East Midlands Academy Trust

Information Security Policy 2023/2025

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

Scope: East Midlands Academy Trust & Academies within the Trust	
Version: V2	**Filename:** EMAT Information Security Policy
Approved: April 2023 *Approved by the Trust Board*	**Next Review: April 2025** *This Policy will be reviewed by the Trust Board (A&R committee) bi-annually*
Owner: Head of Shared Services	**Union Status:** Not Applicable

Policy type:	
Non-Statutory	Replaces Academy's current policy

Referenced Policies / Proceedure
• Data Protection • Online Safety • Acceptable Usage • Access Control • Password Policy

Revision History

RevisionDate	Revisor	Description of Revision
April 2023 – v2	D Unitt	Reviewed – minor updates
October 2021-v1	D Unitt	New EMAT Information Security Policy issued

EMAT Information Security Policy

1. Introduction

This policy has been created to help enforce data protection recommendations across the East Midlands Academy Trust (EMAT) and to minimise the risk of IT security incidents and data breaches in relation to all personal or sensitive data.

The Information Security Policy outlines the Trust's organisational security processes and standards. The policy is based upon the sixth principle of the GDPR which states organisations must protect the personal data, which it processes, against unauthorised loss by implementing appropriate technical and organisational measures.

This policy has been written using the security framework recommended by ISO: 270001 (internationally recognised Information Security Standard).

This policy should be read in conjunction with the other policies in the School's Information Governance policy framework with particular focus on the Acceptable Use Policy and the Information Security Incident Reporting Policy.

This policy has been produced to deliver the following outcomes:

- Ensure Staff are aware of the Trust's expectations regarding information security relating to the Trust's ICT Infrastructure, protecting them from accidently undertaking unacceptable behaviour.
- Minimise the reputational, legal and governance risks to the Trust and its staff and students arising from use of a data breach of cyber incident.
- To ensure a consistent approach is applied across the Trust.
- To identify responsibilities of the Trust its staff and student in line with the following policies:
    - Data Protection
    - Online Safety
    - Social Media
    - Acceptable Usage
    - Password
    - Access Control
    - Records Management Policy and Retention Schedule.

2. Responsibility

It is the responsibility of all staff 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

All 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 Information Security Policy.

The policy applies to information in all forms including, but not limited to:

- Hard copy or documents printed or written on paper,
- Information or data stored electronically, including scanned images,
- Communications sent by post/courier or using electronic means such as email, fax or electronic file transfer,
- Information or data stored on or transferred to removable media
- Information stored on portable computing devices including mobile phones, tablets, cameras and laptops
- Speech, voice recordings and verbal communications, including voicemail,
- Published web content, for example intranet and internet,
- Photographs and other digital images.

4. Policy

4.1. Access Control

The Trust will maintain control over access to the personal data that it processes. These controls will differ depending on the format of the data and the status of the individual accessing the data. The Trust will maintain an audit log detailing which individuals have access to which systems (both electronic and manual). This log will be maintained by Trust.

4.1.1Manual Filing Systems

- Access to manual filing systems (i.e. non-electronic systems) will be controlled by a key management system. All files that contain personal data will be locked away in lockable storage units, such as a filing cabinet or a document safe, when not in use.
- Keys to storage units will be stored securely. The Headteacher or Department head will be responsible for giving authorising individuals access to the safe place. Access will only be given to individuals who require it to carry out legitimate business functions. Where a PIN is used, the password will be changed every three months or whenever a member of staff leaves the organisation, whichever is sooner.

4.1.2 Electronic Systems

- Access to electronic systems will be controlled through a system of user authentication. Individuals will be given access to electronic filing systems if required to carry out legitimate functions. A two tier authentication system will be implemented across all electronic systems. The two tiers will be username and unique password and where system permit Multi Factor Authentication will also be implemented.
- Individuals will be required to adhere the Trust's Password Policy.

4.1.3 Software and Systems Audit Logs

- The Trust will ensure that all major software and systems have inbuilt audit logs so that the school can ensure it can monitor what employees and users have accessed and what changes may have been made. Although this is not a preventative measure it does ensure that the integrity of the data can be assured and also deters individuals from accessing records without authorisation.

