Mapledown School

Working and Learning Together

Access Control Policy

Name of School	Mapledown School
This policy was written on	2nd September 2024
This policy was ratified by FGB on	November 2024
The policy is to be reviewed in	September 2025

CONTENTS

1. Purpose

The objective of this policy is to minimise accidental or unauthorised access to School and/or partner connected systems, networks, applications, and information. It is applicable to all forms of logical access.

This document supports the School's Acceptable Use Policy and Code of Conduct for School Staff. It provides direction and support for the implementation of information security and is designed to help School employees carry out the business of the School in a secure manner. By complying with this policy, the risks facing the School are minimised.

2. Introduction

Individuals who are not explicitly granted access to School information or information systems are prohibited from using such systems.

Individuals employed by or under contract to the School shall be granted access only to information and information systems that are required to fulfil their duties.

Access will be granted only to those staff who have formally agreed to comply with the School's Acceptable Use Policy and have an employment relationship with the school, an appropriate confidentiality / non-disclosure agreement (agency workers, governors) or data processing agreement.

This policy applies to:

- All employees including temporary and agency workers, independent consultants and contractors.
- Governors
- Third party organisations who require access to the School's information systems and facilities should also be aware of the contents of this policy.

These are referred to as "schools workforce" or "users" in the rest of this document. Note that some issues in this document should also be applied to pupils.

The policy is not designed to be obstructive. If you believe that any element of this policy hinders or prevents you from carrying out your duties, please contact the Office and IT Managers.

This policy should be read in conjunction with the following documents:

- Acceptable Use Policy
- Data Protection Policy
- Cyber and Information Security Policy
- Information Classification and Handling Policy

3. Physical Access control

Control of entry into School buildings, sites and locations is important for the security of the School's information systems (both computerised and manual) and its employees.

Only authorised school workforce ix allowed access. The workforce gain entry via pass codes and sign into the building. Access control must be rigidly enforced in buildings and areas housing sensitive information assets.

Our buildings have IT facilities located in them and public access is restricted. Special measures for access enforcement, particularly outside school hours, have been taken.

4. IT operations and network access control

Access to information and information systems will be controlled on the basis of business and security requirements.

An access management process for every system/database must be created, documented, approved, enforced and communicated to all relevant schools, workforce and partner organisations (for instance MIS/finance which are heavily monitored and secure).

Each business application run by, or on behalf of the School, will have a nominated system administrator who is responsible for managing and controlling access to the application and associated information.

Access to information is based on "need to know" and segregation of duties and roles. The appropriate information, system, database, or application owner is the only individual that can authorise a systems administrator to grant or update access via the formal access management process.

Audits are carried out to ensure that access control is appropriately implemented according to 'business need to know' and 'segregation of duty and role' principles.

Special attention is given, where appropriate, to the need to control the allocation of privileged access rights, which allow users to override system controls.

Access control requirements are clearly defined, documented and maintained within an Access Policy Matrix, which specifies the rights of individuals or groups of users.

The School has adopted common Windows-based operating systems, and predefined user profiles will be maintained to restrict access. The matrix will be approved and reviewed by the data owner (the school and its nominated staff, such as IT manager and SLT) and occasionally reviewed by the School Governors.

5. User Access Management

User access management covers all stages of user access, from initial registration, through changes in role, to deregistration and revocation of access.

The security of systems, networks, applications and databases is heavily dependent on the level of protection of user IDs, passwords, and other credentials that provide access to it. Hence, protecting the credentials that provide access to information is indirectly protecting the information.
Identification and authentication of users and systems enables the tracking of activities to be traced to the person responsible.
Members of the school's workforce who require access rights to school data systems are assigned unique User IDs (cloud login accounts and server profiles) for their professional and sole use. Schools' workforce are educated that they are not permitted to allow their user ID to be used by anyone else. Schools' workforce must be made aware of this and how to store them.
The Office Manager issues and revokes the user IDs. Redundant user accounts are monitored and managed.

