Mercia Primary Academy Trust

Cyber Security Policy

Policy Status and Review

Date:	**September 2023**
Review Date:	**September 2024**
Signed by Director:	**Lisa Colclough**
Date Signed:	**25/09/2023**

1. Introduction

1.1 Cyber security has been identified as a risk for the School and every employee needs to contribute to ensure data security.

1.2 The School has invested in technical cyber security measures, but we also need our employees to be vigilant and act to protect the School and its IT systems.

1.4 The CEO is responsible for cyber security across the Trust. This responsibility is delegated through to the Headteacher within the individual School.

1.5 If you are an employee, you may be liable to disciplinary action if you breach this policy.

1.6 This policy supplements other data management and security policies, mainly our [Data Protection Policy, Data Breach Policy, Information Security Policy, Acceptable Use Policy, Home Working Policy, Electronic Information and Communications Policy and Clear Desk Policy].

2. Purpose and scope

2.1 The purpose of this document is to establish systems and controls to protect the Trust/School from cyber criminals and associated cyber security risks, as well as set out an action plan should the School fall victim to cyber-crime**.**

2.2 This policy is relevant to all staff.

3. What is cyber-crime?

3.1 Cyber-crime is simply a crime that has some kind of computer or cyber aspect to it. It takes shape in a variety of different forms, e.g. hacking, phishing, malware, viruses or ransom attacks.

3.2 The following are all potential consequences of cyber-crime which could affect individuals and/or individuals: -

- cost;
- confidentiality and data protection;
- potential for regulatory breach;
- reputational damage;
- business interruption; and
- structural and financial instability.

3.3 It is important, given the serious consequences above, to be careful not to be the victim of cyber-crime and to follow the guidance within this policy.

4. **Cyber-crime prevention**

4.1. This cyber-crime policy sets out the systems we have in place to mitigate the risk of cyber-crime. The CEO/Headteacher/SLT can provide further details of other aspects of the Trust/School risk assessment process upon request.

4.2. The Trust/School have put in place a number of systems and controls to mitigate the risk of falling victim to cyber-crime. These include technology solutions as well as controls and guidance to staff.

4.3 Technology solutions

(a) The School have a variety of technical measures in place for protection against cyber-crime. They include:

(i) firewalls;
(ii) anti-virus software;
(iii) anti-spam software;
(iv) auto or real-time updates on our systems and applications;
(v) URL filtering;
(vi) secure data backup;
(vii) encryption;
(viii) deleting or disabling unused/unnecessary user accounts;
(ix) deleting or disabling unused/unnecessary software;
(x) using strong passwords; and
(xi) disabling auto-run features.

4.4. Controls and guidance for staff

(a) all staff must follow the policies related to cyber-crime and cyber security as listed in the introduction to this policy, see section 1.
(b) all staff will have access to training via the staff training package as appropriate; when there is a change to the law, regulation or policy; where significant new threats are identified and in the event of an incident affecting the Trust/School or any third parties with whom we share data.
(c) all staff must:
- (i) choose strong passwords which contains at least 12 characters long including both numbers, uppercase and lowercase letters and a symbol;
- (ii) keep passwords secret;
- (iii) never reuse a password;
- (iv) never allow any other person to access the school's systems using your login details;
- (v) not turn off or attempt to circumvent any security measures (antivirus software, firewalls, web filtering, encryption, automatic updates etc.) that the IT team have installed on their computer, phone or network or the School IT systems;
- (vi) report any security breach, suspicious activity, or mistake made that may cause a cyber-security breach, to the CEO/Headteacher/SLT as soon as practicable from the time of the discovery or occurrence. If your concern relates to a data protection breach you must follow our data breach policy;

(vii) only access work systems using computers or phones that the School owns. Staff may not connect personal devices to the Trust/School's Wi-Fi;

(viii) not install software, all software requests should be made to the CEO/Headteacher/SLT for authorisation. This authorisation must be provided to the Trust's ICT team; and

(ix) avoid clicking on links to unknown websites, downloading large files, or accessing inappropriate content using Trust/School equipment or networks.

(d) all staff must not misuse IT systems. The School considers the following actions to be a misuse of its IT systems or resources:

(i) any malicious or illegal action carried out against the Trust/School or using the Trust/School's systems;

(ii) accessing inappropriate, adult or illegal content within Trust/School premises or using School equipment;

(iii) excessive personal use of Trust/School's IT systems during working hours;

(iv) removing data or equipment from Trust/School premises or systems without permission, or in circumstances prohibited by this policy;

(v) using Trust/School equipment in a way prohibited by this policy;

(vi) circumventing technical cyber security measures implemented by the Trust's ICT team; and

(vii) failing to report a mistake or cyber security breach.

5. Cyber-crime incident management plan

5.1. The incident management plan consists of four main stages:

(i) **Containment and recovery** to include investigating the breach and utilising appropriate staff to mitigate damage and recover any data lost where possible.

(ii) **Assessment of the ongoing risk** to include confirming what data has been affected, what happened, whether relevant data was protected and how sensitive it is and identifying any other consequences of the breach/attack.

(iii) **Notification** to consider if the cyber-attack needs to be reported to regulators (for example the ICO) and/or colleagues/parents as appropriate.

(iv) **Evaluation and response** to consider any improvements to data security and evaluate future threats to security.

5.2 Where it is apparent that a cyber security incident involves a personal data breach, the school will invoke their Data Breach Policy rather than follow out the process in this section.

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

Version	Date Approved	Changes	Reasons for Alterations
	March 2021	Added a range of formats	Accessibility
	July 2023	Removed mention of staff intranet	No longer in use
	September 2023	Password character update	Accessibility