New Milton Infant School

Cybersecurity Policy

School name	New Milton Infant School
Date of Policy Issue	Spring 2026 To Be Reviewed by Spring 2027
Name of responsible Manager/Headteacher	Amy Wake
Date approved by Governors if statutory	Spring 2026

Cyber attacks and incidents are an increasing threat to all businesses in both the private and public sector. Failure to protect the school against cyber criminals could result in total loss of data and systems, ransom demands and serious data breaches of personal information of our staff, pupils and wider community.

New Milton Infant School has taken all reasonable preventative measures to ensure that we are fully protected from cyber-attacks. This policy outlines the measures our school takes to protect its digital systems, data, and users from cybersecurity threats. It ensures a safe and secure digital environment for pupils, staff, and visitors.

Scope

This policy applies to:

- All staff (teaching and non-teaching)
- Governors and volunteers
- Pupils (with age-appropriate guidance)
- Contractors and visitors using school systems
- All devices connected to the school network

Roles and Responsibilities

- Headteacher: Overall responsibility for cybersecurity.
- Designated Safeguarding Lead (DSL): Ensures online safety is part of safeguarding.
- IT Support Provider: Manages technical security controls.
- Staff: Follow cybersecurity procedures and report concerns.
- Pupils: Taught basic online safety in the curriculum and are supervised by staff when using technology.

Acceptable Use

- Staff must use school devices and accounts for work-related tasks only.
- Pupils use devices under supervision and only access age-appropriate content.
- Personal devices (including external USB's) must not connect to the school network unless approved.
- All users must follow the school's Acceptable Use Agreement.

Data Protection and Privacy

- Personal data must be stored securely and only accessed by authorised staff.
- Staff must not share passwords or leave devices unlocked.
- Pupil data must not be stored on personal devices or shared externally without permission.

Firewall

- All digital technology is protected with a correctly configured software firewall including protection from ransomware attacks. This is kept up to date and supported by our IT service provider.
- All external internet connections run via the firewall.
- Remote access to the firewall is restricted to those who are authorised and need to maintain it.
- Firewall traffic is actively monitored and alerts given when necessary.
- Any attempts to access our network by unauthorised connections are blocked by default.
- Firewall rules are set to allow sufficient access for users to perform their jobs whilst providing a reasonable level of protection.
- A software firewall is in place for digital technology used outside of the school such as in staff homes.

Anti Malware

Anti malware is software designed to detect, stop and remove malicious software and viruses.

- Web pages are scanned as they are being used
- Our IT support provider is able to intervene should anti-malware software fail or not update.
- Files and applications are scanned upon access, when downloaded or opened locally or from a network folder.
- Attachments on incoming and outgoing emails are scanned for malware.
- If staff see a malware alert on their computer, they are advised to immediately disconnect from the school network and call our IT support provider to investigate and remove the threat as necessary or to take precautionary steps depending on the situation.
- Access to potentially malicious websites is prevented.

Security checks

We control the applications and software that can be used on our school's systems and devices.

- Downloads are checked for malware before they can be stored or installed on their device
- All new application/software requests are to be made via our IT support provider to check they do not pose a security risk. Only software from known suppliers are installed.
- A current list of approved software is maintained on the contracts register.
- Internet browser settings are managed and reviewed to make sure the highest form of protection is enabled and users are unable to change these settings to bypass security features
- Our IT support provider maintains documents on how our digital technology is setup and which security features have been enabled/disabled and whether they have conflicting security features.
- Emails are set up to be secure and to reduce the risk of third parties sending imitation emails.

Passwords

- Users are required to follow robust password policies to keep user accounts secure.
- Devices must be locked when unattended.
- Staff are reminded to immediately change passwords if they have been compromised or are suspected of compromise
- Admin access is restricted to authorized personnel only.

For Network Settings

- Staff Users have a password of at least 6 characters to physically access school network
- Staff network passwords can be reset by the Senior Admin Officer or our IT support provider only
- Pupils log into the school network by using their specific username however no password is required due to their age. Pupils are monitored by staff at all times when online in school.
- Pupils and staff can be identified on our filtering and monitoring reports by their username.

Licensing

- All software, systems and applications is used under accordance with our software licences
- Our operating systems and firmware on all our digital technology is kept up to date with updates usually issued overnight to avoid impact on teaching and learning
- Licence expiry dates are recorded in our contracts register to help with budget planning.
- We are notified by our IT support provider of any end of support dates for software packages.

Security updates

- All digital technology is regularly updated to fix security issues.
- Security updates (known as patching) to operating systems, applications and firmware, including configuration changes, are completed within 14 days of the release of the patch where the vulnerability is described as high risk or worse, or has a Common Vulnerability Scoring System (CVSSv3) score
- Devices are isolated if high risk patches are unavailable (this could mean removing the device from the network or separating it from higher risk systems and data)

Data backups

- To ensure our school can recover quickly from a cyber incident. 3 backup copies of data are uploaded to the cloud each day (away from fire, flood, theft and similar risks)

- Backups are immutable (this means that they cannot be changed once they have been created – this helps prevent data loss and reduces the risk of malware or ransomware being introduced into your systems when restoring data

- Backups are tested and logged termly (or whenever there is a significant change) – test includes ability to recover and restore backups

- Restoring data is not usually device specific and can be recovered to a wide range of hardware.

Training and Awareness

- Staff receive regular updates on cybersecurity and online safety.
  Pupils are taught digital responsibility in an age-appropriate way. Parents are offered guidance on keeping children safe online at home.
- All staff need to remain vigilant at all times to the potential threat of a cyber attack.

Reporting a Cyber Incident

- All cybersecurity incidents must be reported to the Headteacher or DSL immediately. The school will investigate and take appropriate action.
- Serious breaches will be reported to external authorities (e.g., DfE, ICO, Action Fraud).
- If the incident involved a data breach it must be reported to the Information Commisioners Office (ICO) under GDPR guidelines.

Policy Review

- This policy will be reviewed annually or following a significant incident or change in guidance.