Acceptable Use of Technology Policy (Staff and Stakeholders) – Summary of Key Points

The aim of this summary is to help identify the key points within this policy, along with any significant changes to BMAT's approach to the issues it contains.

Please also take time to read the full policy, as this summary does NOT provide a complete picture of the entire policy contents.

Key Changes from Previous Versions of this Policy

Topic or Reference	Change to be noted
Staff should always report attempts to steal their usernames or passwords, or those of their students (phishing)	Staff are encouraged to report any suspected attempt to steal their usernames and passwords (ie phishing). They should also report any attempt to steal usernames and passwords from students. This is usually an attempt made via an email link leading to a legitimate-looking login page. Check the email address of any email containing a link before you click, and never click a link or attachment you are not expecting and/or it looks suspicious.

Important Points to Note about this Policy

Topic or Reference	Points to Note
Section 3 – Remote Working	**Use of USB drives and other removable media is not permitted.** You must only store documents, files, messages and emails within BMAT's systems. This might be BMAT's OneDrive or SharePoint, or the remote access provided via school websites, but not Dropbox, Google Drive, iCloud or other online storage. Speak to the IT Service Team for assistance. **Please ensure you read this section.**
Section 5 – Keeping Your IT Credentials Secure	You are not permitted to share your password with **anyone**, including colleagues and IT staff. You are solely responsible for ensuring it is kept secret and reporting any attempts to steal it, or your students' passwords (phishing). You must not use your BMAT account password for anything else and it must be different to your passwords for any other accounts and systems. **Please ensure you read this section.**
Section 6 – Use of Personal Devices (BYOD)	Use of personal phones and tablets must be logged with the IT team and have full security enabled. Personal laptops and other non-BMAT IT equipment are not permitted on school premises. **Please ensure you read this section.**

ACCEPTABLE USE OF TECHNOLOGY POLICY (Staff and Stakeholders)

Executive owner: CIO

Author: CIO

Date of issue in draft: 06/11/2019

Date of approval: 08/01/2019

Date of next review: 01/06/2023

Document Control

Version	Date issued	Author	Update information
1.0	6/11/2019	R Canning	Initial draft
2.0	02/12/2019	R Canning	Added comments from BMAT DPO, including on use of images & video, password protection and monitoring.
3.0	12/06/20	R Canning	Further clarification inserted on staff use of phones, tablets and laptops.
4.0	23/06/21	R Canning	Update Section 5 (21 & 22), to include reporting of phishing attempts against own and students' accounts. Updated Section 10 to explicitly encourage reporting and expand range of organisations with whom breach information might be shared.

Context

This Acceptable Use of Technology Policy for staff and stakeholders explains the obligations and responsibilities for the use of:

- all Trust devices and IT infrastructure,
- any personally owned devices that carry or store Trust data ("BYOD")
- social media, messaging and file-sharing platforms
- any technology not included above that carries or stores Trust data, including videos and images.

The purpose of this policy is to ensure the safety and well-being of our staff, stakeholders and students, as well as maintain the security and continuous availability of all our data, information, systems and devices.

PLEASE NOTE: failure to follow either this policy, or the instructions of a member of the IT Services team, could result in the complete failure of BMAT's IT systems and the catastrophic loss of data and may result in disciplinary action.

This policy should be read in conjunction with BMAT's other policies, as set out below:

- Safeguarding and Child Protection Policy
- Privacy Notice for Staff, Suppliers and Stakeholders
- Data Protection and Freedom of Information Policy
- Staff Code of Conduct

.

We are committed to the promotion of community cohesion in our Trust, local, national and global levels, comparing our Academy Trust community to its local and national context and implementing all necessary actions in relation to:

- ethnicity,
- religion or belief, and
- socio-economic background.

In accordance with the values of BMAT we pledge:

- to respect the equal human rights of all our pupils;
- to educate them about equality; and
- to respect the equal rights of our staff and other members of the Academy community.

