Bring Your Own Device Policy (BYOD)

Document control		POLICY LEVEL: Trust	
Approved by	Full Trustees	Approved Date	14 September 2023
Portfolio	Trust level	Next Review	September 2024
Published Location	Website and Staff Intranet		
Version Number	Date issued	Author	Update information
1.0	6 September 2022	M Greener	First Published Version - new version issued
1.1	****	M Greener	Updates included as per DPO policy template – mobile devices renamed to personal devices. Guest devices pertains to visitors

This document will be reviewed annually and sooner when significant changes are made to the law.

Guidance from the Department for Education about school policies can be found here: https://www.gov.uk/government/publications/statutory-policies-for-schools-and-academy-trusts/statutory-policies-for-schools-and-academy-trusts

Contents

Bring Your Own Device Policy (BYOD)

1. Introduction

- We recognise that mobile technology offers valuable benefits to staff and students from a teaching and learning perspective and to visitors. Our Trust embraces this technology but requires that it is used in an acceptable and responsible way. Schools should not compel school staff to use their own personal devices to access school systems, but if staff choose to use their own devices, this policy should be adhered to.
- Guest devices (any device which is not school owned or on the school asset list) should only be connected to a secure segregated network for access.
- This policy is designed to support the use of guest devices (any device which is not school owned or on the school's asset list) in schools in a way that extends and enhances teaching and learning. It also aims to protect children from harm, minimise risk to the school networks and explain what constitutes acceptable use and misuse of the BYOD policy.
- This policy supports our Data Protection Policy and provides guidance on how to minimise risks associated with the use of guest devices, in line with the General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018).
- The Trust reserves the right to refuse staff and visitors permission to use their personal devices on school premises.
- This applies to all guest devices connecting to school systems.

2. Scope and Responsibilities

This policy applies to all use of guest devices to access the internet via the schools' guest network or to access school information, by staff, pupils or visitors. This is known as "Bring Your Own Device", or "BYOD". Guest devices include laptops, tablets, smart phones, USB sticks, wearable technology (including smart / apple watches) and any other device considered portable and/or with the ability to connect to Wi-Fi and the Internet which is not school owned or on the school asset list, including staff personal devices.

All staff are responsible for reading, understanding and complying with this policy if they are using their personal devices connected to the school Internet, or using personal devices to access information held on school systems.

If you have any concerns surrounding the use of personal devices, please contact our Principal or Designated Safeguarding Lead.

Users should be aware of the need to;

- Protect children from harm
- Understand what constitutes misuse
- Minimise risk from BYOD
- Report suspected misuse immediately
- Be responsible for their own professional behaviour
- Respect professional boundaries

3. Use of mobile devices within schools

Permission must be sought before connecting personal devices to a school's network. The Trust reserves the right to refuse staff, pupils and visitors permission to use their personal devices on school premises.

Staff, pupils and visitors are responsible for their personal devices at all times. The Trust/school is not responsible for the loss, or theft of, or damage to the personal device or storage media on that device (e.g. removable memory card) howsoever caused, including lost or corrupted data.

The Trust/school must be notified as soon as possible of any loss, or theft of a personal device that has been used to access school systems, and these incidents will be logged with the DPO.

Data protection incidents should be reported immediately to the school's Data Protection Officer (dpo@dmatschools,org.uk).

Personal devices used to access school systems must enable automatic updates for security patches from the supplier. Applications installed on the device must also be subject to regular security updates, be supported by the supplier and licensed.

The Trust cannot support users' personal devices, nor has the school a responsibility for conducting annual PAT testing of personal devices.

Permission must be sought before connecting personal devices to a school's wireless or Ethernet connections. The Trust reserves the right to refuse staff, pupils and visitors permission to use their own mobile devices on school premises.

Where the school uses Multi Factor Authentication, personal mobile phones can be used to receive the necessary authentication code.

4. Access to the Trust's internet connections

The Trust provides a guest wireless network connection that staff, pupils and visitors may, with permission, use to connect their personal devices to the Internet. Access to the network is at the discretion of the school, and the school may withdraw access from anyone it considers is using the network inappropriately.

The Trust/school cannot guarantee that the wireless network is secure, and staff, pupils and visitors use it at their own risk. In particular, staff, pupils and visitors are advised not to use the wireless network for online financial transactions.

The Trust does not permit the downloading of apps or other software whilst connected to the school network and the school is not to be held responsible for the content of any downloads onto the user's own device whilst using the school's network.

It is not permissible for any user to bypass proxy server settings unless written permission from the principal is sought and the purpose is documented. Users of mobile devices must not circumvent on site filtering through the use of 4G/5G services.

The Trust/school will have no liability whatsoever for any loss of data or damage to the owner's device resulting from use of the school's network.

