DIOCESE OF SOUTHWELL
& NOTTINGHAM
MULTI ACADEMY TRUST

SNMAT

Bring Your Own Device (BYOD) Policy

A template for SNMAT schools

Policy:	Bring Your Own Device (BYOD) Policy – Template
Approved by:	SNMAT Board of Directors
Date:	April 2025
Review Cycle:	Annual

Versions:			
VERSION	**DATE**	**AUTHOR**	**CHANGES**
2023	Sept 2023	MJH – IT Manager	Initial version.
2024	April 2024	MJH	Updates for pritning. Clarity on personal device support.
2025	April 2025	MJH	References to KCSIE updated to 2024.

Executive Summary

This Bring Your Own Device Policy (BYOD) Template forms part of an overall digital security strategy that the Diocese of Southwell and Nottingham Multi-Academy Trust (SNMAT) use to maximise the safety of our students and pupils as they use the internet, whilst at the same time retaining the flexibility needed for effective teaching and learning.

This template should be customised by Academies that allow students to connect to their BYOD Wi-Fi networks, and the internet.

Template Usage

Throughout this document, notes and suggestions will be made that individual academies within the SNMAT community can use to review and adjust the policy to fit their own requirements.

Keeping Children Safe in Education 2024

The Department for Education's (DfE) Keeping Children Safe in Education 2024 (KCSIE) guidance stipulates that schools should have a clear policy for students and pupils on filtering and monitoring the internet and the use of mobile and smart technology in schools.

Bring Your Own Device Privilege

The Bring Your Own Device (BYOD) privilege prepares students for their future, a world of digital technology and information. As we enter the twenty-first century, excellence in education requires that technology is seamlessly integrated throughout the educational program. Increasing access to technology is essential for that future, and the learning tool of these twenty-first century students is increasing digital devices. The responsible use of suitable digital devices is a way to empower students to learn at their full potential and to prepare them for the real world of university and the workplace.

Access to suitable devices encourages students to solve problems and think critically by stimulating analytical thinking. Learning results from the continuous dynamic interaction among students, educators, parents and the extended community. Technology immersion does not diminish the vital role of the teacher. To the contrary, it transforms the teacher from a director of learning to a facilitator of learning. Learning with Laptops integrates technology into the curriculum anytime, anyplace.

The policies, procedures and information within this document apply to all student BYOD use, including any other device considered by the school, to come under this policy. Teachers may set additional requirements for device use in their classroom.

TEMPLATE NOTE: Consider whether access to the BYOD network will be limited by Key Stage.

Wi-Fi Provision

Whilst we recognise that using personal devices can enhance directed learning, we also recognise the need to protect students from offensive and dangerous material and acknowledge the need to ensure all users make responsible use of the internet.

Internet access will be granted via a voucher system and limited and filtered in compliance with Government guidelines and the school's eSafeguarding Policy.

Access to the school provided BYOD network is a privilege, not a right and can be withdrawn at any time.

TEMPLATE NOTE: Not all Wi-Fi systems support a voucher system. Discuss your requirements with your local MAT IT Team and evaluate the best method of authentication for students. Remember that one-time

vouchers described here give a non-transferable method of connectivity, whilst username/password authentications can be passed onto other individuals.

Internet Access and Filtering

All BYOD internet access is filtered and monitored to fulfil the DfE's statutory requirements for schools and colleges found in KCSIE 2024 guidance and part of PREVENT duties.

More detailed information on internet access can be found in the eSafeguarding Policy.

Suitable Devices

Suitable devices for BYOD that support learning are lightweight laptops, Chromebooks or adequately sized tablets. Vouchers or connections to wireless networking will not be granted to connect mobile phones.

Acceptable Use Policy

If students wish to connect devices to the school provided BYOD network, then they must agree to be bound by the additional rules set out in the BYOD Acceptable Use Policy (AUP).

TEMPLATE NOTES: Consider that both parents/carers and students must agree to the BYOD AUP before any voucher code is provided.

Classroom Usage

When explicitly permitted by a member of staff a personal device may be used in lesson to support the lesson objectives. This could be note taking, or for broader learning during independent study.

Using a device for any other reason other than directed, for example app usage, web browsing or games, is not allowed. If a device is hidden (e.g., under a table, or shielded from an approaching teacher) staff will assume inappropriate use and confiscate the device.

TEMPLATE NOTE: Not all academies will deem classroom usage appropriate.

Independent Study

Sixth Form students can use their own devices to support educational activities in nominated private study rooms; supervised study lessons or the sixth form common room and in lessons as designated by the teacher.

