiple personal data entries) then you must seek advice from the IT team on the necessary security measures, including consideration of whether it is possible to anonymise the data.

6.2 Any data that is transferred should be zipped, password protected and transmitted via a secure system.

6.3 Passwords for any transmitted data, can only be shared with the third party, by a different form of communication i.e. text, call. Data transferred by email must not have the password then shared in a following email from the same person.

7. USB STORAGE

7.1 Whilst USB storage devices are a convenient method for uploading data between computers, they also present significant security risks entailing the loss of personal data. The College has now adopted Microsoft One Drive and this is considered to be a suitable alternative to the use of USB devices. However, this data is not backed up.

7.2 All College devices have encryption to encrypt USB drives provided by the College. For staff, these can be obtained from IT by logging an OTRS ticket. Only encrypted College provided USB devices may be used by staff on College IT equipment from April 2019.

7.3 For the avoidance of doubt, students may continue to save their College work onto USB devices although the use of Office 365 and One Drive should be encouraged as these are also significant cyber security threats to the College networks.

8. EMAIL

Although email is a vital tool, you should always consider if it is the appropriate method for a particular communication. Correspondence by email should be written as professionally as a letter. Messages should be concise and directed only to relevant individuals.

8.1 You must not send abusive, obscene, discriminatory, racist, harassing, derogatory, defamatory, or otherwise inappropriate emails. Anyone who feels that they have been harassed or bullied, or are offended by material received via email should inform their personal tutor or a member of security for students or line manager or the Human Resources Department for employees

8.2 You should take care when sending emails that contain personal data. As the majority of data breaches occur by sending e mails to the wrong person. In addition, if you are sending an email that falls within the definition of either (a) or (b) below you must follow the instructions below in respect of password protection:

a) The email contains the personal data of multiple people

b) The email contains sensitive personal data, i.e. information about one or more of the following:

- race;
- ethnic origin;
- politics;
- religion;
- trade union membership;
- genetics;
- biometrics (where used for ID purposes);
- health;
- sex life; or
- sexual orientation

When password protection is required the personal data should be zipped and password protected. The password must not be sent in the same e mail as the personal data, and ideally should be sent using a different form of communication (e.g. by phone call or text)

8.3 You should take care with the content of email messages, as incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or breach of contract. Remember that you have no control over where your email may be forwarded by the recipient. Avoid saying anything which would cause offence or embarrassment if it was forwarded to colleagues or third parties, or found its way into the public domain.

8.4 Email messages may be disclosed in legal proceedings in the same way as paper documents. Deletion from a user's inbox or archives does not mean that an email cannot be recovered for the purposes of disclosure. All email messages should be treated as potentially retrievable, either from the main server or using specialist software.

8.5 In general, you should not:

(a) send or forward private emails at work which you would not want a third party to read;

(b) send or forward chain mail, junk mail, cartoons, jokes or gossip;

(c) contribute to system congestion by sending trivial messages, copying or forwarding emails to those who do not have a real need to receive them, or using "reply all" unnecessarily on an email with a large distribution list;

(d) agree to terms, enter into contractual commitments or make representations by email unless appropriate authority has been obtained. A name typed at the end of an email is a signature in the same way as a name written at the end of a letter;

(e) download or email text, music and other content on the internet subject to copyright protection, unless it is clear that the owner of such works allows this;

(f) send messages from another person's email address (unless authorised) or under an assumed name; or

(g) send confidential messages via email or the internet, or by other means of external communication which are known not to be secure.

8.6 If you receive an email in error you should inform the sender and potentially contact the senders company GDPR lead.

8.7 Do not use your own personal email account to send or receive email for the purposes of college business/study. Only use the email account we have provided for you.

8.8 The college will not normally access individuals’ email accounts. However, it reserves the right to do so if it is reasonably necessary in the interests of the college, including for the following purposes (this list is not exhaustive):

(a)to monitor whether the use of the email system or the internet is legitimate and in accordance with this policy;
(b)to find lost messages or to retrieve messages lost due to computer failure;
(c) to access information stored in the email accounts of staff who are unavailable due to absence from work (for whatever reason), where that information is required before their likely return to work;
(d) to assist in the investigation of alleged wrongdoing; or

(e) to comply with any legal obligation.
Such access could include providing other members of staff with access and/or auto-forwarding emails to another account (including a group account with a logging system).

