Cyber Security Policy

Sir John Heron Primary School

Change History Record

Version	Description of Change	Date of Policy Release by Judicium
1	Initial Issue	19.10.21
2	Formatting amendments	03.08.22
3	Included details of cyber crime, technology solutions, controls and guidance for staff.	30.08.24

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 ICT Manager (via the School's ICT provider at The Education Space) 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 and Acceptable Use 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 – The global cost of all forms of online crime is estimated to be in excess of £300 billion. We may be fined up to £17.5 million or 4% of the total worldwide annual turnover if we fail to protect our data.

- Confidentiality and data protection - Protecting individuals' confidential information and all forms of personal data is one of the most essential requirements our school. The risk to confidential information and personal data is the biggest of all threats from cyber-crime.

- Potential for regulatory breach – We have various regulatory duties which we could unintentionally breach through falling victim to cyber-crime or a cyber-attack. Loss

of personal data can lead to claims for damages by the individuals concerned and/or significant fines from the Information Commissioners Office (ICO).

- Reputational damage – A cyber security incident can have a major impact on our reputation, particularly if it involves the loss of confidential information, personal data and/or is reported in the media. Protecting our reputation is of utmost importance.

- Business interruption – Some forms of cyber-attack could render key systems (for instance servers including email servers, cloud computing services or our website) unavailable. This would have a major impact on delivering lessons and delivering our services. It may be necessary in such cases to invoke our Business Continuity Plan. The Headteacher is responsible for making that decision and communicating with IT.

- Structural and financial instability – The financial losses flowing from online crime may cause or contribute to financial difficulty.

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 Headteacher 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

(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.

Controls and guidance for staff

- All staff must follow the policies related to cyber-crime and cyber security as listed in this policy.

- Technology solutions in isolation cannot protect us adequately, so our systems and controls extend to cover the human element of cyber-crime/cyber security risk.

- 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.

All staff must:

- Ensure you are familiar with the risks presented by cyber-crime and cyber security attacks or failures and take appropriate action to mitigate the risks by taking a sensible approach, e.g. not forwarding chain letters or inappropriate/spam emails to others. We will help you by continually raising awareness of those risks and providing training where necessary.

Report any concerns you may have.

Passwords

- Choose strong passwords (the School's IT team advises that a strong password contains *capital letters, symbols, numbers and is not a word.*
- 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 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 Breach Policy;
- only access work systems using computers or phones that the School owns.
- not install software onto your School computer or phone. All software requests should be made to the ICT Technician after approval from the Headteacher ; and
- 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.

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. We will notify our insurers as soon as reasonably practicable of any circumstances that may give rise to claim under relevant insurance policies. We will also assess whether it is necessary to invoke our business continuity plan.

(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.