6. User registration

A process for user registration and granting access rights exists and includes:

- Once the onboarding process has been completed (vetting, DBS, reference uptake and photo ID verification), a school ID card is issued, and the IT team create user accounts for access to devices/emails/online services, etc.
- Unique user IDs assigned so that access and modifications can be traced
- Authorised users are aware of their responsibilities for the protection of information within the application and where applicable users sign an appropriate agreement
- Ensuring access is granted once authorisation is obtained
- Maintaining a record of all registered users

7. Change of role

Where a member of the schools workforce changes role within the School the following process is followed:

- Line manager must inform all relevant information owners/system administrators of the names of employees that have transferred to different job/roles within 24 hours of transfer.
- Information owners must review the transferee's access rights to their systems to ensure that they are still valid.
- IT Manager amends the user's access rights as appropriate to their new role and in accordance with the requirements of the school management. This may include upgraded/downgraded permissions to services such as CPOMS (safeguarding), Google Shared Drives and the school's MIS.
- The IT Manager informs necessary staff when transfers to system administrators take place.

8. Review of access rights

Line managers should review access lists to ensure they are still applicable. Necessary modifications must be sent to system administrators for correction.
The data owner must approve access rights prior to set up by the system administrator (IT Manager).
The system administrator does not have the authority to decide who should have access to what information. This is a business decision.

9. Removal of access

On resignation of employment, line managers, in conjunction with HR, will undertake a risk assessment and determine whether existing access rights of an individual should be reviewed and reduced whilst working out their notice. Hostile terminations must be communicated to system administrators immediately and access immediately disabled.
Managers must inform the IT manager of the names of employees that will be leaving at least 2 school days before the end of their last working day.
Access rights should be disabled by 5.00 pm on the leavers' last working day.
It is the responsibility of line managers to ensure that leavers return their entry ID pass at the end of their last working day and to return it to Office Manager for deactivation as well as return all School IT equipment that could be used to gain network access.

10. Password Management and Multi-factor Authentication

To identify school workforce users, usernames must require another access token in order to login into school systems. This can be a biometric, a time-sensitive generated password, a hardware token, a user-managed password or a combination of these. Systems using highly sensitive information may require multi-factor authentication (MFA) depending on the level of access needed by the individual:

- CPOMS requires MFA for Designated Safeguarding Leads to permit access to all student incident reports.
- CPOMS requires MFA for IT Support to permit access to the admin portal (excluding safeguarding rights).
- LGfL requires MFA for elevated USO access rights to services such as the admin portal, WebScreen filtering and Freedom2Roam.
- Google Workspace requires MFA for individual user accounts to permit access to selected shared drives depending on job role.
- Google Admin requires MFA to access the admin portal to manage user accounts, data access and Workspace controls.
- Classroom Cloud requires MFA via a signed-in Google account to access services such as monitoring reports and managing school devices.
- School.apple.com requires MFA to manage app purchases and licences which are synchronised with Meraki MDM.
- Meraki MDM requires MFA to manage school devices, primarily iPads, allowing the creation of profiles and app rollouts.
- Sophos Central requires MFA to access the unified console for managing Sophos antivirus products, allowing the administration of protection across the network and endpoint to cloud security.

All systems must use **at least** passwords for access. Strong password management will be in place according to the individual requirements of various school services.

Controls will be in place to ensure strong password management. Where the software solution allows, the password complexity will adhere to current guidance, e.g. the National Cyber Security Centre (NCSC) “three words” guidance for passwords.

- Passwords must not be displayed on screen at any time.
- Users can reset their own passwords in some systems, in others, only system administrators are permitted to reset passwords or assign new passwords
- System administrators must ensure that they divulge new or reset passwords only to the authorised user of that ID.
- When it is known or suspected that a user ID has been compromised the system administrator must be immediately informed in order to have it revoked and the LBB/LGFL Service Desk informed so that an ICT Security Incident can be logged.
- System passwords, including administrator passwords that are used to access data that is required by the business, must be stored in secure locations such that in the advent of a business requirement the passwords can be recovered.