8.9 In the case of investigations for potential disciplinary events, the college reserves the right to access or search individual email inboxes without prior communication or consent.

9. WORKSTATION, STAND-ALONE AND MOBILE COMPUTER SYSTEMS (I-PADS AND WIDER TABLET TECHNOLOGIES INCLUDED)

9.1 The College owns the equipment on which the files are held and retains the right to supervise its use.

9.2 No workstations should be moved from its physical location unless supervised and agreed by IT. Movements in equipment can lead to potential security breaches and lead to longer lead times in diagnosing faults. Acts of this nature again will be subject to potentially disciplinary sanctions.

9.3 You must not try to reformat or download illegal software knowingly onto any college device. Any breach will be subject to disciplinary action, as this is a potentially high security risk to the college and also the college could be subject to significant fines. This type of behaviour will not be tolerated.

9.4 If you place files on local hard disks or cloud storage solutions, the responsibility for security and backup lies with you. Only data on shared drives is backed up centrally. It is your responsibility to ensure that adequate ability to retrieve files is in place when using a cloud based storage solution. No files that could reasonably be deemed to be sensitive or confidential, or critical for the normal operations of the business, should be saved to private cloud based storage solutions, and must be saved (and therefore backed up) to the shared drive storage facilities available.

10. PERSONAL USE OF OUR SYSTEMS

10.1 We permit the incidental use of our internet, email and telephone systems to send personal email, browse the internet and make personal telephone calls subject to certain conditions set out below. Personal use is a privilege and not a right. It must not be overused or abused. We may withdraw permission for it at any time or restrict access at our discretion.

10.2 Personal use must meet the following conditions:

(a) Use must be minimal and take place substantially out of normal lesson/working hours (that is, during lunch hours, before 9 am or after 5.30 pm);

(b) personal emails should be labelled "personal" in the subject header;

(c) use must not interfere with learning or business commitments;

(d) use must not commit the College to any marginal costs; and

(e) use must comply with this policy and including the Data Protection Policy and Disciplinary Rules.

Our systems are monitored 24 hours a day, both when used at home and in college. Every device for students and staff has monitoring software installed that mean IT can monitor anything that is done on the device and they also receive alerts from our monitoring software.

You should not do the following activities on college devices as they will be monitored and picked up and could be subject to disciplinary action (unless in a genuine work related reason i.e. exploring a theme and opposite content in lessons), even if at home and outside of work hours:

a. search for illegal or explicit content on the internet

b. use of offensive or foul language

c. undertake bully or harassment of anyone else

d. use of sexually explicit language

e. anything that would be treated as a hate crime

f. anything that does not promote British values and Prevent ethos

g. anything that could be considered concerning under safeguarding

This list is not exhaustive, but gives a guide of behaviours that could bring the college into disrepute.

All cases are investigated thoroughly as part of the disciplinary process before any actions are taken.

10.3 You should be aware that personal use of our systems may be monitored and, where breaches of this policy are found, action may be taken under the disciplinary procedure. We reserve the right to restrict or prevent access to certain telephone numbers or internet sites if we consider personal use to be excessive.

11. MOBILE TELEPHONES

11.1 All phones used by employees, including personal mobiles phones with access to work emails and used for work purposes must have a PIN placed on them to ensure that personal data cannot be easily accessed if a phone is lost or stolen.

11.2 The college will issue mobile phones to staff who have a need for a mobile phone to fulfil their role. The types of staff that are issued with mobile phones are set out in the college’s mobile phone policy and issuing procedures.

11.3 **College mobile phones should not be used abroad under any circumstances without approval from SLT and phones would need to be unblocked.** College mobile phones are only to be used for work purposes. Mobile phone bills are monitored each month and the college will expect the employee to pay for any excessive personal use and can be deducted from an employee's salary.

Excessive personal mobile use can be classified below:

- Large volumes of personal calls, including overseas/international calls
- Excessive numbers of personal texts or high cost texts (competitions or services)
- Excessive data downloads and any increased charges as a result (limited are set on the majority of mobile phones within college)

This list is not exhaustive, but any misuse will be followed up through the college's disciplinary policy.

12. PORTABLE DEVICE SECURITY

12.1 All mobile devices, including laptops, that are issued by the College are password protected and subject to data encryption. The type of data encryption will depend on the age of the PC with older PCs supplied with a USB key.

