DIOCESE OF SOUTHWELL
& NOTTINGHAM
MULTI ACADEMY TRUST

SNMAT

Bring Your Own Device (BYOD) Policy

Policy:	Bring Your Own Device (BYOD) Policy
Approved by:	Board of Directors
Date:	July 2024
Review Cycle:	Annual

Versions:			
VERSION	**DATE**	**AUTHOR**	**CHANGES**
2020	March 2020	DO – IT Director	Initial version.
2021	April 2021	DO – IT Director	No changes.
2022	May 2022	SKP & MY	Changed IT Director to Trust Technical Lead. Cyber Security Policy added to Links to other Policies.
2023	June 2023	MJH – IT Coordinator	Redesigned Document and complete rewrite to be relevant to modern Bring Your Own Device scenarios in SNMAT. Added DSL to responsibilities. Updated the role of the Trust IT Team. Consolidated Appendix 1 into a Bring Your Own Device Acceptable Use Policy that covers staff, students and visitors.
2024	May 2024	MJH – IT Manager	Introduced responsibilities for SLT Digital Leads from their introduction as part of DfE Meeting Digital and Technology Standards in Schools and Colleges (2024). Added further risks from allowing BYOD devices, including the introduction of malware and ransomware, and the risk of unauthorised access to systems and data. Added requirement for personal devices to be clear of malware, virus and ransomware infections. Added responsibility for Heads/Principals to evaluate the need for a more detailed student BYOD policy.

EXECUTIVE SUMMARY

1. Bring Your Own Device (BYOD) is where a member of staff, a student, or a guest uses a personal device to connect to the Diocese of Southwell and Nottingham Multi-Academy Trust (SNMAT) network, or SNMAT resources or services.

SCOPE

2. This policy applies to all members of the Trust/academy community (including staff, pupils/students, volunteers, parents / carers, visitors, community users) who use a personal device to connect to the SNMAT BYOD network, or SNMAT resources or services.
3. This policy applies to all non-school owned devices that are used to access the internet via an SNMAT BYOD network or to access school information and services.
4. Devices include PCs, laptops, tablets, smart phones, smart watches, smart devices, or any other device with the ability to connect to Wi-Fi and the internet and SNMAT services.

RATIONALE

5. The internet and other technologies play a key role in 21st century life and the aim of this policy is to maximise data security and safeguarding whilst promoting the effective use of such technologies to enhance teaching and learning, support workflows and give members of the SNMAT community access to resources or services.

6. This policy can be used as an addendum to the SNMAT Overarching eSafeguarding Policy where Headteachers or Principals recognise the benefits to learning from offering students the opportunity to use personal devices in school to support educational activities whilst promoting safe and appropriate practice through establishing clear and robust acceptable mobile user guidelines.

OBJECTIVES

7. Allowing external devices to connect to networks comes with risk. This policy sets guidelines to mitigate risk as far as technically possible and attempts to ensure SNMAT IT infrastructure and devices are secure, compliant, and not open to misuse or malicious attacks.

8. This policy supports our Data Protection Policy and provides guidance on how to minimise risks associated with the use of non-school owned electronic mobile devices, in line with the General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018).

ROLES AND RESPONSIBILITIES

Board of Directors

9. The Board of Directors is accountable for the effective operation of the BYOD policy overall.

Data Controller

10. The Diocese of Southwell and Nottingham Multi-Academy Trust is the corporate body registered with the Information Commissioner's Office as Data Controller. The Directors are ultimately accountable for the implementation of GDPR and must be able to demonstrate they have secured, controlled, or deleted access to personal data on the SNMAT network, and any personal data on a particular device in the event of a security breach.

Local Governing Bodies

11. Each of the academies within SNMAT is named on the data protection register. The Board of Directors has delegated the responsibility to Local Governing Bodies and specifically the named Data Protection Governor to ensure that all personal data on a particular device has been secured, controlled or deleted in the event of a security breach.

Principal / Headteacher

12. The responsibility for the day-to-day operation of the BYOD policy has been delegated to the Principal/Headteacher and DSL. The Principal/Headteacher and DSL is responsible for:

    - Authorising the availability of BYOD where appropriate
    - Ensuring that all the staff have read and understand the BYOD policy.
    - Ensuring that members of the school community adhere to the BYOD policy.
    - Ensure that any visitor adheres to the BYOD policy.
    - Ensuring that staff or students using their own device understand that failure to follow the policy may result in disciplinary action.
    - Ensuring that BYOD network/service users are informed that the academy may monitor their usage to ensure the security of personal data.
    - Evaluating whether students require a separate BYOD policy outlining further stiuplations.

SLT Digital Lead and The Designated Safeguarding Lead

13. SNMAT standards promote a secure internet environment to help protect and monitor what children can access online. However, all technical solutions are not 100% guaranteed, so Digital and Safeguarding Leads should evaluate and discuss with the Principal/Headteacher the potential eSafeguarding risks from allowing users, and specifically students to access BYOD and use their own devices in school:

    - Attempts to circumnavigate school internet filtering;
    - Attempts to access school systems and data;
    - Introducing threats to systems, including viruses, malware or ransomware;
    - Sharing of personal data;
    - Access to illegal or inappropriate materials;
    - Inappropriate on-line contact with adults/strangers;
    - Potential or actual incidents of grooming;
    - Cyber-bullying.

