East Midlands Academy Trust

Acceptable Usage Policy

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

Scope: East Midlands Academy Trust & Academies within the Trust	
Version: V7	**Filename:** EMAT Acceptable Usage Policy
Approval: October 2024	**Next Review: October 2025** This Policy will be reviewed & approved by the CEO annually
Owner: Head of Shared Services	

Policy type:	
	Replaces Academy's current policy

Revision History

Revision Date	Revisor	Description of Revision
October 2024 v7	DU	• Update to include the details around the use of personal hardware and online storage and communications accounts by staff and volunteers with explicit mention of smart devices, personal accounts to align with KCSIE 2024 section 6.0 • Update section 1.2 to reference KCSIE 2024and fixed hotlinks
July 2024 v6	DU	• Updated to align with KCSIE Part 1 2023
Dec 2023 v5.1	DU	• Updated to include that personal hotspots are not to be used in schools. Inclusion of Password policy content. • Responsibility for approval passed from board to Trust Leadership Team.
Oct 2023 v5	DU	• Updated to reference equipment loan agreement, KCSiE 2023 and Online Safety Policy, removed appendix 1 as no longer needed
Nov 2022 v4	DU	• Policy review – no changes.
Sept 2022 v3.1	DU	• Update to permit new staff who have not started to be able to access systems using personal devices
April 2022 v3		• Policy review – No changes from previous version
Jan 2021 v2		• Policy review - New Acceptable Usage Policy issued
July 2020 v1		• Acceptable Usage Policy issued

EMAT Acceptable Usage Policy

1. Information

1.1 This Acceptable Use Policy is intended to provide a framework for such use of East Midland Academy Trust's (EMAT) ICT Infrastructure. It should be interpreted such that it has the widest application including new and developing technologies and uses, which may not be explicitly referred to.

1.2 This policy has due regard to all relevant legislation and statutory and non-statutory guidance including, but not limited to, the following:

- Computer Misuse Act (1990);
- General Data Protection Regulation (2018);
- The Counter-Terrorism and Security Act 2015;
- Keeping Children Safe in Education 2024
- Guidance on Safer Working Practices

1.3 As a professional organisation with responsibility for safeguarding, all staff, and volunteers within EMAT are expected to take all possible and necessary measures to protect data, information systems and devices from damage, loss, unauthorised access, infection, abuse and theft.

1.4 All users of EMAT's ICT Infrastructure have a responsibility to use that infrastructure in a professional, lawful, and ethical manner, consistent with EMAT's values, national/local guidance and expectations, the law and relevant policies including:

- Employee Code of Conduct
- Data Protection Policy
- Online Safety Policy
- Disciplinary Policy
- Safeguarding Policy
- Social Media Policy

In addition, users who are issued with EMAT equipment will be bound by EMAT's Equipment loan agreement.

2. Responsibilities

It is the responsibility of all users of EMAT ICT Infrastructure, to read and understand this policy. This policy is reviewed on an annual basis but is liable for amends more frequently to comply with changes in governance to address technology trends.

3. Scope

All users (staff, students, trustees, governors, volunteers, visitors, contractors) of the Trust's facilities to this ICT Acceptable Usage Policy.

4. System Security and Policy

4.1 Hardware and software provided by the workplace for staff, volunteers and students use can only be used for educational use. Personal accounts or information such as personal photographs or personal files must not be accessed or stored on school devices and EMAT accepts no liability for loss of such data, EMAT's Equipment loan agreement provides further information.

4.2 Downloading or accessing programmes or files that have not been authorised by the Head of Shared Services or IT Business Partner could result in the activation of malware or ransomware when devices are reconnected to school networks. If in doubt, users should ask the IT team for guidance. Where there is a resultant breach, users may be individually liable for such a breach.

4.3 Users must not remove or attempt to inhibit any software placed on EMAT devices that is required for network compliance or security.

4.4 Users must not attempt to bypass any filtering, monitoring and/or security systems put in place by EMAT.

4.5 Damage or loss of a computer, system or data including physical damage, viruses or other malware must be reported to the IT team as soon as possible.

