



Cybersecurity Policy



Introduction

A cybersecurity incident can have a major impact on any organisation for extended periods of time. For a school, this can range from minor reputational damage and the cost of restoring systems from existing backups, to major incidents such as losing student work or access to learning platforms and safeguarding systems, which could lead to data-protection fines or even failing an inspection.

This Cybersecurity Policy outlines Oak Lodge School's guidelines and security provisions which are there to protect our systems, services and data in the event of a cyberattack.

Scope of Policy

This policy applies to all Oak Lodge School staff, contractors, volunteers and anyone else granted permanent or temporary access to our systems and hardware. It also covers the physical and technical elements that are used to deliver IT services for the school.

Risk Management

Oak Lodge School will include cybersecurity risks on its organisational risk register, regularly reporting on the progress and management of these risks to Governors X1 times a year.

Physical Security

Oak Lodge School will ensure there is appropriate physical security and environmental controls protecting access to its IT Systems, including but not limited to air conditioning, lockable cabinets, and secure server/communications rooms.

Asset Management

To ensure that security controls to protect the data and systems are applied effectively, Oak Lodge School will maintain asset registers for, files/systems that hold confidential data, and all physical devices (servers, switches, desktops, laptops etc) that make up its IT services.



Cybersecurity Policy

User Accounts

Users are responsible for the security of their own accounts. If at any time they believe their credentials may have been compromised, for example after a phishing scam, they must change their password and inform IT Manager as soon as possible. Personal accounts should not be used for work purposes. Oak Lodge School will implement multi-factor authentication where it is practicable to do so.

Devices

To ensure the security of all Oak Lodge School issued devices and data, users are required to:

- Lock devices that are left unattended
- Update devices when prompted
- Report lost or stolen equipment as soon as possible to IT Manager
- Change all account passwords at once when a device is lost or stolen (and report immediately to IT Manager)
- Report a suspected threat or security weakness in Oak Lodge School's systems to the IT Manager

Devices will be configured with the following security controls as a minimum:

- Password protection
- Full disk encryption
- Client firewalls
- Anti-virus / malware software Sophos and Malwarebytes.
- Automatic security updates
- Removal of unrequired and unsupported software
- Autorun disabled
- Minimal administrative accounts

Data Security

Oak Lodge School will take appropriate measures to reduce the likelihood of the loss of availability to, or the disclosure of, confidential data.

Oak Lodge School's defines confidential data as:

- [Personally identifiable information](#) as defined by the ICO
- [Special Category personal data](#) as defined by the ICO
- Unpublished financial information

Critical data and systems will be backed up on a regular basis following the 3-2-1 backup methodology

- 3 versions of data
- 2 different types of media
- 1 copy offsite/offline



Cybersecurity Policy

Sharing Files

Oak Lodge School recognises the security risks associated with sending and receiving confidential data. To minimise the chances of a data breach users are required to:

- Consider if an email could be a phishing email or that a colleague's account could be 'hacked'. If something does not feel right check with the sender by another method, particularly in relation to financial transactions, attachments, or links to websites
- Wherever possible, keeping Oak Lodge School's files on school systems
- Not sending school files to personal accounts
- Verifying the recipient of data prior to sending
- Using file encryption where possible, sending passwords/keys via alternative communication channels
- Alerting [IT Support/DPO] to any breaches, malicious activity or suspected scams

Training

Oak Lodge School recognises that it is not possible to maintain a high level of Cybersecurity without appropriate staff training. It will integrate regular Cybersecurity training into Inset days, provide more specialist training to staff responsible for maintaining IT systems and promote a "No Blame" culture towards individuals who may fall victim to sophisticated scams

System Security

IT Manager will build security principles into the design of IT services for Oak Lodge School

- Security patching – network hardware, operating systems and software
- Pro-actively plan for the replacement of network hardware, operating systems and software before vendors stop providing security support for them
- Actively manage anti-virus systems
- Actively manage and test backups
- Regularly review and update security controls that are available with existing systems
- Segregate wireless networks used for visitors' & staff personal devices from school systems
- Review the security risk of new systems or projects



Cybersecurity Policy


Major Incident Response Plan

Oak Lodge School will develop, maintain, and regularly test a Cybersecurity Major Incident Response Plan. This will include identifying or carrying out:

- Key decision-makers
- Key system impact assessments and restoration priorities (i.e. which backups needs to be restored first for the school to become operational again)
- Emergency plans for the school to function without access to systems or data
- Alternative methods of communication, including copies of contact details
- Emergency budgets and who can access them / how
- Key agencies for support (e.g. IT support company)

Maintaining Security

Oak Lodge School understands that the financial cost of recovering from a Major Cybersecurity Incident can far outweigh the ongoing investment in maintaining secure IT systems. Oak Lodge School will budget appropriately to keep cyber related risk to a minimum.

 Oak Lodge School	Headteacher / Principal	Ms Caroline Rowlandson
	Chair of Governors	Mr Stephen Cave
	IT Manager	Mr Chivna Tseayo
	Date this policy was reviewed and by whom	26 th September 2024 by Chivna Tseayo
	Date of next review and by whom	26 th September 2025 by Chivna Tseayo