4.1.4 Data Shielding

- The Trust does not allow employees to access the personal data of family members or close friends. Employees should declare, upon employment, whether they are aware of any family members or friends who are registered at the East Midlands Academy Trust.
- The Trust will upon notification make arrangements that staff members will prevented access to files of family or friends and where possible any electronic files will be locked down so that the declaring employee cannot access that data.
- Employees who knowingly do not declare family and friends registered at the school may face disciplinary proceedings and may be charged with an offence under Section 170 of the Data Protection Act 2018 (unauthorised access to information).

4.1.5 External Access

- On occasions the Trust will need to allow individuals who are not employees of the Trust to have access to data systems. This could be, for example, for audit purposes, to fulfil an inspection, when agency staff have been brought in, or because of a Partnership arrangement with another Trust. A member of the Executive team in the trust or SLT in the Academy is required to authorise all instances of third parties having access to systems.

4.2 Physical Security

The Trust will maintain high standards of Physical Security to prevent unauthorised access to personal data. The following controls will be maintained by the school:

4.2.1 Clear Desk Policy

- Individuals will not leave personal data on desks, or any other working areas, unattended and will use the lockable storage units provided to secure personal data when not in use.

4.2.2 Alarm System

- The school will maintain a security alarm system at its premises so that, when the premises are not occupied, an adequate level of security is still in operation.

4.2.3 Building Access

- External doors to the premises will be locked when the premises are not occupied. Only authorised employees will be key holders for the building premises. The Head of Estates will be responsible for access to site but may to a member of their team, will be responsible for authorising key distribution and will maintain a log of key holders.

4.2.4 Internal Access

- Internal areas that are off limits to visitors, pupils and parents will be kept locked and only accessed through PIN or keys. PINs will be changed annually or whenever a member of staff leaves the organisation. Keys will be kept in a secure location and a log of any keys issued to staff maintained.

4.2.5 Visitor Control

- Visitors to the any Trust site are required to sign in a visitor systems and state their name, organisation, car registration (if applicable) and who they are visiting in electronic format.
- Visitors will not be allowed to access restricted areas without employee supervision.
- Visitor recorded will be retained inline with the Trust's Records Management Policy and Retention Schedule.

4.3 Environmental Security

As well as maintaining high standards of physical security, to protect against unauthorised access to personal data, the Trust must also protect data against environmental and natural hazards such as power loss, fire, and floods. It is accepted that these hazards may be beyond the control of the Trust, but the Trust will implement the following mitigating controls:

4.3.1 Back Ups

- The Trust will back up all electronic data and systems on a regular basis. Backups are kept on and off site by for on premise data and cloud services are backed up at alternative tenants. Should the Trust's electronic systems be compromised by an environmental or natural hazard, then the Trust will be able to reinstate the data from the backup with minimal destruction.

4.3.2 Fire Doors

- Areas of the premises which contain paper records or core electronic equipment, such as servers, will be fitted with fire doors so that data contained within those areas will be protected, for a period of time, against any fires that break out on the premises. Fire doors will not be propped open unless automatic door releases are installed.

4.3.3 Fire Alarm System

- The Trust maintains a fire alarm system at all its premises to alert individuals of potential fires and so the necessary fire protocols can be followed.

4.4 Systems Security

As well as physical security the Trust also protects against hazards to its ICT Infrastructure. It is recognised that the loss of, or damage to, ICT Infrastructure could affect the Trust's ability to operate and could potentially endanger the lives of its Pupils. The Trust has implemented the following systems security controls in order to mitigate risks to it's ICT Infrastructure:

4.4.1 Software Download Restrictions

- All sites within the Trust use a Firewall that features anti-malware protection, HTTPS inspection, anonymous proxy detection & blocking, intrusion detection & prevention and web-filtering.

4.4.2 Phishing Emails

- In order to avoid the Trust's ICT Infrastructure from being compromised through phishing emails, Users are encouraged not to click on links that have been sent to them in emails when the source of that email is unverified. Users will also take care when clicking on links from trusted sources in case those email accounts have been compromised. Users will check with the Trusts IT Shared Service Department Service Desk if they are unsure about the validity of an email.

4.4.3 Firewalls and Anti-Virus Software

- The Trust will ensure that the firewalls and anti-virus software is installed on electronic devices and routers. The Trust will update the firewalls and anti-virus software when updates are released. The Trust will review its firewall and anti-virus software on an annual basis and decide if still fit for purpose.