You must ensure that you;

(i) Follow any instructions from the IT team concerning password security

(ii) Follow any instructions from the IT team concerning encryption. In particular if it is necessary to use a USB key to encrypt your College laptop you must use the key as instructed, disconnect the key from the laptop when not in use, and store it in a safe place separate from the laptop.

(iii) Co-operate promptly with instructions from the IT team to update security settings or software on your device

The IT team will maintain an asset register of portable devices allocated to staff and can advise on the security features and encryption arrangements of your devices. However, it is your responsibility to use the equipment responsibly and seek such advice if necessary.

13. USING THE INTERNET

13.1 Internet access is provided primarily for learning and business purposes. Occasional personal use may be permitted.

13.2 When a website is visited, devices such as cookies, tags or web beacons may be employed to enable the site owner to identify and monitor visitors. If the website is of a kind described in paragraph 14 (Prohibited Use of Our Systems) such a marker could be a source of embarrassment to the visitor and us, especially if inappropriate material has been accessed, downloaded, stored or forwarded from the website. Such actions may also, in certain circumstances, amount to a criminal offence if, for example, the material is pornographic in nature.

13.3 You should not access any web page or download any image, document or other file from the internet which could be regarded as illegal, offensive, in bad taste or immoral. Even web content which is legal in the UK may be in sufficient bad taste to fall within this prohibition. As a general rule, if any person (whether intended to view the page or not) might reasonably be offended by the contents of a page, or if the fact that our software has accessed the page or file might be a source of embarrassment if made public, then viewing it will be a breach of this policy.

14. MONITORING

Our systems enable us to monitor telephone, email, voicemail, internet and other communications. For business reasons, and in order to carry out legal obligations in our role as an employer, use of our systems including thetelephone and computer systems, and any personal use of them, may be continually monitored by automated software or otherwise. Monitoring is only carried out to the extent permitted or as required by law and as necessary and justifiable for business purposes.

14.1 We reserve the right to retrieve the contents of email messages or check internet usage (including pages visited and searches made) as reasonably necessary in the interests of the business, including for the following purposes (this list is not exhaustive):

(a) to monitor whether the use of the email system or the internet is legitimate and in accordance with this policy;

(b) to find lost messages or to retrieve messages lost due to computer failure;

(c) to assist in the investigation of alleged wrongdoing; or

(d) to comply with any legal obligation.

15. PROHIBITED USE OF OUR SYSTEMS

15.1 Misuse or excessive personal use of our telephone or email system or inappropriate internet use will be dealt with under our Disciplinary Procedure.

Misuse of the internet can in some circumstances be a criminal offence. In particular, it will usually amount to gross misconduct to misuse our systems by participating in online gambling, forwarding chain letters, or by creating, viewing, accessing, transmitting or downloading any of the following material (this list is not exhaustive):

(a) pornographic material (that is, writing, pictures, films and video clips of a sexually explicit nature);

(b) offensive, obscene, or criminal material or material which is liable to cause embarrassment to the college;

(c) a false and defamatory statement about any person or organisation;

(d) material which is discriminatory, offensive, derogatory or may reasonably cause embarrassment to others;

(e) confidential information about us or any of our staff or clients (except as authorised in the proper performance of your duties);

(f) any other statement which is likely to create any criminal or civil liability (for you or us); or

(g) music or video files or other material in breach of copyright.

Any such action will be treated very seriously and is likely to result in expulsion/summary dismissal.

15.2 Where evidence of misuse is found we may undertake a more detailed investigation in accordance with our Disciplinary Procedure, involving the examination and disclosure of monitoring records to those nominated to undertake the investigation and any witnesses or managers involved in the Disciplinary Procedure. If necessary such information may be handed to the police in connection with a criminal investigation.

16. PHISHING AND MALWARE

a. The college provides annual cyber security training to all staff, which includes phishing, malware, viruses and all other aspects of cyber security and help for staff to keep themselves and the college safe

b. The college conducts phishing simulations twice per year to test the impact of training and the level of risk within the organisation posed by staff.

c. Persistent offenders of both real and simulated phishing tests, or staff that are often subject to compromised accounts through items like malware and viruses, may be subject to the removal of their devices and subject to disciplinary action. Staff are the biggest cyber threat to the college and staff need to be aware and take precautions seriously.

