East Midlands Academy Trust

East Midlands Academy Trust

Use Your Own Device (UYOD) Policy

'Every child deserves to be the best they can be'

Inclusion Innovation Impact

Scope: East Midlands Academy Trust & Academies within the Trust	
Version: V1	**Filename:** UYOD Policy
Review: January 2025	**Next Review: April 2025** This policy will be reviewed by the Owner and approved at least annually by the Trust CEO.
Owner: Head of Shared Services	**Union Status:** Not Applicable
Policy type:	
Non-Statutory	New Policy

RevisionDate	Revisor	Description of Revision
January 2025 v1	D Unitt	New Policy implemented as a result of DPIA, template provided by Education data hub, the Trust's Data Protection Officer

1. Introduction

- East Midlands Academy Trust (EMAT) recognises that mobile technology offers valuable benefits to students from a teaching and learning perspective. EMAT embraces this technology but requires that it is used in an acceptable and responsible way.
- In certain scenarios, EMAT requires users to use their own personal devices to access school systems, these are outlined in the scope section of this document.
- Personal devices (any device which is not owned by EMAT) should only ever be connected to our secure segregated Guest or BYOD Wi-Fi networks, for internet access.
- This policy is designed to support the use of personal devices in a way that extends and enhances teaching and learning. It also aims to protect children from harm, minimise risk to EMAT systems.
- This policy supports our Data Protection Policy and provides guidance on how to minimise risks associated with the use of personal devices, in line with the General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018).
- This applies to all personal devices connecting to EMAT systems.
- EMAT reserves the right to refuse permission to use a personal device on the premises.
- This policy should be read in conjunction with any applicable EMAT policies.

2. Scope and Responsibilities

The following users are defined as in scope:

- All KS3 & KS4 Students will be required to use their own personal devices to access EMAT approved educational software via Microsoft Single Sign On (SSO), when working from home.
- All KS5 students will be required to use their own personal devices to access EMAT approved educational software via Microsoft Single Sign On (SSO), when working from home.
- All KS5 students may also use personal devices to access EMAT approved educational software via Microsoft Single Sign On (SSO), when working at school.
- Third party Agencies and Contractors will be required to use devices not owned by EMAT, in order to access the EMAT system(s) relevant to their business area and contractual relationship with EMAT.
- Trustees & Members will be required use personal devices for accessing Office 365, GovernorHub, SmartLog and National College services provided by EMAT.
- All other EMAT employees, and all EYFS, KS1 & KS2 students are not permitted to use their own devices.
    - Except named employees, at the discretion of the IT Business Partner or Head of Shared Services, using personal mobile phones, which are subject to additional Mobile Application Management (MAM) requirements.

The following users are defined as NOT in scope, but must still adhere to AUP and other relevant policies:

- Guests using the Guest Wi-Fi for internet access only.

- Governors using personal accounts and devices for accessing GovernorHub, SmartLog and National College Services provided by EMAT.
- Exam Invigilators using personal accounts and devices for accessing SmartLog and National College Services provided by EMAT.
- Newly onboarding colleagues using their personal email address and device for National College Services provided by EMAT.

All users are responsible for reading, understanding and complying with this policy.

If you have any concerns surrounding the use of personal devices, please contact the IT Business Partner or Head of Shared Services.

Users should be aware of the need to:

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

3. Use of personal devices

Permission must be sought before connecting personal devices to EMATs systems. EMAT reserves the right to refuse permission to use personal devices, without providing a reason.

Users are responsible for their personal devices at all times. EMAT is not responsible for the loss, 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 IT Business Partner or Head of Shared Services must be notified as soon as possible of any loss or theft of a personal device that has been used to access EMAT systems, and these incidents will be logged with the DPO.

Data protection incidents should be reported immediately to the schools Data Protection Officer, or a member of the IT department.

Personal devices used to access EMAT systems must have automatic updates enabled 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.

EMAT cannot and will not support users' personal devices, nor does EMAT hold the responsibility for conducting annual PAT testing of personal devices.

4. Access to EMATs Guest Wi-Fi connection

EMAT provides guest wireless connections on all its sites that users may, with permission, use to connect their personal devices to the Internet. Access to these connections is at the discretion of EMAT, who may withdraw access from anyone it considers to be using the service inappropriately.

EMAT cannot guarantee that the wireless networks are secure, and use is entirely at the users own risk. In particular, users are advised not to use the wireless network for online financial transactions.

EMAT does not permit the downloading of apps or other software whilst connected to the wireless connections and EMAT is not responsible for the content of any downloads onto the user's own device.

EMAT accepts no liability for any loss of data or damage to personal devices resulting from use of the network.

5. Access to EMATs IT systems

Where employees, trustees, members and consultants are permitted to connect to EMATs IT systems from their personal devices, a second layer of security should be enabled such as a password and/or encryption, 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. Students are excluded from the requirement to enable a second layer of security.

Users must **not** store personal data about EMAT staff or students on any personal devices, or on cloud servers linked to their personal accounts or devices.

With permission, it may be necessary for users to download EMAT 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 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 EMATs network and devices.

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

Before selling or giving your personal device which has been used to access the EMAT networks including cloud-based systems to someone else, including a family member or spouse, it must be cleansed of all EMAT related data, emails, systems and apps.

6. Monitoring the use of devices

EMAT reserves the right to use technology that detects and monitors the use of personal devices, which are connected to or logged on to our network or IT systems. The use of such technology is for the purpose of ensuring the security of its IT systems and company data.

The information that EMAT 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 EMAT IT systems, the content of emails sent via the network, and peer-to-peer traffic transmitted via the network.

Any inappropriate content received through EMATs IT services or EMATs internet connection should be reported to the Headteacher / IT Business Partner / Designated Safeguarding Lead as soon as possible.

7. Security of personal devices

Users must take all sensible measures to prevent unauthorised access to their personal devices, including but not limited to the use of a PIN, pattern or password to unlock the device, and ensuring that the device auto-locks if inactive for a short period of time.

EMATs Acceptable Use of IT and IT Security policies set out in further detail the measures to ensure responsible behaviour online.

8. Permissible and non-permissible use

Users participating in UYOD must comply with the ICT Acceptable Use Policy.

- Where there are particular safeguarding or safety requirements in some settings, for example, in SEND provisions & nurseries, the Headteacher has the right to require storage of personal devices in a secure location such as lockers.
- The Headteacher can decide if personal devices can or cannot be taken into areas around site where there are particular safeguarding issues (such as changing rooms). In such cases, EMAT should agree with and inform staff, students and visitors the areas which are expected to be "UYOD free".
- Users visiting the site should be informed of the policy regarding personal devices upon arrival (please refer to our Visitors and Contractors Policy).
- Personal devices must not be taken into controlled assessments and/or examinations, unless special circumstances apply.
- Users should not use their own personal mobile phone for contacting children and young people or parents/ carers, unless it is an emergency, and they are unable to use or access EMATs 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 EMAT.

9. Use of cameras and audio recording equipment

Users subject to this policy may not use their own mobile devices to take photographs, video, or audio recordings on any EMAT site, unless permission has been sought of the person/s being recorded.

In order to protect the privacy of our staff and students, 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 (for further information, please refer to our Social Media Policy).