WIDFORD LODGE

PREPARATORY SCHOOL

Cyber Security Policy

This policy applies to all pupils at Widford Lodge School including those in the EYFS

Reviewed and approved by the Proprietor: September 2026

Date of next review: September 2027

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 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, esafety and IT security policy and Acceptable Use of Technology agreement.

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. The Headteacher can provide further details of other aspects of the School's 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.

(xii) Implementing MFA

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.
- All Staff who wish to access their data from home will be required to setup MFA (Multi Factor Authentication) on their account which will either send a code to their phone or an official authentication app.
- 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 partly achieved through IT security measures but we may implement other controls such as disposing of confidential documents securely, discouraging staff from reading confidential documents or discussing sensitive matters in public, restricting who opens incoming correspondence.
- We may conduct due diligence on the cyber security controls and cyber crime prevention measures of 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. We will help you by continually raising awareness of those risks and providing training where necessary.
- Report any concerns you may have.
- Choose strong passwords (the School's IT team advises that a strong password contains a minimum of 8 characters and a maximum of 256 characters. They also require 3 out of 4 of the following: lowercase characters, uppercase characters, numbers 0-9, symbols. It cannot contain any parts of the username);
- 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 devices that the School owns. Staff may only connect personal devices to the school Wi-Fi provided;
- not install software onto your School computer or devices. All software requests should be made to softegg and 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.

(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 the Data Breach Policy rather than follow out the process above.