GEOFFREY FIELD INFANT SCHOOL

CYBER SECURITY POLICY

Introduction

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

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.

The Headteacher is 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, Information Security Policy, Acceptable Use Policy and the Home Working Policy

Purpose and 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.

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.

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 Business Manager can provide further details of other aspects of the School risk assessment process upon request.

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

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 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.

Controls and guidance for staff

All staff must follow the policies related to cyber-crime and cyber security as listed in earlier 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 the School or any third parties with whom we share data.

It may be appropriate in some instances to limit the number of people involved or who have access to information on a matter to ensure the security of the data involved. This can be part achieved through IT security measures. We may implement other controls that are more practical in nature, e.g.:

- Physically ringfencing the individuals or teams working on a matter;
- Taking steps to ensure our system for opening, distributing and/or scanning incoming correspondence (by post, email or otherwise) does not allow or inadvertent sharing of confidential information;
- Getting a signed confidentiality agreement from each staff member;
- Disposing of confidential documents securely;
- Having a clear desk policy;
- Discouraging staff from reading confidential papers or discussing sensitive matters in public.

Due diligence – we may conduct due diligence on the cyber security controls and cyber-crime prevention measures that other parties with whom we share information.

Governor training and cybersecurity responsibility

Governing boards have strategic oversight of their school's cyber security. This requires governors to have sufficient knowledge and understanding to inform conversations with school leaders about managing cyber security risks.

The new DfE Governance Guides published in March state that 'At least one governor/trustee should complete cyber security training'.

Governing bodies will seek assurances from senior leaders that their school is adequately prepared if a cyber incident occurs and that, as governors, they are aware of cyber risks.

(DfE Maintained School Governance Guide section 7.7.3)

Safeguarding and cybersecurity link governor- Zoe Glancy

All staff must:

(i) choose strong passwords (the School's IT support advises that a strong password contains upper case and lowercase letters, numbers and special characters)

(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 School Business Manager 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 and visitors that are given permission by school leadership, may connect personal devices to the school Wi-Fi provided;

(viii) not install software onto your School computer or phone. All software requests should be made to the School Business Manager who will liaise with Soft Egg over the request; and

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

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, the School will invoke their Data Breach Policy rather than follow out the process above.

Issue Date	Review Date	Issued by
October 2025	October 2026	N Sibley SBM