Bruce Grove Primary School

CYBER SECURITY POLICY

September 2023

Document Owner and Approval

Janice George, Headteacher, 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 shared drive.

Decision making body & date of approval	The Governors of Bruce Grove Primary School

Version History Log

Version	Description of Change	Date of Policy Release by Judicium
1	Initial Issue	19.10.21
2	Formatting amendments	03.08.22

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 to act to protect the School IT systems.

The IT manager/IT Tech support team 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, Information Security Policy, Acceptable Use Policy, Home Working Policy, Electronic Information and Communications Policy and Clear Desk 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 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-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. Claudia Walsh 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 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.

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 the School 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 mixture of characters, numbers, upper and lower case letters and at least 8 characters).
- 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, phone or network or the School IT systems;
- report any security breach, suspicious activity or mistake made that may cause a cyber security breach, to IT manager or SBM 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 or phones that the School owns. Staff may only connect personal devices to the Wi-Fi provided;

- not install software onto your School computer or phone. All software requests should be made to Ian Jenkins, IT manager
- avoid clicking on links to unknown websites, downloading large files or accessing inappropriate content using School equipment and/or networks.

The School considers the following actions to be a misuse of its IT systems or resources:

- any malicious or illegal action carried out against the School or using the School's systems;
- 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.

<u>Cyber-Crime Incident Management Plan</u>

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.