Robert Peel Primary School

Cyber Security Policy

Date policy last reviewed: September 2023

Signed by:

_____ Headteacher Date: _____

_____ Chair of Governors Date: _____

1. Introduction

This document provides the overarching governance policy for the protection and security of our school data and information.

The policy aims to define the high-level governance of Cyber Security within the school.

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

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

This policy supplements other data management and security policies, namely our

- Data Protection Policy
- Acceptable Use Policy
- Business Continuity Policy

2. Objectives

The main objectives of this policy are:

- To present the management approved requirements, control objectives and principles for Cyber Security.
- To define the structure and roles within our school's Cyber Security structure
- To maintain confidence that our school's Cyber Security governance meets its corporate and ICT risk appetite.
- To maintain confidence that our school's Cyber Security governance meets the requirements of the law including the data protection regulations, the guidance on government use of cloud services and other compliances as required.

3. Scope

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

This policy is relevant to all staff.

4. Policy Mandate, Approval and Maintenance

This policy is approved by the Governing Body. The policy will be reviewed regularly and at least annually, and in case of any impacting changes (for example, changes to policy, legislation, regulation, industry standards, school ICT environment, etc.), to ensure it remains current, appropriate and applicable.

5. What is Cyber Crime?

Cyber-crime is simply a criminal activity carried out using computers or the internet: hacking, phishing, malware, viruses or ransom attacks.

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

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

6. Cyber-Crime Prevention

Given the seriousness of the consequences noted above, it is important for the School to take preventative measures and for staff to follow the guidance within this policy.

This cyber-crime policy sets out the systems we have in place to mitigate the risk of cyber-crime.

The 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 for staff.

Technology solutions

(a) The School have implemented the following technical measures to protect against cyber-crime:

(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.

7. Controls & Guidance for staff

(a) all staff must follow the policies related to cyber-crime and cyber security as listed in earlier in this policy.

(b) all staff will be provided with training at induction and refresher training 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 School or any third parties with whom we share data.

(c) all staff must:

(i) choose strong passwords (the School's IT team advises that a strong password contains [list of types of characters, password length etc. as permitted by your IT systems]);

(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 Headteacher 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 Protection Policy;

(vii) only access work systems using computers that the School owns.

(viii) not install software onto your School computer. All software requests should be made to the Headteacher, and

(ix) avoid clicking on links to unknown websites, downloading large files, or accessing inappropriate content using School equipment and/or networks. This includes attachments in emails.

(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 School or using the School's systems;

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

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

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

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

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

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

8. Cyber-Crime Incident Management Plan

The incident management plan consists of four main stages:

(i) ***Containment & Recovery:*** To include investigating the breach, utilising appropriate staff to mitigate damage and where possible, to recover any data lost.

(ii) ***Assessment of the Ongoing Risk:*** To include confirming what happened, what data has been affected and whether the relevant data was protected. The nature and sensitivity of the data should also be confirmed, and any consequences of the breach/attack identified.

(iii) ***Notification:*** To consider whether the cyber-attack needs to be reported to regulators (for example, the ICO and National Crime Agency) and/or colleagues/parents as appropriate.

(iv) ***Evaluation & Response:*** To evaluate future threats to data security and to consider any improvements that can be made.

Where it is apparent that a cyber-security incident involves a personal data breach, the School will invoke their Data Protection Policy rather than follow out the process above.