BDMAT
Birmingham Diocesan
Multi-Academy Trust

BDMAT IT Policy

Issued: April 2018

Reviewed: November 2022

Next Review Date: Autumn 2025

Contents

1. Purpose 3

2. Definitions 3

3. Related Policies and Legislation 4

4. Acceptable Use of IT 5

5. Acceptable Use of IT - Students 6

6. Acceptable Use of IT - Parents 6

7. IT equipment 6

8. Personal devices 7

9. Monitoring 7

10. Data Security 8

11. Cyber Security 9

12. Network and Internet access 9

13. Changes to BDMAT IT systems 10

Appendix 1: Staff acceptable use agreement 11

Appendix 2: Model pupil acceptable use agreement 12

1.0 Purpose

Information technology (IT) is an integral part of the way BDMAT operates, and is a critical resource for pupils, staff, governors, volunteers and visitors. IT supports teaching and learning, pastoral support and the various business and administrative functions of BDMAT and its schools.

The use of IT resources and systems also poses risks to data protection, online safety and safeguarding, which need to be managed.

This policy aims to:

- Set guidelines and rules on the use of school ICT resources for staff, pupils, parents and governors
- Support policies on data protection, online safety and safeguarding
- Prevent disruption that could occur to the school through the misuse, or attempted misuse, of IT systems
- Support the school in teaching pupils safe and effective internet and IT use

This policy covers all users of our school's ICT facilities, including governors, staff, pupils, volunteers, contractors, and visitors.

Breaches of this policy may be dealt with under school behaviour policies, BDMAT staff code of conduct, or BDMAT disciplinary policies.

2.0 Definitions

IT systems: all facilities, systems and services including but not limited to network infrastructure, desktop computers, laptops, tablets, phones, music players or hardware, software, websites, web applications or services, and any device system or service which may become available in the future which is provided as part of the BDMAT IT service.

Users: anyone authorised by the school to use or access BDMAT IT systems, including governors, staff, pupils, volunteers, contractors, and visitors

Personal use: any use or activity not directly related to the user's employment, study or purpose agreed by an authorised user

Authorised personnel: employees authorised by BDMAT to perform systems administration and/or monitoring of the IT systems

Removable storage media: any storage device that is easily connected and disconnected from IT systems, including portable USB storage drives and SD cards.

3.0 Related Policies and Legislation

This policy references or relates to the following other BDMAT policies:

- GDPR policy
- Safeguarding policy – central staff
- Safeguarding policy - schools
- Staff code of conduct

This policy refers to, and complies with, the following legislation and guidance:

- Data Protection Act 2018
- The UK General Data Protection Regulation (UK GDPR) – the EU GDPR was incorporated into UK legislation, with some amendments, by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020
- Computer Misuse Act 1990
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- Education Act 2011
- Freedom of Information Act 2000
- Education and Inspections Act 2006
- Keeping Children Safe in Education 2022
- National Cyber Security Centre (NCSC): Cyber Security for Schools
- Education and Training (Welfare of Children) Act 2021
- Meeting digital and technology standards in schools and colleges

4.0 Acceptable Use of IT – Staff, including governors, directors, visitors, volunteers, and contractors.

4.1 Access to BDMAT IT systems is provided for, and must only be used for, work purposes.

4.2 Staff must only use their own accounts to access BDMAT IT systems. Staff must keep the credentials for such accounts (e.g. passwords) secret.

4.3 Staff must not allow anyone else to use their access to BDMAT IT systems, including when leaving equipment or systems unattended.

4.4 Staff should enable multi-factor authentication on their accounts where systems allow for this. The BDMAT IT team may enforce multi-factor authentication and / or additional security measures as required.

4.5 BDMAT provides each member of staff with an email account. This email account should be used for work purposes only.

4.6 Staff must ensure that their use of BDMAT IT systems is in line with the staff code of conduct. This includes, but is not limited to, section 8: Communication and Social Media, section 9: Acceptable use of technology, and section 10: Use of technology for online/virtual teaching

4.7 Staff may not use BDMAT IT systems, for personal use.

4.8 Staff must follow guidance from the BDMAT IT services team on how to store data and files in the appropriate systems and locations.

4.9 Staff must not connect removable storage media to BDMAT IT systems without explicit approval from the BDMAT IT services team. Such requests will only be granted under exceptional circumstances.

4.10 Where remote access is provided to BDMAT IT systems, staff must abide by the same rules as apply when accessing systems on site.

4.11 Staff must be particularly vigilant if they use the school's ICT facilities outside the school and take such precautions as the BDMAT IT team may require against importing viruses or compromising system security.

4.12 Our ICT facilities contain 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.

5.0 Acceptable Use of IT - Students

5.1 Schools should use the BDMAT template policy for student access to IT systems. The template Acceptable Use Policy is included at Appendix A to this policy.