We will assess and analyse our current Academy practices and implement all necessary resulting actions to ensure pupils are not discriminated against because of their:

- Age

- Disability
- Gender Reassignment
- Race
- Religion or belief
- Sex
- Sexual orientation
- Marriage and Civil Partnership
- Pregnancy or maternity

These 'Protected characteristics' have been set out in law in the Equality Act 2010.

BMAT is committed to eliminating practices, which could result in unfair or less favourable treatment for persons with a protected characteristic.

Key definitions used in this policy

TERM	DEFINITION
The Trust	BMAT
BYOD	"Bring Your Own Device". This refers to any personally owned device that is used on the Trust network or that receives or stores Trust data. For example, a personal mobile phone used by a member of staff to receive and send emails for work purposes.
IT Service	All personnel, processes, infrastructure, software and hardware employed, commissioned, in use, planned and/or under consideration for implementation at BMAT.
IT Services Team	The team employed to provide technical and operational support and management for the IT Service.
Personal device	A computer, phone, laptop or other technology hardware owned by individuals (for example, someone's own mobile phone).
Staff	Collective term for all adult employees, contractors and other stakeholders provided with access to the IT Service.
Stakeholders	Any person or organisation not directly employed or on the pupil roll within BMAT, with access to the IT Service.
The Board/Directors/ Trust Board	The Board of Directors of BMAT
Trust device	A computer, phone, laptop or other technology hardware owned by BMAT.
Trust system	Any software application, package or tool, including websites and online services, or other technology provided by BMAT that is not considered hardware.

BMAT School Abbreviations

BMA	Burnt Mill Academy
CS	Cooks Spinney Primary Academy and Nursery
ESJ	Epping St John's
FHS	Forest Hall School
FW	Freshwaters Primary Academy and Nursery
LP	Little Parndon Primary Academy
MC	Magna Carta Primary Academy
MHA	Mark Hall Academy
RDA	Royal Docks Academy
RY	Roydon Primary Academy
SFG	Sir Frederick Gibberd
STEM	BMAT STEM

Each BMAT school is legally defined as an Academy, regardless of whether the term 'school' is used to describe it in the policy.

Contents

1. Scope

1) This policy is intended to provide a safe and secure environment for the use of BMAT's IT Service. It applies to anyone using the IT Service, including students, staff and third-party individuals who have been given access to the service for specific purposes.

2) This policy should be interpreted in the widest application possible. It applies to new and developing technologies that might not be mentioned explicitly or might not yet be in use at BMAT.

3) It is the responsibility of all users of the IT Service to read, understand and comply with this policy and any additional safeguarding and information security policies and procedures.

4) All users of the IT Service must immediately comply with any reasonable written or verbal instructions issued by people with delegated authority in support of this policy, such as the BMAT IT Services team.

2. Acceptable Use

5) Use of the IT Service is permitted only for activities related to the objectives of the Trust and not for personal business or benefit. This applies whether using the IT Service for commercial, political or promotional activities not expressly directed by BMAT is prohibited.

6) When using the IT Service, you must ensure your actions:
   i. do not cause or facilitate harm or distress to others
   ii. do not threaten the continuity, availability, safety or security of the IT Service
   iii. are in accordance with relevant BMAT policies and guidance, in particular the current data protection and safeguarding policies and staff code of conduct
   iv. adhere to the law, in particular the Data Protection Act 2018 and the GDPR.

7) All electronic communication (eg email), online activity, file sharing, storage and other uses of technology that might arise in the course of working at BMAT must only be carried out on systems provided by the IT Service. Use of systems not provided or authorised by the IT Service is strictly prohibited. Some examples of prohibited use are:
   i. personal email for work purposes
   ii. your own computer/laptop for work
   iii. your own mobile phone for storing work files and emails (online email access is acceptable)
   iv. using removable (USB) devices to store and transport files
   v. using Google Drive, Dropbox, Whatsapp or similar online storage and messaging

8) When using the IT Service from another premises, you are subject to both BMAT's policies and those of the premises from where you are accessing the IT Service.

9) You must not deliberately or recklessly consume excessive IT resources such as processing power, bandwidth, storage or consumables, or attempt to disrupt or circumvent IT security measures.

