



Cyber Security Policy

Status	Non - statutory
Review cycle	Annual
Date written/last reviewed	April 2026
Date of next review	April 2027
Signature of Co-Headteacher Mrs Wreford	
Signature of Chair of Governors Christina Powell	
Published on website	No

Introduction

This policy is part of the School's Statutory Safeguarding and GDPR policy and Staff Code of Conduct.

- The Information Security policy, which details our IT infrastructure, will be reviewed annually as part of our annual GDPR audit. Or when any significant changes occur with regard to the technologies in use within the school
- There is widespread ownership of the policy and it has been agreed by the SLT and approved by Governors. All amendments to this policy will be disseminated to all members of staff and pupils.

Scope

This policy applies to all members of our community (including staff, pupils/pupils, volunteers, parents/carers, governors, visitors, community users) who have access to and are users of our IT systems, both in and out of Meadlands Primary School

This policy is broken up into the following sub-sections

1. **Managing IT and Communication System**

- Internet access, security (virus protection) and filtering
- Network management (user access, backup, curriculum and admin)
- Passwords policy
- E-mail
- School website
- Learning platform
- Social networking
- Video Conferencing

2. **Data Security**

- Management Information System access
- Data transfer
- Asset Disposal

Managing the IT Infrastructure

Managing IT and Communication System

Internet access, security (virus protection) and filtering

This school:

- informs all users that Internet/email use is monitored;
- uses the LGfL age appropriate filtering system which blocks sites that fall into categories (e.g. adult content, race hate, gaming). All changes to the filtering policy are logged and only available to staff with the approved 'web filtering management' status;
- Uses Sophos anti-virus software (from LGfL);
- Uses DfE, LA or LGfL approved systems including DfE S2S, LGfL USO FX2 secure file/email to send 'protect-level' (sensitive personal) data over the Internet
- Uses encrypted devices or secure remote access where staff need to access 'protect-level' (sensitive personal) data off-site;
- Works in partnership with the LGfL to ensure any concerns about the system are communicated so that systems remain robust and protect pupils.

Network management (user access, backup)

This school

- Uses individual, audited log-ins for all users - the LGfL USO system;
- Uses guest accounts occasionally for external or short term visitors for temporary access to appropriate services;

- Uses teacher 'remote' management control tools for controlling workstations/viewing users/setting-up applications and Internet web sites, where useful;
- Has additional local network monitoring/auditing software installed;
- Ensures the Systems Administrator/network manager is up-to-date with LGfL services and policies/requires the Technical Support Provider to be up-to-date with LGfL services and policies;
- Has daily back-up of school data (admin and curriculum);
- Uses secure, 'Cloud' storage for data back-up that conforms to [DfE guidance](#);
- Storage of all data within the school will conform to the EU and UK data protection requirements; Storage of data online, will conform to the [EU data protection directive](#) where storage is hosted within the EU.

To ensure the network is used safely, this school:

- Ensures staff read and sign that they have understood the school's online safety Policy. Following this, they are set-up with Internet, email access and network access. Online access to service is through a unique, audited username and password.
- All pupils have their own unique username and password which gives them access to the Internet and other services; they each have a Google Chrome login and a LGfL login.
- Makes clear that no one should log on as another user and makes clear that pupils should never be allowed to log-on or use teacher and staff logins;
- Requires all users to log off or lock their screen when they have finished working or are leaving the computer unattended as per GDPR school procedures.
- Ensures all equipment owned by the school and/or connected to the network has up to date virus protection;
- Makes clear that staff are responsible for ensuring that any computer or laptop loaned to them by the school, is used primarily to support their professional responsibilities.
- Makes clear that staff accessing LA systems do so in accordance with any Corporate policies; e.g. Borough email or Intranet; finance system, Personnel system etc.
- Maintains equipment to ensure Health and Safety is followed;
- Ensures that access to the school's network resources from remote locations by staff is audited and restricted and access is only through school/LA approved systems:
- Does not allow any outside Agencies to access our network remotely except where there is a clear professional need and then access is audited restricted and is only through approved systems;
- Has a clear disaster recovery system in place that includes a secure, remote off site back up of data in The Cloud;
- This school uses secure data transfer; this includes DfE secure S2S website for all CTF files sent to other schools;
- To transfer SEND files, for example reports and referral forms which include personal data, secure sending platforms such as Egress, USO-FX or Cisco are used;
- Ensures that all pupil level data or personal data sent over the Internet is encrypted or only sent within the approved secure system in our LA or through USO secure file exchange (USO FX);
- Our wireless network has been secured to industry standard Enterprise security level /appropriate standards suitable for educational use;