4.6 Users are liable for any loss, theft, or damage to equipment whilst in their care and may be charged for any such damage unless it can be attributed to reasonable wear and tear. The Equipment Loan Agreement provides greater detail.

4.7 EMAT reserves the right to monitor the activity of users on any if its ICT systems and devices and all devices should be considered always monitored.

4.8 Password security is important. Get Safe Online provides guidance on password security and recommend Do's and Don'ts https://www.getsafeonline.org/protecting-yourself/passwords/

4.9 Equipment issued under the EMAT equipment load policy remains the property of EMAT. EMAT may request the return of the any equipment for any reason at any time by giving appropriate notice. If staff are leaving EMATS employment, staff must return equipment prior to the leaving

date. Student leaving education that have been issued devices must return devices prior to their last day, failure to do so will result in the equipment value being deducted from final salary payments further details are provided in the EMAT Equipment load agreement.

4.10 EMAT's ICT infrastructure may not be used directly or indirectly by any user for any activity which is deemed to be unacceptable use, this consists of but is not limited to the following definitions:

The download, creation, manipulation, transmission, or storage of:

- any offensive, obscene, or indecent images, data or other material, or any data capable of being resolved into obscene or indecent images or material.
- unlawful material, or material that is defamatory, threatening, discriminatory, extremist or which has the potential to radicalise themselves or others.
- unsolicited "nuisance" emails, instant messages, or any other form of communication.
- material which is subsequently used to facilitate harassment, bullying and/or victimisation of a member of the Trust or a third party.
- material which promotes discrimination based on race, gender, religion or belief, disability, age or sexual orientation.
- material with the intent to defraud or which is likely to deceive a third party.
- material which advocates or promotes any unlawful act.
- material that infringes the intellectual property rights or privacy rights of a third party, or that is in breach of a legal duty owed to another party.
- material that brings the EMAT into disrepute.

Using EMAT's ICT Infrastructure deliberately for activities having, or likely to have, any of the following characteristics:

- intentionally wasting staff effort or other EMAT resources;
- corrupting, altering or destroying another User's data without their consent;
- disrupting the work of other Users or the correct functioning of EMAT ICT Infrastructure; or
- denying access to EMAT ICT Infrastructure and its services to other users.
- pursuance of personal commercial activities.

5. Data Protection

5.1 Staff and volunteers must be aware of their responsibilities under Data Protection legislation (including GDPR UK) regarding personal data of pupils, staff or parents/carers. This means that all personal data must be obtained and processed fairly and lawfully, kept only for specific purposes, held no longer than necessary and kept private and secure with appropriate security measures in place, whether used in the workplace, hosted online or accessed remotely. This includes safe and secure back up.

5.2 Staff and volunteers should seek to use designated school to store, manage, process or view personal information wherever possible to ensure security of information, appropriate deletion and archiving, and to ensure that searches in response to Subject Access Requests can easily and readily be completed. Data must not be extracted from these systems and installed in personal spreadsheets or documents unless absolutely necessary.

5.3 Emails, text messages, teams posts created or received as part of your role are subject to disclosure in response to a request for information under the Freedom of Information Act 2000 or a Subject Access Request under the Data Protection Act 2018. All e-mails, texts and messages should be written and checked carefully before sending, in the same way as a letter written on school headed paper. Do not use data subjects (staff, students, parents, contractors, volunteers) names in communications unless absolutely required where appropriate use initials. All electronic communications with students, parents, outside agencies and staff must be compatible with the professional role of staff. The person about whom a communication mail relates may request copies of the information therein.

5.4 Staff and Volunteers are reminded that any sharing of data with third parties should be subject to scrutiny by the Trust's Data Protection Lead to ensure an appropriate GDPR compliant data sharing agreement and appropriate licencing are in force. If you are not aware of whom your locations data protection lead is, please contact the senior administrator or school operations manager or the Head of Shared Service who will be able to inform you who the relevant person is.

