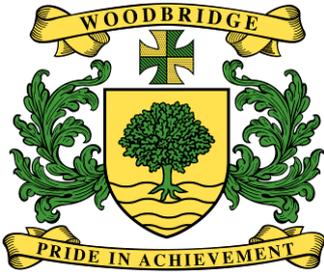


# **WOODBIDGE HIGH SCHOOL**

## **CYBER SECURITY POLICY**

**2025-2026**



# WOODBIDGE HIGH SCHOOL

## Cyber Security Policy

Updated: Autumn 2025

<b>Name of organisation:</b>	Woodbridge High School
<b>Designated Officer:</b>	Jeremy Clifton
<b>Deputy Designated Officer:</b>	

### Contents

1. Introduction
2. Core Principles
3. Risk Management
4. Acceptable Use
5. Data Security
6. Incident Response
7. Policy Review

## 1. Introduction

This policy outlines the procedures and expectations for ensuring the cyber security of Woodbridge High School's information and systems. Its purpose is to protect against unauthorised access, use, disclosure, alteration, or destruction of data. This policy is applicable to all staff, students, governors, and third-party users of the school's ICT systems.

## 2. Core Principles

The school is committed to:

- **Confidentiality:** Ensuring that information is not disclosed to unauthorised individuals.
- **Integrity:** Maintaining the accuracy and completeness of data.
- **Availability:** Ensuring that information and systems are accessible when needed.

## 3. Risk Management

The school has identified several key cyber security risks, including:

- **Third-Party Supplier Breaches:** The school relies on numerous software and service providers, and a breach of one of these could expose school data.
- **Phishing and Social Engineering:** Staff and students are targets for phishing emails that attempt to steal login credentials.
- **Ransomware:** A ransomware attack could encrypt the school's data, making it inaccessible.

To mitigate these risks, the school has implemented the following controls:

- **Onsite and Offline Backups:** Data is backed up daily to two onsite locations and two offsite cloud locations. One of the cloud backups is an "immutable" backup, which protects against malware.
- **Malware and Antivirus Software:** The school uses malware protection from LGfL and Sophos Intercept X antivirus software.
- **Network Monitoring:** LGfL provides 24/7 network monitoring to detect suspicious activity.
- **Staff Training:** All staff and governors are required to complete annual NCSC Cyber Security Training and regular training provided by Boxphish.

## 4. Acceptable Use

All users of the school's ICT systems must adhere to the **Acceptable Use Policy**. Key points include:

- **Confidentiality:** Do not share confidential information with unauthorised individuals.
- **Access Control:** Do not attempt to access systems or information for which you do not have authorisation.
- **Personal Use:** Personal use of school ICT systems is permitted but should be limited.
- **Removable Media:** Be cautious when using removable media, such as USB drives, as they can be a source of malware.

## 5. Data Security

- **Passwords:** All users must create strong passwords that are at least 8 characters long and contain a mix of uppercase and lowercase letters, numbers, and special characters.
- **Data Encryption:** Sensitive data should be encrypted, especially when stored on portable devices.
- **Data Disposal:** When disposing of old equipment, ensure that all data is securely erased.

## 6. Incident Response

In the event of a cyber security incident, the school will follow the **RPA Cyber Response Plan**. The plan includes procedures for:

- **Reporting the incident:** All incidents should be reported immediately to the IT Support team and the Deputy Headteacher in charge of ICT.
- **Containing the incident:** The IT team will take steps to contain the incident and prevent further damage.
- **Investigating the incident:** The incident will be investigated to determine the cause and extent of the damage.
- **Recovering from the incident:** The school will restore data from backups and take steps to prevent similar incidents from happening in the future.

## 7. Policy Review

This policy will be reviewed annually by the Designated Officer and the F&GP Committee.

**Policy Approval: Approved via F&GP Chair's Action on 3<sup>rd</sup> November 2025**

**Reviewer: Mr J. Clifton (Deputy Headteacher)**

**Fate of Next Review: Autumn term 2026**