Mercia Primary Academy Trust

School Password Security Policy Principles

Policy Status and Review

Date:	**June 2021**
Review Date:	**June 2023**
Signed by Director:	
Date Signed:	

Introduction

The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that:

- users can only access data to which they have right of access
- no user should be able to access another's files, without permission (or as allowed for monitoring purposes within the school's policies).
- access to personal data is securely controlled in line with the school's personal data policy
- logs are maintained of access by users and of their actions while users of the system (Securas)

A safe and secure username / password system is essential if the above is to be established and will apply to all school ICT systems, including email.

Responsibilities

The management of the password security policy will be the responsibility of the ICT Co-ordinator.

All users (adults and young people) 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 that there has been a breach of security.

Passwords for new users, and replacement passwords for existing users will be allocated by the ICT Co-ordinator with the support of the ICT Technician. Any changes carried out must be notified to the manager of the password security policy (above).

Users will change their passwords every 90 days and are not re-used for 12 months.

Training / Awareness

Members of staff will be made aware of the school's password policy:

- at induction
- through the school's e-safety policy and password security policy
- through the Acceptable Use Agreement

Pupils / students will be made aware of the school's password policy:

- in ICT and e-safety lessons
- through the Acceptable Use Agreement

Policy Statements

All users will have clearly defined access rights to school ICT systems.

All users will be provided with a username and password by the ICT Co-ordinator with the support of the ICT Technician,

The following rules apply to the use of staff passwords:

- passwords should be changed every 90 days.
- passwords should not be re-used within a 12-month period
- the password should be a minimum of 8 characters long and should include – lowercase characters, numbers and special characters•
- Passwords shall not be displayed on screen, and shall be securely hashed (use of one-way encryption)

Audit / Monitoring / Reporting / Review

The responsible person (the ICT Co-ordinator with the support of the ICT Technician) will ensure that full records are kept of:

- User Ids and requests for password changes
- User logins

In the event of a serious security incident, the police may request and will be allowed access to passwords used for encryption.

The trust's Auditors also have the right of access to passwords for audit investigation purposes

User lists, IDs and other security related information must be given the highest security classification and stored in a secure manner.

This information can be made available in a range of formats and languages, including Braille and large print. If this would be useful to you or someone you know, please contact your Directorate HR Unit.

A signed copy of this document is available from the school office.

Version control

Date approved	Version	Changes made	Reason for amendment
Jan 2014	1		
February 2016	2	none	
July 2018	3	NONE	
Oct 2020	3	None	
March 2021		Added range of formats	Accessibility