6.0 Acceptable Use of IT - Parents

6.1 Parents should not have access to the school's ICT facilities as a matter of course. However, parents working for, or with, the school in an official capacity (for instance, as a volunteer or as a member of the PTA) may be granted an appropriate level of access or be permitted to use the school's facilities at the Headteacher's discretion.

6.2 Where parents are granted access in this way, they must abide by this policy, as well as the associated policies listed in section 3, as they apply to staff.

7.0 IT equipment

7.1 All BDMAT IT equipment must be recorded on the BDMAT asset database.

7.2 Staff may be issued with laptops, phones, monitors or other IT equipment to allow them to carry out their role.

7.3 The BDMAT IT team will manage the assignment of devices to staff. Where appropriate, the BDMAT IT team may delegate this responsibility to schools.

7.4 Staff must sign a loan agreement for all equipment that they are issued.

7.5 Staff must take reasonable care of loan equipment, taking good care of the physical condition of the equipment. Staff may be required to pay for repairs where there is evidence they have been negligent in their use and care of issued equipment.

7.6 Staff must ensure that all loan equipment is stored securely when not in use, including when taking devices away from BDMAT premises.

7.7 Staff must not remove IT equipment from its assigned location without permission from the BDMAT IT team. The BDMAT IT team may delegate this authority to schools.

7.8 Fixed IT equipment (e.g. desktop computers, printers, photocopiers, servers, networking equipment) may not be moved, altered, or otherwise changed without approval from the BDMAT IT team in accordance with the Change Enablement process.

7.9 All networking, server, storage, or other infrastructure equipment must be stored in a secure location, only accessible to the BDMAT IT team and delegated keyholders.

8.0 Personal devices

8.1 Staff are permitted at their discretion, to access BDMAT IT systems and services from personal devices. When using personal devices on BDMAT IT systems, staff must ensure that such usage is in line with this section.

8.2 All personal devices used to access BDMAT IT systems must be up to date with the latest security patches, up-to-date anti-virus, running a currently supported operating system, and protected by strong encryption and passwords.

8.3 The BDMAT IT services team may implement policies to enforce compliance with security requirements for personal devices and prevent access from devices that do not pass these checks.

8.4 BDMAT may require staff to grant limited access to manage personal devices when using them to access BDMAT IT systems.

8.5 BDMAT may suspend or remove access to BDMAT systems from personal devices at any time.

8.6 BDMAT reserves the right to automatically remove work data from personal devices at the end of a member of staff's employment.

8.7 BDMAT reserves the right to remove work data from personal devices in order to prevent, mitigate or otherwise address a data breach, cyber security risk, or policy breach.

8.8 For the purposes of intellectual property any data held on personal devices is the property of BDMAT.

8.9 For the purposes of GDPR BDMAT is the data controller for any BDMAT data held on personal devices. BDMAT data is any that relates to the individual's work as an employee of BDMAT. This data is disclosable under Freedom of Information and Subject Access Requests.

9.0 Monitoring

9.1 To safeguard and promote the welfare of children and provide them with a safe environment to learn, BDMAT reserves the right to filter and monitor the use of its ICT systems, services, and equipment.

9.2 Monitoring includes, but is not limited to, the filtering and monitoring of Internet activity, bandwidth usage, user activity, access and audit logs, telemetry data and any other electronic communications.

9.3 Only authorised IT or safeguarding personnel may filter, inspect, monitor, intercept, assess, record, and disclose the above, to the extent permitted by law.

9.4 The effectiveness of any filtering and monitoring will be regularly reviewed by the Deputy CEO and Head of IT.

9.5 Where appropriate, authorised personnel may raise concerns about monitored activity with the school's Designated Safeguarding Lead (DSL) and the BDMAT IT team or through BDMAT's Whistleblowing Policy.

10.0 Data Security

10.1 Schools are responsible for making sure appropriate levels of security protection and procedures are in place to safeguard its systems, staff and pupils.

10.2 Schools must take steps to protect the security of all computing resources, data and user accounts. The effectiveness of these procedures will be reviewed periodically by the Deputy CEO and Head of IT to ensure security is sufficient to protect the school from evolving cyber-crime technologies.

10.3 Staff, pupils, parents and other who use the BDMAT IT facilities should use safe computing practices at all times.

10.4 BDMAT aims to meet the cyber security standards recommended by the DfE's guidance on digital and technology standards in schools and colleges

10.5 All users of BDMAT IT systems should set strong passwords for their accounts and keep these passwords secure. Users may view the current requirements on passwords on the BDMAT IT Services Help Centre

10.6 Users are responsible for the security of their passwords and accounts, and for setting permissions for accounts and files they control.