- All IT and communications systems installed professionally and regularly reviewed to ensure they meet health and safety standards;

Password policy

- This school makes it clear that staff and pupils must always keep their passwords private, must not share with others; if a password is compromised the school should be notified immediately.
- All staff have their own unique username and private passwords to access school systems. Staff are responsible for keeping their password(s) private.
- Staff passwords are to be changed every 90 days.
- We require primary contacts (Mrs McGeoch, Mrs Frank and Mrs Gee) to change their passwords into the MIS, LGfL USO admin site, every 90 days.
- We require staff using critical systems to use two factor authentication.

E-mail

This school

- Provides staff with an email account for their professional use, London Staffmail/LA email and makes clear personal email should be through a separate account;
- Will contact the Police if one of our staff or pupils receives an e-mail that we consider is particularly disturbing or breaks the law.
- Will ensure that email accounts are maintained and up to date
- We use a number of LGfL-provided technologies to help protect users and systems in the school, including desktop anti-virus product Sophos, plus direct email filtering for viruses.

Staff:

- Staff can only use the LA or LGfL e-mail systems on the school system
- Staff will use LA or LGfL e-mail systems for professional purposes
- Access in school to external personal e mail accounts may be blocked
- Ensures that all pupil level data or personal data sent over the Internet is encrypted or only sent within the approved secure system in our LA or through USO secure file exchange (USOFX);

School website

- The SLT, supported by the Governing body, takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained;
- Most material is the school's own work; where other's work is published or linked to, we credit the sources used and state clearly the author's identity or status;
- Photographs published on the web do not have full names attached. We do not use pupils' names when saving images in the file names or in the tags when publishing to the school website;

Cloud Environments

- Uploading of information on the school's online learning space is shared between different staff members according to their responsibilities e.g. all class teachers upload information in their class areas;
- Photographs and videos uploaded to the school's online environment will only be accessible by members of the school community;
- In school, pupils are only able to upload and publish within school approved 'Cloud' systems.

Social networking

Staff, Volunteers and Contractors

- Staff are instructed to always keep professional and private communication separate.
- Teachers are instructed not to run social network spaces for pupil use on a personal basis or to open up their own spaces to their pupils, but to use the schools' preferred system for such communications.
- For the use of any school approved social networking will adhere to our Twitter Policy and Staff Code of Conduct.

School staff will ensure that in private use:

- No reference should be made in social media to pupils, parents/carers or school staff;
- School staff should not be online friends with any pupil. Any exceptions must be approved by the Headteacher.
- They do not engage in online discussion on personal matters relating to members of the school community;
- Personal opinions should not be attributed to the school and personal opinions must not compromise the professional role of the staff member, nor bring the school into disrepute;
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

Pupils:

- Where appropriate are taught about social networking, acceptable behaviours and how to report misuse, intimidation or abuse through our online safety curriculum work.
- Pupils are required to sign and follow our Pupil Acceptable Use Agreement.

Parents:

- Parents are reminded about social networking risks and protocols through our parental Acceptable Use Agreement and additional communications materials when required including In Safe Hands.
- Are reminded that they need to ask permission before uploading photographs, videos or any other information about other people. This information is always shared at the start of any parent attended assembly.

3. Data security: Management Information System access and Data transfer

Strategic and operational practices

At this school:

- We ensure staff know who to report any incidents where data protection may have been compromised.
- All staff have had a satisfactory DBS check and records are held in single central record

Technical Solutions

- Staff have secure areas on the network to store sensitive files.
- We require staff to log-out of systems when leaving their computer.
- We use the LGfL USO Auto Update, for creation of online user accounts for access to broadband services and the LGfL content.
- All servers are in lockable locations and managed by DBS-checked staff.
- Details of all school-owned hardware will be recorded in a hardware inventory.
- Details of all school-owned software will be recorded in a software inventory.
- Where any protected or restricted data has been held we get a certificate of secure deletion for any server that once contained personal data.
- We are using secure file deletion software.