# Cyber Security Policy

**Document Owner and Approval**

Marsh Green Primary School is the owner of this document and is responsible for ensuring that this policy document is reviewed in line with the school's policy review schedule.

A current version of this document is available to all members of staff on the staff drive.

Signature: Date: 17/04/2024

# Cyber Security Policy

## Introduction

Cyber security has been identified as a risk for Marsh Green Primary and every employee needs to contribute to ensure data security.

Marsh Green Primary has invested in technical cyber security measures, but we also need our employees to be vigilant and to act to protect Marsh Green Primary IT systems.

Mrs Joanna Hervey and Mr. Kieran Jonson are responsible for cyber security within the school.

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, Data Breach Policy, Acceptable Use Policy, Home Working Policy, and Clear Desk Policy.

## Purpose and Scope

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

This policy is relevant to all staff.

## What is Cyber-Crime?

Cyber-crime is simply a criminal activity carried out using computers or the internet including 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.

# Cyber Security Policy

**Cyber-Crime Prevention**

Given the seriousness of the consequences noted above, it is important for Marsh Green Primary 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. Mrs Joanna Hervey or Mr. Kieran Johnson can provide further details of other aspects of the school risk assessment process upon request.

Marsh Green Primary has put in place several 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**

Marsh Green Primary 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.

# Cyber Security Policy

**Controls and Guidance for Staff**

- All staff must follow the policies related to cyber-crime and cyber security as listed in this policy.
- 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 Marsh Green Primary or any third parties with whom we share data.
- All staff must:

- Choose strong passwords (the School's IT team advises that a strong password contains a capital letter, numbers, and a special character.
- keep passwords secret.
- never reuse a password.
- never allow any other person to access the school's systems using your login details.
- 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, tablet or any other portable device or network or Marsh Green Primary IT systems.
- report any security breach, suspicious activity or mistake made that may cause a cyber security breach, to Mrs Joanna Hervey 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.
- only access work systems using computers, tablet, or any other portable device that Marsh Green Primary owns. Staff are not permitted to connect personal devices to the Wi-Fi.
- not install software onto your school computer, tablet, or any other portable device. All software requests should be made to Mrs Joanna Hervey and
- avoid clicking on links to unknown websites, downloading large files or accessing inappropriate content using School equipment and/or networks.

# Cyber Security Policy

- Marsh Green Primary considers the following actions to be a misuse of its IT systems or resources:

- any malicious or illegal action carried out against Marsh Green Primary or using the school's systems to do so.

- accessing inappropriate, adult, or illegal content within School premises or using School equipment.

- excessive personal use of School's IT systems during working hours.

- removing data or equipment from School premises or systems without permission, or in circumstances prohibited by this policy.

- using School equipment in a way prohibited by this policy.

- circumventing technical cyber security measures implemented by the School's IT team; and

- failing to report a mistake or cyber security breach.

**Cyber-Crime Incident Management Plan**

The incident management plan consists of four main stages:

(i) *Containment and 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 and 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, Marsh Green Primary will invoke their Data Breach Policy rather than follow out the process above.