TEMPLATE NOTE: Not all Wi-Fi systems support a voucher system. Discuss your requirements with your local MAT IT Team and evaluate the best method of authentication for students. Remember that one-time vouchers described here give a non-transferable method of connectivity, whilst username/password authentications can be passed onto other individuals.

Access To Documents

Students will not have access to documents that reside on the school network. All documents must be accessed via internet-based Google, Office365 and Microsoft 365 services.

Access To Printing

Students will not have access to printing via BYOD.

Device Security and Management

It is not the school's responsibility to provide or support personal devices. Any request for technical support for a personal device within an Academy will be declined.

The purchase, maintenance, safety, insurance, and security of personal devices must be borne by parents/students/carers.

All personally owned devices brought to school are responsibility of the device owner. The Academy accepts no responsibility for the loss, theft or damage of personally owned devices.

There are no secure facilities provided at school to store personal devices. Students should therefore always keep their personal devices with them.

Misuse

Illegal and inappropriate use of IT services will not be tolerated. Students may face disciplinary action if they engage in such activities, including Cyber-Bullying and bypassing internet filtering, or the use of electronic communications in any format to harass, abuse or radicalise others.

If there is a reason to believe that a student has violated school policy or engaged in misconduct whilst using their device, then evidence will be obtained and removed from that device.

Access to the school provided BYOD network is a privilege, not a right and can be withdrawn at any time.

TEMPLATE NOTE: Ensure staff are familiar with their eSafeguarding responsibilities, are trained with any available classroom management tools and follow DfE and SNMAT guidance on investigating and removing evidence from devices.

Charging

Students are responsible for charging their personal devices prior to bringing them into school.

Personal devices cannot be connected to school power outlets.

TEMPLATE NOTE: Allowing students to plug in non-PAT tested devices into power outlets is not recommended. Students must not connect devices via cable to PCs or network sockets. Academies may choose to provide suitable charging for students, either with USB ports alongside regular outlets, or isolated power sockets that are made available.

Relevant Policies

To underpin the values and ethos of our Academy and our intent to ensure that all students are appropriately safeguarded the following policies are also included under our safeguarding umbrella:

eSafeguarding

TEMPLATE NOTE: Add links to other policies here; Anti-Bullying, Behaviour, etc.

Student BYOD Acceptable Use Policy

Students must check their personal devices daily to ensure that they are free from unsuitable materials, viruses and be kept up-to-date with any security before bringing them into school.

Students must use headphones to listen to audio, such as music or video when using their devices. The volume should be kept at a level that does not disturb or disrupt others.

You may not use devices connected to the BYOD network for any improper activities. These include, without limitation:

No attempting to hack the security of, access, or tamper with parts of the Wi-Fi service.

No attempting to circumvent the Wi-Fi service filtering – this includes the use of VPNS, proxies or other programs to bypass safeguarding and security.

Students must not communicate with others using a device connected to BYOD, including other students, parents, guardians, friends or family during school time.

Students must not use personal devices to take, record, or distribute pictures, video or any other material relating to staff, students or areas of the school.

During directed learning and when devices are allowed, connections to the internet must be via the school provided BYOD network. Unfiltered personal data connections must not be used.

Where directed by staff, you may use a device to take pictures, or record video or other material relating to educational activities. You must install the OneDrive app on your device and use your school provided Office365 account to store this material on your device. Media must not be saved outside the OneDrive mechanism on personal device storage or camera-rolls.

TEMPLATE NOTE: Consider whether students are allowed to do this and provide adequate guidance and education if required. The OneDrive mobile app has a built-in “add photo or video” option.

You are not permitted to use personal devices for storage or any images, video or sound clips of fellow students or staff.

There are no secure facilities provided at school to store personal devices. You should therefore always keep your device with you at all times.

You bring your device with you at your own risk. It is your duty to act responsibly with regard to that device. The Academy is not responsible for personal devices that are broken, lost or stolen whilst at school; any data that is lost on personal devices whilst in school; or maintenance, technical support, troubleshooting or upkeep of any personal device whilst in school.

You must ensure that your device has a suitable protective case or carry bag and has adequate insurance in place to cover the cost of replacement or repair in the event of loss or damage.

To mitigate data loss or misuse, where possible your device must have a PIN, biometric or other suitable device lock and be backed up regularly. Tracking apps should be installed and activated.

You must take all reasonable steps to prevent the transmission and receipt of malicious software such as viruses or malware. Any device that does not have up-to-date anti-virus and anti-ransomware software must not be used.

You are responsible for charging personal devices prior to bringing them into school. If USB or other charging is provided, then they can be used. You must not connect any personal devices and chargers to school power outlets or connect them via cable to school computers or school network sockets.