5.5 Users should use appropriate trust platforms (such as Office 365 or teams) to access work documents and files in a password protected environment.

5.6 Staff are not permitted to use USB sticks to connect to any Trust device, no data is permitted to be stored on USB sticks.

5.7 Any images or videos of staff or students must only be for official EMAT use and reflect parental or age-appropriate student consent. Staff should ensure photos and videos are regularly uploaded to a shared network or official cloud drive, regularly deleted in line with retention policies, and removed from standalone devices.

5.8 Users are expected to respect copyright and intellectual property rights.

5.9 It is the responsibility of each account holder to keep their password secure. For the safety and security of users and recipients, all mail is filtered and logged, if necessary, e-mail histories can be traced. EMAT email account should be the account that is used for all school business.

5.10 Staff should actively manage e-mail accounts, delete e-mails of short-term value and carry out frequent housekeeping on all folders and archives, Email should never be used as filing system it is to be used as a communications system only, staff should ensure information is store on appropriate storage systems such as Arbor, Sam People, My Concern, SmartLog, Iris etc.

6. BYOD

6.1 Staff and volunteers are not permitted to use their personal devices or personal accounts to connect to EMAT's ICT Infrastructure or to access or store data belonging to the trust, the exemptions currently in place are.

- Access to SmartLog to allow Exam Invigilators and lunch time supervisors to undertake statutory training.
- Access to National College to allow Onboarding staff to complete statutory training.

- Access to GovHub for LAB members, trustees, and members to access papers and training to allow to provide governance to the trust

6.2 Staff and volunteers are not permitted to use personal mobile phones, personal tablets, personal smart watches, personal digital cameras, personal cloud storage accounts(icloud, OneDrive personal, google doc, google drive) , personal data transmission services (drop box, wee transfer,) to take store or transmit photos of student or staff, store or transmit EMAT data, any data that could be classed as Personal, Sensitive relating to a data subject linked to EMAT or commercials sensitive information unless explicit permission has been granted by the IT Business Partner

6.3 Staff and volunteers are not permitted to use personal mobile phones, personal tablets, personal smart watches, personal digital cameras whilst interacting with or in the presence of pupils

6.4 Staff and volunteers are not permitted to allow student to access or interact with their personal mobile phones, personal tablets, personal smart watches or personal digital cameras.

6.5 Staff and volunteers must never user personal communication tools to interact with students or parents with personal communications account (whatsapp, telegram, skype, teams, zoom etc) with the exception of when the student or parent is a family member, in which case a conversation should had with your DSL or head teacher explaining this is the case and confirming the relationship with the parent or student and when the communication is not related to EMAT and it's activities

6.6 Staff and volunteers should never use personal mobile phones, smart watches, connected smart devices or tablets to communicate with parents or students with the exception of when the student or parent is a family member, in which case a conversation should had with your DSL or head teacher explaining this is the case and confirming the relationship with the parent or student and when the communication is not related to EMAT and it's activities

6.7 Students are permitted to use personal devices to connect to the trust's ICT Infrastructure, as part of their learning, only if the academy has determined the device is appropriate (for example not a mobile phone) and the students is in a cohort that is permitted to bring in personal devices (for example sixth form students).

6.8 Staff and students are not to use personal hotspots when situated in a trust operated location.

7. Safeguarding

7.1 Staff are expected to immediately report any illegal, inappropriate, harmful material or any incidents they become aware of, to a Designated Safeguarding Lead.

7.2 Queries or questions regarding safe and professional practice online, either in an academy or off site should be raised with a Designated Safeguarding Lead, your local Headteacher or the People & Culture team.