5. Access to the Trust IT systems

Where staff are permitted to connect to school IT systems from their personal devices, a second layer of security should be enabled such as password and/or encryption must be in place and notifications must be turned off the lock screen. It is the responsibility of the owner of that device to ensure it is safe for the purposes for which they wish to use it.

Staff must **not** store personal data about pupils or others on any personal devices, or on cloud servers linked to their personal accounts or devices.

With permission, it may be necessary for staff to download school information to their personal devices in order to view it (for example, to view an email attachment). Email attachments are the most common source of cyber-attacks. Please follow staff guidance on cyber security and email protection and be aware that personal devices are not subject to the same security controls and safeguards that protect the school network and devices.

Any unauthorised access to, or distribution of, confidential information should be reported to the Principal and Data Protection Officer as soon as possible in line with the school's data protection policies. This includes theft or loss of a personal device which has been used to connect to school information systems or which may contain personal information.

Before selling or giving your personal device (which has been used to access a school's network including cloud based systems) to someone else, including a family member or spouse, it must be cleansed of all school related data, emails, systems and apps.

Staff must not send school information or personal data to/from their personal email accounts or social media or similar accounts.

Users must follow the procedures for connecting to school systems.

6. Monitoring the use of mobile devices

The Trust/school reserves the right to use technology that detects and monitors the use of personal devices which are connected to or logged on to our wireless network or IT systems. The use of such technology is for the purpose of ensuring the security of its IT systems and school information.

The information that the school may monitor includes (but is not limited to) the addresses of websites visited, the timing and duration of visits to websites, information entered into online forms, information uploaded to or downloaded from websites and school IT systems, the content of emails sent via the network, and peer-to-peer traffic transmitted via the network.

Any inappropriate content received through school IT services or the school internet connection should be reported this to the Digital Helpdesk and advise a Designated Safeguarding Lead as soon as possible.

7. Security of staff personal devices

Staff must take all sensible measures to prevent unauthorised access to their personal devices, including but not limited to the use of a PIN, pattern, face recognition or password to unlock the device, and ensuring that the device auto-locks if inactive for a short period of time. Staff must ensure that appropriate security software is installed on their mobile devices and must keep the

software and security settings up to date.

Staff must never attempt to bypass any security controls in school systems or their own devices.

The school's Acceptable Use – Staff Policy set out in further detail the measures to ensure responsible behaviour online.

8. Permissible and non-permissible use

Staff and visitors participating in BYOD must comply with the Acceptable Use – Staff Policy.

- The Principal has the right to locally enforce storage of staff or visitor devices to a secure location such as the school office.
- The Principal can decide if devices can or cannot be taken to into areas around the school where there are particular safeguarding issues (such as changing rooms). In such cases, the school should agree with and inform staff, pupils and visitors the areas which are expected to be "BYOD free".
- Visitors and contractors to the school/site should be informed of the policy regarding personal devices upon arrival (please refer to our Volunteering Policy).
- Personal devices may only be used to access computer files on internet sites which are relevant to the classroom curriculum.
- The school or setting should agree and inform users of devices regarding what areas would be expected to be "BYOD free". We do not allow the use of personal devices in toilets, bathrooms and changing rooms.
- Personal devices must not be taken into controlled assessments and/or examinations, unless special circumstances apply.
- Staff, volunteers and contractors should not use their own personal devices for contacting children and young people or parents/ carers, unless it is an emergency and they are unable to use or access the school's telecommunication systems.
- If it is necessary for a phone call or text to be taken or received, care should be taken to avoid disturbance or disorder to the running of the school.
- When driving on behalf of their organization, any staff member or volunteer should ensure the safe use of any personal device.

9. Use of cameras and audio recording equipment

Parents and carers and visitors may **not** take photographs, videos or audio recordings of their children at school events for their own personal use.

Staff wishing to take photographs, video, or audio recordings in school **must** ensure that they are using a trust provided device e.g. camera, laptop etc. Parental permission to take photographs, films or recordings of the relevant individuals must have been received by the School and checked before photographs and video are taken. This includes any individual who might be identifiable in the background.

Photographs, video or audio recordings made by staff on their own mobile devices should be deleted as soon as reasonably possible after they have been used, e.g. uploaded for use on one of the School's social media sites or website. If photographs, video or audio recordings are to be retained for further legitimate use, they should be stored securely via the School network.

In order to protect the privacy of our staff and pupils, and, in some cases their safety and wellbeing, photographs, video, or audio recordings **must** not be published on blogs, social networking sites or disseminated in any other way without the permission of the people identifiable in them.

No one must use mobile devices to record people at times when they do not expect to be recorded, and devices must not be used that would enable a third party acting remotely to take photographs, video, or audio recordings in school (for further information, please refer to our Social Media Policy).