10) You must not use the IT Service to create, download, store or transmit unlawful material, or material that is indecent, offensive, threatening or discriminatory. In the event that there is a genuine academic need to carry out an activity which might breach this condition, you must seek written agreement from your line manager maintain a record of written approval to proceed (e.g. an email).

11) You must adhere to any licence conditions when using software provided by the IT Service.

3. Remote Working

12) When working remotely (eg working at home), you must use the online portal provided by the IT Service in order to access and store your files. Using removable media, such as USB drives and pens, is not permitted.

13) If you are allocated a Trust device, you must always ensure its safety and security, including storing it in a secure location when not in use and ensuring the privacy and security settings are always switched on.

14) You must ensure your home or public wireless connection is secure and private by following the instructions available on your device and given by your internet service provider.

15) You must ensure that people around you cannot easily see your screen and that they cannot gain access to your device. This includes family members.

16) Never lend or allow members of your family or the public to use your Trust device, or any system provided by the IT Service.

17) Do not allow anyone except the IT Services Team to load software, insert disks or USB drives, or browse the internet on your Trust device.

4. Loss, Damage or Theft of a Trust or Personal Device (BYOD)

18) If your Trust device is lost, stolen or damaged, you must immediately report it to your line manager and to the IT Service (See Appendix A for helpdesk reporting procedure). If your own device has been lost or stolen and has been used for work at BMAT, you must report it in the same way.

19) You are required to make all reasonable efforts to retrieve the device, as well as secure or destroy any data belonging to BMAT on the device, including user credentials, emails, files, media and text messages (See “Securing your Personal Credentials”, below).

5. Keeping Your IT Credentials Secure

20) You must always safeguard your username, password and any other IT credentials issued to you. This includes keeping your password confidential from colleagues within the Trust.

21) If you suspect your password is known to someone else, you must change it immediately. Likewise, if you suspect an attempt by anyone to obtain your credentials (eg through a phishing attempt), you should cease responding to that attempt (eg do not enter your details), and report it to IT Services.

22) If you suspect an attempt by anyone to obtain a student credentials (eg through a phishing attempt), you should advise the student to cease responding to that attempt (eg not to enter their details), and report it to IT Services.

23) You must not allow anyone else to use your IT credentials. Nobody has the authority to ask you for your password and you must not disclose it to anyone, including the IT Services Team.

24) Never store a password reminder or prompt alongside your device, or within items that you ordinarily carry in the course of your daily work within BMAT.

25) You must use a range of passwords for different systems and not use your BMAT account password for any other accounts or systems.

26) Password complexity is considered critical to the security of the IT Service. You must follow the instructions and direction of the IT Service Team when asked to change your password.

27) You must not attempt to obtain or use anyone else's credentials. You will be held responsible for all activities undertaken using your IT credentials, including access to online services.

28) You must not impersonate someone else or otherwise disguise your identity when using the IT Service.

6. Use of Personal Devices (BYOD)

29) Personal devices such as phones and tablets should not be used to store BMAT files or data, including emails and attachments, without express permission by the BMAT IT Services Team. Personal laptops and other IT equipment not owned by BMAT are not to be used or brought into school premises.

30) Where permission to use a personal device is granted, you must ensure the device:
    i. has anti-virus protection
    ii. is up to date with all system updates and patches
    iii. is locked at all times when not in use
    iv. has a screen timeout function to lock the device
    v. has remote wiping/deletion enabled (where the device is capable)
    vi. is used in a manner consistent with this policy, in particular the 'Remote Working' section, above.

7. Keeping Information Secure

31) When using the IT Service, you must safeguard BMAT's data and information in accordance with the law, the Staff Code of Conduct and with the data protection and safeguarding policies.

32) You must not attempt to access, delete, modify or disclose information belonging to other people without their permission, or without explicit approval from a member of BMAT's Executive team.

33) You must lock the screen of your device screen when leaving it unattended (eg computer or mobile phone). This includes very short periods, such as leaving your desk to make a drink.

