East Midlands Academy Trust

Acceptable Usage Policy 2023/2024

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

Scope: East Midlands Academy Trust & Academies within the Trust	
Version: V3.1	**Filename:** EMAT Acceptable Usage Policy
Approval: April 2023	**Next Review: April 2024** *This Policy will be reviewed by the FHR committee annually*
Owner: East Midlands Academy Trust Board of Trustees Head of Shared Services	

Policy type:	
Statutory	Replaces Academy's current policy

Revision History

RevisionDate	Revisor	Description of Revision
November 2022	DU	• **Policy review – no changes.**
September 2022 v3.1	DU	• **Update to permit new staff whom have not started to be able to access systems using personal devices**
April 2022 – v3		• **Policy review – No changes from previous version**
January 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 the Trust's 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 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 2020
- Guidance on Safer Working Practices

1.3 As a professional organisation with responsibility for safeguarding, all staff within the East Midlands Academy Trust 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 the Trust's ICT Infrastructure have a responsibility to use the Trust's computer systems in a professional, lawful, and ethical manner, consistent with the Trust's ethos, national/local guidance and expectations, the law and relevant Trust and academy policies including:

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

2. Responsibilities

It is the responsibility of all users of the East Midlands Academy Trust (EMAT) 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

Members of the Trust and all other users (staff, students, trustees, governors, volunteers, visitors, contractors and others of the Trust's facilities are bound by the provision of its policies in addition to this ICT Acceptable Usage Policy.

4. System Security and Policy

4.1 Hardware and software provided by the workplace for staff and students use can only be used by for educational use. Personal accounts or information such as personal photographs or personal files should not be accessed or stored on school devices and the Trust accepts no liability for loss of such data.

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 school devices that is required by the Trust for network compliance or security.

4.4 Users must not attempt to bypass any filtering and/or security systems put in place by the Trust.

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 The Trust reserves the right to monitor the activity of users on any if its ICT systems and devices and all devices should be considered 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 remains the property of the Trust. The Trust may request the return of the any equipment for any reason at any time by giving appropriate notice. If staff are leaving employment of the Trust, 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 available in the EMAT Equipment loan agreement ***see appendix 1***

4.10 The Trust ICT infrastructure may not be used directly or indirectly by any user for any activity which is deemed to be unacceptable use, this consists 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 on the basis of 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; or
- material that brings the Trust into disrepute.

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

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

5. Data Protection

5.1 Staff must be aware of their responsibilities under Data Protection legislation (including GDPR) 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 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 messagesshould 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) names in comminications unless absolutely required where appropriate use initals 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 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 adminisatror or school operations manager or the Head of Shared Service who will be able to inform you who the relevant person is.

5.5 Staff must not keep trust-related personal information, including sensitive information, images, files, videos or emails, on any non-Trust issued devices unless approval has been granted by Head of Shared Services or IT Business Partner prior to the start of any activity.

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

5.7 Staff are not permitted to use USB sticks to connect to any Trust device, no data is permitted to be stored on USB sticks unless explicit approval has been granted by the Head of Shared Services or IT Business Partner for technical reasons and such devices are encrypted.

5.8 Any images or videos of students must only be for official Trust 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..

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

5.10 Staff must use trust provided accounts for all official communication, personal account must never be used. It is the responsibility of each account holder to keep the 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. The school email account should be the account that is used for all school business. Under no circumstances should staff contact students, parents or conduct any school business using personal e-mail addresses.

5.11 Staff should actively manage e-mail accounts, delete e-mails of short-term value and carry out frequent housekeeping on all folders and archives.

6. BYOD

6.1 Staff are not permitted to use personal devices to connect to trust's ICT Infrastructure unless explicitly permitted to do so by the Head of Shared Service or IT Business Partner. Exceptions generally only apply to teaching staff that have been recruited to join the trust and would like early access to trust online resources prior to starting with the trust and being issued with their official IT equipment. In the event that permission has been granted by the Trust the following conditions must be met to enable personal machine usage.

The user must consent to having their device being monitored by the trust's IT Department

The device must be viruses and malware free

The device must not be jail broken or running any unlicensed software

The device must be fully patched and not running any end of life software

6.2 Students are permitted to use any personal device they wish to connect to the trust's ICT Infrastructure either onsite or remotely

7. Safeguarding

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

8. 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.

9. Consequences

In the event of a breach of this ICT Acceptable Usage Policy by a user may in its sole discretion:

- 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.

10. Monitoring

All Trust ICT systems and devices are monitored in accordance to policy, so personal privacy cannot be assumed when using trust 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 compute (Tablets, Laptops, Desktop computer, mobile phones etc.) without prior notification or authorisation from Users when justifiable concerns have been raised. This will be in line with the Trust's Investigation procedure

11. 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.

Appendix 1

EMAT Equipment Loan Agreement

This agreement is between the East Midlands Academy Trust (EMAT) and the Custodian (referred to as the person receiving the equipment and signing the agreement). It covers short and long term equipment belonging to the trust which can include mobile computers, mobile phones, tablets, Keys, ID Badges and associated devices such as chargers and carry cases to members of staff on either permanent or fixed term contracts with the Trust as well as long term agency staff.

The Custodian agrees to receiving the items listed below, thus becoming the "registered custodian" of the equipment, the Custodian agrees to reasonable care of the issued equipment, any loss, damage or faults must be reported immediately to either the IT or Estates department via support desk ticket (servicedesk.emat.uk) or via email (servicedesk@emat.uk)

As part of the loan agreement the Custodian acknowledges custodianship of the items explicitly listed below, the equipment loaned to the Custodian will be recorded on the EMAT's assets register which is maintained by the trust's Shared Service team.