11. Privilege management

A process is in place for the allocation and removal of system administration level access or increased user privilege and includes the following controls:

- Every level of privilege within each application and the categories of users to which they need to be allocated are identified and recorded
- Privileges are allocated to an individual as an event requires
- Authorisation is recorded for each allocated level of privilege and only granted once authorisation is obtained
- The development of system routines are identified and implemented to avoid the use of privileged access
- Privileges are assigned to a different user ID from those used for normal business use and where possible a log of increased user privilege is recorded.

12. Monitoring System Access and Use

Systems will be monitored to detect deviation from the Access Control Policy and record events to provide evidence in case of security incidents.

The school employs Sophos Intercept X for both Endpoint and Server protection to safeguard Windows systems against malware threats and security incidents. Sophos Central provides a security management platform, benefitting from superior cyber protection using pre-configured policies, summary reporting and automatically prioritised alerts.

Chromebook security is provided by onboard layers of protection and is supported by the Google Admin portal which can force account sign-outs and necessitate the reauthentication of Chromebooks via MFA to protect school data. Further details: https://support.google.com/chromebook/answer/3438631?hl=en-GB

The system administrator and school management will provide logging and monitoring reports as required for investigative purposes such as incidents, audit, fraud and legal obligations. Event logs will be adequately secured, possibly centrally and separately from privileged-level employees (separation of duties).

13. Access from Overseas

Access to the School's network from overseas is subject to additional controls to ensure compliance with relevant legislation and this will place additional personal liability on users. Please refer to the Acceptable Usage Policy for details.

ICT equipment supplied by the School may only be taken to countries identified as having an assessment of adequate data protection by the ICO or the School. See the ICO page:
https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-transfers/

Note that the above applies equally to school owned devices and personal devices with ability to access School data (i.e. BYOD).

14. Access to secure areas

All network equipment (including, but not limited to WAN service termination equipment, routers, switches, cabling patch panels) will be kept in appropriate locked facilities whenever practicable. All network equipment outside of designated communication rooms must be kept securely. School workforce must ensure that communications cabinet and communications room doors are secured when they are left unattended. All keys must be limited to those who need them to carry out their duties. If any key is lost or mislaid, or any door found unlocked, then this must be reported immediately as an IT security incident.

All physical servers are kept physically secure in an area for authorised individuals only. A process of allocating and monitoring access to server rooms/areas must be implemented – this may include electronic access control or the use of signing in books as appropriate.

15. Policy compliance

The School requires that all schools' workforce comply with the directives presented within this policy. This policy will be included within the Internal Audit Programme, and compliance checks will take place to review the effectiveness of its implementation.

16. Exceptions

In the following exceptional cases compliance with some parts of the policy may be relaxed. The parts that may be relaxed will depend on the particular circumstances of the incident in question.

- If complying with the policy would lead to physical harm or injury to any person
- If complying with the policy would cause significant damage to the School's reputation or ability to operate
- If an emergency arises

In such cases, the user concerned must take the following action:

- Ensure that their manager is aware of the situation and the action to be taken
- Ensure that the situation and the actions taken are recorded in as much detail as possible on a non-conformance report

- Ensure that the situation is reported to the Office and IT Managers as soon as possible.
- Failure to take these steps may result in disciplinary action.

The School will not take disciplinary action in relation to known, authorised exceptions to the information security management system.

17. Penalties

Non-compliance is defined as any one or more of the following:

- Any breach of policy statements or controls listed in this policy
- Unauthorised disclosure or viewing of confidential data or information belonging to the School or partner organisation
- Unauthorised changes to information, software or operating systems
- The use of hardware, software, communication networks and equipment, data or information for illicit purposes which may include violations of any law, regulation or reporting requirements of any law enforcement agency or government body
- The exposure of the School or partner organisation to actual or potential monetary loss through any compromise of security
- Any person who knows of or suspects a breach of this policy must report the facts immediately to the Information Security Officer or senior management.

Any violation or non-compliance with this policy may be treated as serious misconduct.
Penalties may include termination of employment or contractual arrangements, civil or criminal prosecution.