Malden Oaks
School & Tuition service

Making the MOST of every day

CYBERSECURITY POLICY

Responsible: Laura Dandy / SLT

Status: Not Statutory

Date reviewed: Autumn 2023

Next review Date: Autumn 2025

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.

Scope of Policy

This policy applies to all 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.

Physical Security

Malden Oaks will ensure there are 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.

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 the Head of Business Services as soon as possible. Personal accounts should not be used for work purposes. Malden Oaks will implement multi-factor authentication where it is practicable to do so.

Devices

To ensure the security of all 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 the Head of Business Services
- Change all account passwords at once when a device is lost or stolen (and report immediately to the ICT Officer)
- Report a suspected threat or security weakness in Malden Oaks' systems to the Head of Business Services

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

- Password protection
- Client firewalls
- Anti-virus / malware software [eg Sophos and Malwarebytes for LGfL schools – see sophos.lgfl.net / malwarebytes.lgfl.net]
- Automatic security updates
- Removal of unrequired and unsupported software
- Autorun disabled
- Minimal administrative accounts

Data Security

Malden Oaks will take appropriate measures to reduce the likelihood of the loss of availability to, or the disclosure of, confidential data.

Malden Oaks defines confidential data as:

- **Personally identifiable information as defined by the ICO**
- **Special Category personal data as defined by the ICO**
- **Unpublished financial information**

Sharing Files

Malden Oaks 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 Malden Oaks' 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 the Head of Business Services to any breaches, malicious activity or suspected scams

Training

Malden Oaks recognises that it is not possible to maintain a high level of Cybersecurity without appropriate staff training. We will provide specialist training for staff responsible for maintaining IT systems and promote a "No Blame" culture towards individuals who may fall victim to sophisticated scams.

System Security

Our IT Support Service (Strictly Education) build security principles into the design of our IT services

· Security patching – network hardware, operating systems and software

· 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

· Review and update security controls that are available with existing systems

· Review the security risk of new systems or projects

Major Incident Response Plan

Malden Oaks will include Cybersecurity within its Critical 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
- Key agencies for support (e.g. IT support company)

Maintaining Security

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