Trust IT Support Team

The Trust IT Support Team will:

14. Ensure that the SNMAT BYOD infrastructure is configured to be as secure as possible, and Wi-Fi provision is sufficient and capable of effectively managing large numbers of connections.
15. Ensure that BYOD networks, technical policies and filtering adheres to SNMAT Cyber Security, GDPR and eSafeguarding policies.
16. Ensure that devices that connect to SNMAT resources where possible are forced to be secured with a PIN, geometric pattern, or biometric authentication.
17. Respond, or provide guidance to allow local school IT Support teams to respond quickly to a report of a security breach – for example a lost or misplaced device and use available

remote wipe, device blocking and password reset mechanisms to mitigate any potential data loss.

INTERNET FILTERING STANDARDS

18. All BYOD connections for visitors or unauthenticated users will have the default pupil filtering applied.
19. For authenticated users, pupil eSafeguarding filtering will be applied.

BRING YOUR OWN DEVICE – ACCEPTABLE USE POLICY

You must adhere to the SNMAT Data Protection and Privacy policies, eSafeguarding Policy, ICT, Social Media and the following Bring Your Own Device Acceptable Use Policy (BYOD-AUP) when using your own personal device to connect to SNMAT BYOD networks or services via the internet.

All Users:

1. Must act responsibly, safely and respectfully in line with GDPR and eSafeguarding Policies.
2. Should be aware that the MAT and its schools have the right to take, examine and search any device that is suspected of unauthorised use, either technical or inappropriate.
3. Must mitigate data loss or misuse, and should secure their device with a PIN, geometric pattern or biometric authentication lock.
4. Bring their devices into school at their own risk. SNMAT does not take responsibility for devices that are misplaced, lost, stolen or damaged.
5. Are responsible for the maintenance, support, troubleshooting and upkeep of personal devices. SNMAT will not provide technical support for personal devices.
6. Must keep their devices with them at all times. If secure facilities are provided, then phones should be locked and stored when not in use.
7. Should ensure that their personal devices are up-to-date and are running the latest version of operating systems with the latest security updates applied.
8. Should ensure that their personal devices have up-to-date anti-virus and anti-malware software and are scanned and clear.
9. Are responsible for charging of personal devices prior to bringing them into school. If USB charging outlets are provided then they can be used. You must not connect personal devices or chargers to power outlets or connect them via cable to school computers.
10. Once connected to the SNMAT network must not share or lend their devices to another person.
11. Should not use their device to record audio or take photographs or video of any member of the school community without prior permission from the Headteacher/Principal. Where permitted the data should be stored in line with GDPR and eSafeguarding laws and policies.
12. Must not access any inappropriate material that breaches the SNMAT GDPR or eSafeguarding Policies that may or may not have already been downloaded or accessed on the device.
13. Are prohibited to use Virtual Private Networks (VPNs) when connected to the SNMAT BYOD network.
14. Must be aware that access to SNMAT BYOD networks is a privilege, not a right, and can be withdrawn at any time.

Students:

You are expected to be a responsible user of IT. Illegal and inappropriate use of services will not be tolerated. You may face disciplinary action if you engage in any such activities. These include, without limitation; cyber-bulling; attempting to hack the security of, access or tamper with any parts of the Wi-Fi service; attempting to circumvent the internet filtering service – this includes setting up proxies or using programs to bypass firewall securities; calling, texting, emailing, or communication

with any others from a personal device, including other students, parents, guardians, friend and family during school time; or taking, recording or distributing pictures, video or any other material relating to students, staff or areas of the school.

15. During directed learning where devices are allowed, connections to the internet must be via BYOD Wi-Fi only. Unfiltered personal data connections must not be used.
16. Where directed to by staff, a personal device may be used in lesson to support educational objectives. This could be note taking, or for broader learning during directed study. Using a device for any other reason other than directed, for example games, is not allowed.
17. Where directed to by staff, you may use a device to take photos, record video or other material relating to educational activities. You must install the Microsoft OneDrive app and use your school provided Office 365 account to store this material on your device. Media must not be saved outside of OneDrive on personal device camera-rolls or internal storage.
18. Must not use their device to record audio, or take photographs or video of other students or staff.
19. If a device is hidden (e.g. under a table, or shielded from an approaching member of staff) staff will assume inappropriate use and confiscate the device.

Parents:

20. Should ensure that pupil devices are fully insured to cover loss and damage outside of the home.
21. Should ensure that pupil devices have a location finder application installed and activated to aid tracking in the case of loss.
22. Should apply parental controls on pupil devices, check for VPNs and ensure any material accessed in or out of school is appropriate.

LINKING WITH OTHER POLICIES

23. The Bring Your Own Device (BYOD) Policy must be read in conjunction with the other following policies:

- GDPR Policy
- ICT Policy
- Cyber Security Policy
- Data Protection Policy
- eSafeguarding Policy
- Social Media Policy

REVIEW

24. The application and outcomes of this policy will be monitored to ensure it is working effectively.

25. This policy is reviewed annually by SNMAT in consultation with recognised trade unions.