4.4.4 Shared Drives

- The Trust maintain multiple a shared drives on in the cloud or on premise. Whilst Users are informed not to store personal data on the Trust's ICT Infrastructure. Shared drives and file stores will have restricted areas that only authorised employees can access. For example a HR folder in the shared drive will only be accessible to employees responsible for HR matters.

- Department heads can request the granting of access to data they control via the Trusts IT Shared Service Department Service Desk. All data stored on the Trust's ICT Infrastructure will still be subject to the Trust's Records Management Policy and Retention document.

4.5 Communications Security

- The transmission of personal data is a key business need and, when operated securely is a benefit to the all users. However, data transmission is extremely susceptible to unauthorised and/or malicious loss or corruption. The Trust has implemented the following transmission security controls to mitigate these risks:

4.5.1 Sending Personal Data by post

- When sending personal data, excluding special category data, by post, the Trust will use Royal Mail's standard postal service. Employees will double check addresses before sending and will ensure that the sending envelope does not contain any data which is not intended for the data subject.

4.5.2 Sending Special Category Data

- The Trust will follow the Department for Educations guidelines for transferring data

4.5.5 Using the BCC function

- When sending emails to a large number of recipients, such as a mail shot, or when it would not be appropriate for recipients to know each other's email addresses, then Trust employees will utilise the Blind Copy (BCC) function for such activity.

4.6 Surveillance Security

The Trust operates CCTV at all its Academies. Due to the sensitivity of information that is collected as a result of this operation, the Trust has a separate CCTV Policy. This policy has been written in accordance with the ICO's Surveillance Code of Practice.

4.7 Remote Working

It is understood that on some occasion users of the Trust will need to work at home or away from the Trust's premises. If this is the case then the users will adhere to the following controls:

4.7.1 Lockable Storage

- If users are working at home they will ensure that they have lockable storage to keep personal data and Trust equipment safe from loss or theft. If the user does not have access to lockable storage then devices should be stored out of sight. Users must not keep personal data or Trust equipment unsupervised at home for extended periods of time (for example when the employee goes on holiday). Users must not keep personal data or Trust equipment in cars if unsupervised.

4.7.2 Private Working Area

- Users must not work with personal data in areas where other individuals could potentially view or even copy the personal data (for example on public transport). Users should also take care to ensure that other household members do not have access to personal data and do not use Trust equipment for their own personal use.

4.7.3 Trusted Wi-Fi Connections

- User will only connect their devices to trusted Wi-Fi connections and will not use 'free public Wi-Fi' or 'Guest Wi-Fi'. This is because such connections are susceptible to malicious intrusion. When using home Wi-Fi networks employees should ensure that they have appropriate anti-virus software and firewalls installed to safeguard against malicious intrusion. If in doubt users should seek assistance from the Trusts IT Shared Service Department Service Desk.

4.7.4 Encrypted Devices and Email Accounts

- Users will only use Trust issued encrypted devices to work on Personal Data. Employees will not use personal devices for accessing, storing, or creating personal data. This is because personal devices do not possess the same level of security as a Trust issued device. Users will not use personal email accounts to access or transmit personal data. User must only use Trust issued email accounts.

4.7.5 Data Removal and Return

- Users will only take personal data away from Trust sites if this is required for a genuine business need. Users will take care to limit the amount of data taken away from site. Users will ensure that all data is returned to the Trust premises either for re-filing or for safe destruction. Users will not destroy data away from the premises as safe destruction cannot be guaranteed

5 Consequences of Breach of Policy

In the event of a breach of this Information Security Policy by a user the Trust may in its sole discretion:

- restrict or terminate a user's right to use the Trust's ICT Infrastructure;
- 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.

6 Monitoring

All Trust ICT systems may be monitored in accordance with the Acceptable Usage Policy, so personal privacy cannot be assumed when using school hardware, software or services. The Trust can monitor the usage of its own Infrastructure and services (internet access, email, teams, Wi-Fi 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 which available from the Trust's HR team on request

7 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.

Staff – Those working for the Trust on a full time, part time or flex time basis, apprentices, agency workers and contractors.

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.