SOCIAL MEDIA

17. GENERAL

17.1 In this policy when we refer to Social Media it is a reference to the use of all forms of social media, including Instagram, Facebook, LinkedIn, Twitter, Google+, Wikipedia and all other social networking sites, internet postings and blogs. It applies to use of social media for college purposes as well as personal use that may affect our business in any way.

18. COMPLIANCE WITH RELATED POLICIES AND AGREEMENTS

18.1 Social media should never be used in a way that breaches any of our other policies. If an internet post would breach any of our policies in another forum, it will also breach them in an online forum. For example, you are prohibited from using social media to:

(a) breach any of the terms of this Policy;

(b) breach any obligations contained in policies relating to confidentiality;

(c) breach our Disciplinary Policy or procedures;

(d) harass or bully other staff or students in any way**;**

(e) unlawfully discriminate against other staff, students or third parties

(f) breach our Data Protection Policy (for example, never disclose personal information about a colleague online); or

(g) breach any other laws or regulatory requirements.

18.2 Staff and students should never provide references for other individuals on social or professional networking sites, as such references, positive and negative, can be attributed to the organisation and create legal liability for both the author of the reference and the organisation.

18.3 Staff and students who breach any of the above policies will be subject to disciplinary action up to and including termination of employment/learning programme.

19. PERSONAL USE OF SOCIAL MEDIA

Personal use of social media at college is permitted so long as it does not involve unprofessional or inappropriate content, use must be minimal and take place outside of normal college hours, and usage otherwise complies with this policy.

20. PROHIBITED USE

20.1 You must avoid making any social media communications that could damage our business interests or reputation, even indirectly.

20.2 You must not use social media to defame or disparage students, the college, our staff or any third party; to harass, bully or unlawfully discriminate against staff, students or third parties; to make false or misleading statements; or to impersonate colleagues, students or third parties.

20.3 You must not express opinions on the College’s behalf via social media, unless expressly authorised to do so by the Director of Marketing. You may be required to undergo training in order to obtain such authorisation.

20.4 You must not post comments about sensitive college-related topics, such as our performance, or do anything to jeopardise our confidential information and intellectual property. You must not include our logos or other trademarks in any social media posting or in your profile on any social media.

20.5 Staff must not engage with students on social media except through the College’s official social media accounts.

20.6 You must not engage in a professional capacity with our clients, partners or suppliers except through the college’s email or social media accounts.

21. BUSINESS USE OF SOCIAL MEDIA

21.1 If your duties require you to speak on behalf of the organisation in a social media environment, you must still seek approval for such communication from the Director of Marketing, who may require you to undergo training before you do so and impose certain requirements and restrictions with regard to your activities.

21.2 Likewise, if you are contacted for comments about the organisation for publication anywhere, including in any social media outlet, direct the enquiry to the Director of Marketing and do not respond without written approval.

21.3 The use of social media for business purposes is subject to the remainder of this policy.

22. GUIDELINES FOR RESPONSIBLE USE OF SOCIAL MEDIA

22.1 You should make it clear in social media postings, or in your personal profile, that you are speaking on your own behalf. Write in the first person and use a personal e-mail address.

22.2 Be respectful to others when making any statement on social media and be aware that you are personally responsible for all communications which will be published on the internet for anyone to see.

22.3 Staff should ensure that their profile and any content they post are consistent with the professional image they present to clients and colleagues.

22.4 If you are uncertain or concerned about the appropriateness of any statement or posting, refrain from posting it until you have discussed it with your manager/personal tutor.

22.5 If you see social media content that disparages or reflects poorly on the College, you should contact Director of Marketing.

23. MONITORING

23.1 We reserve the right to monitor, intercept and review, without further notice, staff and student activities using our IT resources and communications systems, including but not limited to social media postings and activities, to ensure that our rules are being complied with and for legitimate business purposes and you consent to such monitoring by your use of such resources and systems.

24. RECRUITMENT

We may use internet searches to perform due diligence on candidates in the course of recruitment. Where we do this, we will act in accordance with our data protection and equal opportunities obligations.

25. COMPLIANCE

25.1 You may be required to remove any social media content that we consider to constitute a breach of this policy. Failure to comply with such a request may in itself result in disciplinary action.