The Custodian agrees to reasonable use and care of the issued equipment, no other parties are permitted to have access the loaned equipment key whatsoever. Use of equipment loaned to a Custodian by a third party is strictly forbidden and could lead disciplinary procedures.

The Custodian also acknowledges the Loan Conditions and Processes listed below and is aware of the associated Tariffs for lost or damaged equipment which can be deducted from salary payments

Loan Conditions

- Usage of digital equipment is solely in line with the EMAT's Acceptable usage policy this policy is located online at the following location Trust policies (emat.uk)
- All equipment and accessories issued remain the property of the Trust.
- All loaned equipment issued must be returned on final day of employment with the Trust as per the staff leaving process listed below.
- Equipment must be secure and must never be left unattended in locations such as unlocked classrooms or offices, public areas in the school site, in your car (included the boot) or in a public place outside of the school such as bus, train or library.
- The Custodian must take all reasonable measures to ensure loaned equipment is treated with due care and kept in good condition and damage free.
- Any loss or damage to loaned equipment must be reported immediately, see the damaged or lost devices process.
- Mobile phones must remain in their trust issued protective case at all times.
- Under no circumstances should the Custodian allow any other individual to use or borrow loaned equipment, this includes other members of trust staff.
- Only members of the IT Department are permitted to carry out any form of hardware or software maintenance on loaned digital equipment.

- Loaned equipment must be produced whenever requested by authorised members of the trust.
- Serial numbers must match to ensure tariffs are not applied.
- Mobile phones returned locked without a PIN code will be deemed unusable and will incur a tariff being applied

Processes

Staff leaving Process

All loaned equipment must be returned at the end of the contracted term of employment by the Custodian. The equipment must be in a full working order and clean condition showing only acceptable usage wear and tear, any unreported damages or missing equipment will be deducted from the final salary payment using the tariffs listed in this loan agreement.

Equipment must be handed into an authorised member of the Trust these being

- A member of the central HR Department
- A member of the central IT Department
- Head Teacher for your academy
- HR/Senior Administrator, Operations Manager for your academy.

On handing in loaned equipment the Custodian will be issued a copy of the equipment returned record sheet for their records the Custodian should confirm all information is correct to avoid incorrect tariffs being applied to their salary.

Under no circumstance should equipment be given to other members of staff or left for in drawers or cupboards. Failure to return loaned equipment to authorised staff will result in the device being recorded as missing equipment and associated tariffs will be deducted from the final salary of the Custodian using the tariffs listed in this loan agreement.

Damaged or lost devices Process

Should a Custodian damage or lose their device they must report it immediately to the service desk. Via support desk ticket (servicedesk.emat.uk) if the device was a computer or mobile phone it must also be reported to your Academy's Data Protection Leads as this will be a GDPR Data Breach which will need recording and investigating, failure to report a breach can result in disciplinary action.

If it is determined that the device was lost due to failing to follow the conditions of the loan agreement or negligence on part of the Custodian, the Custodian will be changed accordingly from their salary using the associated tariffs listed on this loan agreement.

The Trust acknowledges that accidents do happen in which case replacement or repair costs will be deducted from the department budget or school budget, however repeated accidents will deemed to be negligence.

Tariffs for loss or damage

Laptop Computer	£550.00
Laptop Screen (Internal)	£200.00
Laptop Keyboard(internal)	£100.00
Laptop Power Supply	£50.00
Laptop Case	£25.00
Mouse	£15.00
Mobile Phone	£150.00
Mobile Phone Case	£15.00
Mobile Phone Screen	£100.00
Mobile Phone Charger	£15.00
ID Badge and lanyard	£15.00
Key or Alarm fob	£15.00
Tablet Device	£150.00
Tablet Screen	£100.00
Tablet Charger	£15.00
Tablet Case	£15.00

Equipment Loan Agreement

By signing this agreement, you agree to abide by the terms and conditions and processes set out above and relevant associated policies such as the EMAT Acceptable Usage Policy.

The below equipment has been loaned to you whilst you remain employed by the Trust but can be withdrawn/deactivated at any time.

Custodian	
Full Name	
Academy	
Equipment Issue Date	

Issuing Staff Member	
Full Name	

Loaned Digital Equipment			
Device	**Asset Tag**	**Serial Number**	**Accessories**

ID Badge/Keys/Alarm Fobs

Item	Academy	Room or Item Key	Key ID Number

I agree to the above conditions and acknowledge the processes listed in this agreement

Custodian Signature and Print Name	
Signature	
Print Name	
Date	

Loan Equipment Return Record

Below to be completed by authorised staff members on the return of loaned equipment

Returned Equipment Recipient	
Name of Custodian	
Recipient of equipment *Must be an authorised staff member*	
Date Equipment Returned	

Returned Equipment			
Device	**Asset Tag**	**Serial Number**	**Accessories**

Returned ID Badge/Keys/Alarm Fobs			
Item	**Academy**	**Room or Item Key**	**Key ID Number**

Equipment Inspection	
IT Technician Name	
Date Equipment Inspected	

Missing, Damaged, Serial Number Mismatch Equipment			
Device	**Asset Tag**	**Serial Number**	**Accessories**

Missing ID Badge/Keys/Alarm Fobs			
Item	**Academy**	**Room or Item Key**	**Key ID Number**

Salary Deduction Calculations	
Total Value of Deduction	
HR Payroll Notified Date	
HR/Payroll Acknowledgment	