8. Social Media

34) The use of social media presents a significant safeguarding and data protection risk. The following describes the acceptable use of social media platforms such as Facebook and Twitter, but the general approach applies to all interactions through communication and media-sharing features:

    i. Never follow, post to, or send direct messages to a student's account
    ii. Always refuse direct messages and connection requests from students

iii. Never post pictures or videos of pupils and staff without their explicit consent. Always bear in mind that **they will always own their picture or appearance in a video,** so you must think first how you will remove/destroy/delete it if they later ask you to do so.
iv. Always check your posts to ensure you are not in breach of this policy and are not revealing the identity of a child or colleague

35) Should you receive direct messages from students, or have a concern about a pupil's well-being, no matter how trivial you may feel it may be, it is your duty to report this concern in line with BMAT's Safeguarding and Child Protection policy. If you are unsure who to tell, see your immediate line manager for guidance.

36) You are advised to operate two online 'personas'; one for your professional life and one for your personal life. Only use your professional account for posts and connections related to your work in BMAT. Check this regularly to ensure it contains only professionally acceptable and compliant content and communication.

37) Where you could be identified as a BMAT employee or stakeholder, your use of social media, including activity on sites, in web applications and in forums, must adhere to the expectations set out within the BMAT Staff Code of Conduct and the data protection and safeguarding policies.

38) Social media or other online accounts used for supporting and representing official BMAT communication must only be created with authorisation and in the format provided by the BMAT Information Team.

9. Monitoring

39) BMAT records and monitors the use of its IT Service, for the purpose of:

i. supporting, maintaining and improving technology provision
ii. investigation, detection and prevention of infringement of the law, this policy or other BMAT policies (in particular the safeguarding and data protection policies)
iii. investigation of alleged misconduct by staff or students.

40) Monitoring of the IT Service includes all internet browsing and email and messaging systems, so you must not use these systems for personal messages or activities.

41) Should you have any questions regarding monitoring within the IT Service, please direct them to the IT Services Team.

10. Implementation and Enforcement of this Policy

42) You must comply with any reasonable written or verbal instructions issued by people with delegated authority in support of the implementation of this policy.

43) If you believe this policy has been violated, you must report the matter to IT Services, at the earliest opportunity.

44) Where a violation has been identified, any relevant media or material must be removed from hosted applications, websites, or any other shareable storage immediately upon request from personnel with management authority.

45) Everyone makes mistakes and you are encouraged to report breaches and violations, even if you are at fault. This will help us all to stay safe.

46) Where violation of this policy, or related illegal activities, are determined to be deliberate, information may be passed to appropriate law enforcement and government agencies, and to other organisations whose requirements you may have breached.

11. Legal Compliance

47) The user must comply with all relevant legislation and legal precedent, including the provisions of the following specifically related Acts of Parliament, or any re-enactment thereof:

- Malicious Communications Act 1988
- Computer Misuse Act 1990
- Data Protection Act 2018
- General Data Protection Regulation (GDPR)
- Regulation of Investigatory Powers Act 2000
- Investigatory Powers Act 2016
- Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- Communications Act 2003
- Counter-Terrorism and Security Act (2015)

12. Declaration

Please sign below to confirm the following:

BMAT Acceptable Use of Technology Policy (Staff & Stakeholders)

1) I have read, understood and will comply with this policy.

2) I understand that if I do not comply with this policy, or with the instructions of the IT Services team, I threaten the safety and security of all adults and children within BMAT.

3) I will immediately report accidental or deliberate breaches of this policy, by me or by anyone else, to the IT Services team.

Name:

Signature:

Job Title/Role at BMAT:

Date:

Appendix A

Helpdesk Reporting Procedure

BMAT Staff

All staff must send reports and requests for assistance using the ‘Resolve’ link within their email software, or by using the link provided on the desktop view of their BMAT computer.

Third parties with BMAT Accounts

All third parties with BMAT accounts must speak directly to their BMAT contact in order to send reports and requests for assistance to BMAT IT Services.