East Midlands Academy Trust

Password Policy

2023/2024

‘Every child deserves to be the best they can be’

East Midlands Academy Trust is a company limited by guarantee registered in England & Wales No. 08149829
Orchard Academy, Shepherdswell Academy, Castle Academy, Hardingstone Academy, Stimpson Avenue Academy,
Prince William School and Northampton International Academy are all business names of the East Midlands Academy Trust.

Scope: East Midlands Academy Trust & Academies within the Trust	
Version: V1	**Filename:** EMAT Password Policy 2023-2024
Approved: April 2023 *Approved by the Trust Board*	**Next Review: April 2024** *This policy will be reviewed by the Trust Board (FHRE committee) annually*
Owner: Head of Shared Services	**Union Status:** Not Applicable

Policy type:	
Non Statutory	Replaces Academy's current policy

Referenced Policies / Procedure
• Data Protection • Online Safety • Social Media • Acceptable Usage • Access Control

Revision History

RevisionDate	Revisor	Description of Revision
April 2023	D Unitt	Reviewed – no changes
July 2021 – v1	D Unitt	New EMAT Password Policy 2021/2022

EMAT Password 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.

A safe and secure password policy is essential if the above is to be established and will apply to all ICT infrastructure and social media accounts.

This policy has been produced to deliver the following outcomes:

- Ensure Staff are aware of the Trust's expectations when using passwords to access 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
    - Access Control

2. Responsibility

The Trust's IT Team will be responsible for ensuring that all ICT Infrastructure is safe and secure as is reasonably possible.

- users can only access data to which they have right of access
- no user should be able to access another's files, without permission
- logs are maintained of access by users and of their actions while users of the system

The IT Business Partner working with each academy Head Teacher will be responsible for ensuring that users conform to the policy on a day-to-day basis.

It is the responsibility of all users of the East Midlands Academy Trust (EMAT) ICT Infrastructure to read and understand this policy. This policy is reviewed on an annual basis but might be subject to amends more frequently to comply with changes in governance and/or to address technology trends.

3. Scope

Members of the Central office 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 Password Policy.

4. Policy

Description

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 Support Team and will be reviewed, at least annually.

All Trust ICT systems will be protected by secure passwords that are changed frequently 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 will be 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 Trusts 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

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.

Student/pupil passwords

- All users from KS2 and above will be provided with personal user accounts username and password.
- Students will be taught the importance of password security.
- The password complexity will be set with regards to the cognitive ability of the students

5. Exceptions

Exemptions from Password Policy: if there is legitimate justification for not following items defined in this policy, for example the limitations of the system password length or where a service with a single user account must be shared with multiple staff or students, then notification must be made to the Head of Shared Services or IT Business Partner and a record be kept of this no compliance with justification reasons.

6. Consequences of Breach of Policy

In the event of a breach of this Password Policy by a user, the Trust reserves the right to:

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

7. Monitoring

All Trust ICT systems may be monitored in accordance with the Password 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 is available from the Trust's HR team on request

8. 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.