East Midlands Academy Trust

Acceptable Usage Policy 2022/2023

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

Scope: East Midlands Academy Trust & Academies within the Trust	
Version: V3	**Filename:** EMAT Acceptable Usage Policy
Approval: April 2022	**Next Review: April 2023** *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
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, unathorised 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 Trust can provide details of the value of the equipment for any personal insurance purposes.

4.7 The Trust reserves the right to monitor the activity of users on any if its ICT systems and devicies from time to time.

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.

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 software such as SIMS, My Concern, or other proprietary software 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.

5.3 Emails created or received as part of your role may be 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 should be written and checked carefully before sending, in the same way as a letter written on school headed paper. Avoid using student/ staff names in email headers. All electronic communications with students, parents, outside agencies and staff must be compatible with the professional role of staff. The person about whom an email 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.

5.5 Staff must not keep school-related personal information, including sensitive information, images, files, videos or emails, on any non-school 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 school platforms (such as Office 365 or teams) to access work documents and files in a password protected environment.

5.7 Any data being removed from the school site (such as via email) must be suitably protected. This may include email/ data being encrypted by a method approved by the school.

5.8 Staff are not permitted to use USB sticks unless approval has been granted by the Head of Shared Services or IT Business Partner for technical reasons and such devices are encrypted.

5.9 Any images or videos of students must only be for official Trust use and reflect parental 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 such as iPads.

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

5.11 Staff must use school provided email accounts for all official communication, to minimise unsolicited or malicious email and to ensure all personal data is processed securely. 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.

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

5.13 Emailing personal, sensitive, confidential or classified information should be sent using appropriate secure email services, to a named recipient, with Delivered/ Read receipt, or other secure delivery services such as S2S.

6. Safeguarding

6.1 Staff are expected to immediately report any illegal, inappropriate, harmful material or any incidents they become aware of, to the Head of Governance or Designated Safeguarding Lead.

6.2 Queries or questions regarding safe and professional practice online either in school or off site should be raised with the Head of Governance, or the Designated Safeguarding Lead, or the Headteacher or HR.

7. 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.

8. 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 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.

9. Monitoring

All Trust ICT systems may be monitored in accordance to policy, so personal privacy cannot be assumed when using school hardware. 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

10. 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 to Acceptable Usage Policy: Equipment Loan Agreement

This agreement covers short and long term loan of Trust equipment. The term 'equipment' refers to any electronic device and/or non-electronic apparatus.
The below equipment has been loaned to you while you remain employed by the Trust but can be withdrawn at any time.

Security and Usage

- Usage is solely for professional use and not for personal use
- The laptop and all accessories remain the property of the Trust.
- The laptop and any other equipment must be returned when you leave your post or when requested by the Trust.
- At all times the laptop must be secure and must not be left unattended:
    - In your car
    - In a public place
- The laptop and equipment must be treated with due care and kept in good condition.

Software

- Only software installed by the IT team may be installed and used on the laptop.
- Personal software must not be loaded on to the laptop.

Faults

- All faults must be reported to and repaired by the EMAT IT team.
- Under no circumstances should hardware faults be repaired by any other member other than the EMAT IT team.

You are responsible for transferring or backing up any files/data you have created and stored within its internal memory/ hard drive. School/College staff cannot accept responsibility for the loss of data stored in this way, or data which are lost or erased during repair or reconfiguration.

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

You are responsible for transferring or backing up any files/data you have created and stored within its internal memory/ hard drive. School/College staff cannot accept responsibility for the loss of data stored in this way, or data which are lost or erased during repair or reconfiguration.

I agree to the above conditions:

Equipment Type	
Make and Model	
Asset No.	
Signature (staff)	
Print Name	
Date Returned	

Received in good condition Y/N	
Signed (IT support)	