8. Passwords

8.1 All users will have clearly defined access rights to school technical systems and devices. Details of the access rights available to groups of users will be recorded by the IT Team and will be reviewed, at least annually. All Trust ICT systems will be protected by secure passwords that are changed in line with IT Security best practice. The "administrator" passwords for the Trust systems will be allocated only to appropriate staff members, under the approval of the IT Business Partner or Head of Shared Service. Where possible, all administrator level accounts will be also protected with multi factor authentication Passwords for new users, allocated by the EMAT IT Team. Replacement network/application passwords will be allocated by the IT Support Team or authorised school personnel with access to specific tools. Wherever possible self-service password recovery services will be made available to end users. A record will be kept of all authorised personnel. All users will have responsibility for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence of a breach of security to one of the following:

- A member of the Trust's IT Department
- A Teacher (if a student identifies an issue)
- One of the Trust's Data Protection Leads (DPL).

Requests for staff password changes will be recorded using the IT Service desk. If required, solutions will be put into place to allow dedicated staff to change pupils/students' passwords.

EMAT will have administrator level passwords for all its systems and service, no supplier will have sole access to administrator level passwords.

Generic user accounts and passwords will never be issued to multiple staff or students.

8.2 Staff passwords

- All staff users will be provided with usernames and passwords to access the Trust's ICT infrastructure.
- The password will be a minimum of 8 characters long and must include three of – uppercase character, lowercase character, number, special characters.
- The password must not include proper names or any other personal information about the user that might be known by others.
- The account will be "locked out" following 10 successive incorrect log-on attempts where systems permit.
- Temporary passwords (e.g., used with new user accounts or when users have forgotten their passwords) will be enforced to change immediately upon the next account log-on.
- Passwords will not be displayed on screen and shall be securely hashed (use of one-way encryption) wherever possible.
- Passwords must never be left on public display or written down in an unsecured location.

- Passwords should be different for different accounts, to ensure that other systems are not put at risk if one is compromised and should be different for systems used inside and outside of school.
- Should be changed at least every 365 days.
- Should not re-used for 6 months and be significantly different from previous passwords.

8.3 Student/pupil passwords

- In Primary Phase from KS2 all students will be provided with their own user accounts depending on the technology and complexity and will be dependent on the cognitive ability of the students.
- Students will be taught the importance of password security.
- Student in secondary phase will follow the same policy as for staff passwords.

9. Exceptions

Exemptions from Unacceptable use: if there is legitimate academic activity that may be considered unacceptable use, as defined in this policy, for example, research into computer intrusion techniques, then notification must be made to the Head of Shared Services or IT Business Partner prior to the start of any activity.

10. Consequences

Failure to comply with this ICT Acceptable Usage Policy may result in one or more of the following actions taking place:

- restrict or terminate a User's right to use the Trust's ICT Infrastructure;
- withdraw or remove any material uploaded by that User in contravention of this Policy;
- disclose information to law enforcement agencies and take any legal action against a User for breach of this Policy, including but not limited to claiming all costs, fees and disbursements (including but not limited to legal fees) connected therewith; or
- where the User is also a member of the Trust community, the Trust may take disciplinary action up to and including expulsion from study or termination of employment.

11. Monitoring

All Trust ICT systems and devices are monitored in accordance with the Online Safety Policy and compliance with Keeping Children Safe in Education. Personal privacy cannot be assumed when using the Trust's hardware or systems. The Trust can monitor the usage of its own Infrastructure and services (internet access, email, teams, WiFi etc.) as well as activity on end user computer (Tablets, Laptops, Desktop computer, mobile phones etc.) without prior notification or authorisation from users when justifiable concerns have been raised.

12. Definitions

ICT Infrastructure – all computing, telecommunication, software, services and networking facilities provided by the Trust either onsite at any of its academies or related premises or remotely, with reference to all computing devices, either personal or Trust owned, connected to systems and services supplied by the Trust.

Users - any person granted authorisation to use any computer or device on the Trust ICT Infrastructure. This includes (but is not limited to) staff, students, visitors, customers (tenants or using site facilities), temporary workers, contractors, vendors, volunteers and sub-contractors authorised to access the network locally or remotely, for any reason, including email and Internet or intranet web browsing.

The Trust - refers to the East Midlands Academy Trust, Central Services and all Academies and sites associated with it.