10.7 Members of staff or pupils who disclose account or password information may be subject to disciplinary action. Parents, visitors, or volunteers who disclose account or password information may have their access rights revoked.

10.8 If users suspect that their password has been shared or discovered, they must change it immediately. If users suspect that their account may have been accessed by anyone else, they must change their password immediately and then contact the BDMAT IT team.

10.9 The BDMAT IT team ensures that all BDMAT devices and systems are protected by an appropriate level of encryption.

10.10 School staff may only use personal devices (including computers and USB drives) to access school data, work remotely, or take personal data (such as pupil information) out of school if they have been specifically authorised to do so by the headteacher.

10.11 Use of such personal devices will only be authorised if the devices have appropriate levels of security and encryption.

11.0 Cyber Security

11.1 BDMAT understands the importance of cyber security and will ensure cyber security is given the time and resource needed to keep the trust and its schools secure.

11.2 BDMAT will endeavour to meet the Cyber Security Standards as published by the DfE.

11.3 BDMAT will provide annual training for staff on the basics of cyber security.

11.4 BDMAT and its schools will make sure staff are aware of the correct procedures for reporting and responding to cyber security incidents.

11.5 BDMAT will keep backups of key systems and data according to an appropriate schedule based on risk.

11.6 The BDMAT IT services team will manage and monitor the backup systems, report and address faults, and keep records of such checks and remediation actions.

11.7 BDMAT will develop, review, and test a Cyber Security Incident Response Plan. This plan will be activated in the event of a cyber security incident and will be updated as needed following incident reviews.

11.8 BDMAT will take steps to check the security of supplier IT systems when procuring or renewing systems, goods, or services.

12.0 Network and Internet access

BDMAT provides network and internet access for staff, students, visitors, and others as required for their role. Such access is provided and to be used in accordance with the following:

12.1 BDMAT Internet connections must be secured by a suitable firewall and filtering solution.

12.2 Changes to filtering must be logged, approved, and implemented in line with the BDMAT Change Enablement Process.

12.3 Changes to filtering must be approved by the Head of IT. The Head of IT may delegate this authority as required.

12.4 Staff must report any sites they believe are inappropriate that have not been correctly identified and blocked by the filtering systems to the BDMAT IT services team via the helpdesk.

12.5 Staff should report any sites they believe have been incorrectly blocked by the filtering systems to the BDMAT IT services team via the helpdesk.

12.6 Any attempts to bypass BDMAT firewalls or web filtering may result in disciplinary action.

13.0 Changes to BDMAT IT systems

13.1 Any changes to BDMAT IT systems must be managed and approved through the BDMAT Change Enablement process.

13.2 All changes must be approved by the Change Advisory Board (CAB) prior to implementation.

13.3 A guide to the Change Enablement Process is published on the BDMAT IT services help centre for all staff to access.

13.4 Any unauthorised changes to BDMAT IT systems may result in disciplinary action.

Appendix 1: Staff acceptable use agreement

Name:	

I have read and understood the full BDMAT IT Security and Acceptable Use Policy and agree to uphold the spirit and the letter of the approaches outlined there.

I will ensure that my use of IT systems is conducted in line with this policy, and I will take all reasonable steps to ensure the security and safety of the IT systems I have access to, and any equipment that is loaned to me.

I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the BDMAT GDPR policy.

I understand that BDMAT may monitor the websites I visit, and my use of IT systems.

I will only use my own accounts to access BDMAT IT systems. I will set secure passwords and I will not share my passwords with anyone else.

I will always use the school's ICT systems and internet responsibly and ensure that pupils in my care do so too.

Signed:	**Date:**

Appendix 2: Model pupil acceptable use agreement

Name of pupil:	
When I use the school's IT systems (like computers and equipment) and go on the internet in school, I will not: • Use them without asking a teacher first, or without a teacher in the room with me • Use them to break school rules • Go on any inappropriate websites • Go on Facebook or other social networking sites (unless my teacher said I could as part of a lesson) • Use chat rooms • Open any attachments in emails, or click any links in emails, without checking with a teacher first • Use mean or rude language when talking to other people online or in emails • Send any photos, videos or livestreams of people (including me) who aren't wearing all of their clothes • Share my password with others or log in using someone else's name or password • Bully other people I understand that the school will check the websites I visit and how I use the school's computers and equipment. This is so that they can help keep me safe and make sure I'm following the rules. I will tell a teacher or a member of staff I know immediately if I find anything on a school computer or online that upsets me, or that I know is mean or wrong. I will always be responsible when I use the school's ICT systems and internet. I understand that the school can discipline me if I do certain unacceptable things online, even if I'm not in school when I do them.	
Signed (pupil):	**Date:**
Parent/carer agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.	
Signed (parent/carer):	**Date:**