LONDON BOROUGH OF HAVERING

ST. URSULA'S CATHOLIC PRIMARY SCHOOL

CYBER SECURITY POLICY

"With God at the heart of our St Ursula's family, we welcome all as we learn and grow together"

Autumn 2024

1. 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 and Computing Lead 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 policies.

2. 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 set out an action plan should the School fall victim to cyber-crime.

3. What is cyber-crime?

Cyber-crime is simply a crime that has some kind of computer or cyber aspect to it. It takes shape in a variety of different forms, e.g. hacking, phishing, malware, viruses or ransom attacks.

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

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

It is important, given the serious consequences above, to be careful not to be the victim of cyber-crime and to follow the guidance within this policy.

4. Cyber-crime prevention

This cyber-security policy sets out the systems we have in place to mitigate the risk of cyber-crime. The Headteacher and Computing Lead can provide further details of other aspects of the school risk assessment process upon request.

The School has 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 to staff.

Technology solutions

a) The School have a variety of technical measures in place for protection against cyber-crime. They include: (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.

Controls and guidance for staff

(a) all staff must follow the policies related to Computing and cyber security as listed in the introduction to 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;

(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 Head teacher 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.

(viii) do not install software onto your School computer or phone. All software requests should be made to the SNS; and

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

5. Cyber-crime incident management plan

The incident management plan consists of four main stages:

(i) **Containment and recovery** to include investigating the breach and utilising appropriate staff to mitigate damage and recover any data lost where possible.

(ii) **Assessment of the ongoing risk** to include confirming what data has been affected, what happened, whether relevant data was protected and how sensitive it is and identifying any other consequences of the breach/attack.

(iii) **Notification** to consider if the cyber-attack needs to be reported to regulators (for example the ICO) and/or colleagues/parents as appropriate.

(iv) **Evaluation and response** to consider any improvements to data security and evaluate future threats to security.

Where it is apparent that a cyber security incident involves a personal data breach, the school will invoke their Data Breach Policy.

Signed: _____

Head teacher

Signed: _____

Governing Body

11th December 2024