OUR LADY OF LOURDES

CATHOLIC MULTI-ACADEMY TRUST

Systems Access Policy

Nottingham Diocese Multi Academy Trusts

CATHOLIC SCHOOLS Moving Forward Together

Issue Date	May 2024
Review Date	May 2027
Reviewer	Audit & Risk Committee/OLOL Exec Board
Author	Will Ottewell – Director of IT
Version	1.0

Purpose

The purpose of this Access Control Policy is to establish guidelines and procedures for granting, modifying, and revoking access to computer systems and information resources within Our Lady of Lourdes CMAT or any of its Academies. This policy aims to ensure the confidentiality, integrity, and availability of sensitive information and resources while promoting a secure computing environment.

Scope

This policy applies to all employees, contractors, vendors, and third-party users who have access to Our Lady of Lourdes CMAT or one of its Academies' computer systems and networks.

Access Control Principles

Least Privilege

Access to systems and information will be granted with the principle of least privilege. Users will be given the minimum access necessary to perform their job responsibilities. This includes local administrative access to devices.

Need-to-Know

Access to specific information and systems will be granted based on an individual's job role and the requirement to know the information to perform their duties.

Accountability

Each user is responsible for the actions performed under their assigned account. Users are prohibited from sharing login credentials.

Authentication and Authorization

Users must authenticate their identity through secure and unique credentials. Authorization will be based on the principle of least privilege and will be granted only after proper authentication.

Access Control Procedures

User Account Management

1) User accounts will be created, modified, and deactivated by the Trust IT Team, contracted IT support organisation or automatically via authorised systems integrations in accordance with HR records, MIS records and relevant roles.
2) Account passwords must meet Our Lady of Lourdes CMAT's password complexity requirements, based upon the recommendations of NCSC.

3) User access rights will be reviewed on a periodic basis to ensure alignment with job responsibilities.

Access Request Process

1) Job roles will be assigned a standard level of access to systems.
2) For additional systems access, all access requests must be submitted through the Trust access request form.
3) Access requests will be approved by the user's supervisor or department head before being processed by the IT department.
4) Requests for elevated privileges will be subject to additional scrutiny and require approval from the Trust IT Director or Trust IT Network and Support Managers.
5) General staff will not have administrative access to computers or systems.

Access Revocation

1) Access to systems will be promptly revoked upon termination of employment, change in job role, or any other change in status that necessitates access modification.
2) Immediate access revocation will be enforced for any user found violating security policies.

Monitoring and Auditing

Access Logs

1) Access logs will be regularly reviewed to detect and investigate any unauthorized access or suspicious activity.
2) Monitoring tools will be implemented to track and analyze user activity within the network.

Periodic Audits

1) Periodic security audits will be conducted to ensure compliance with this policy.
2) Any discrepancies or violations discovered during audits will be addressed promptly.

Enforcement

Violations of this Access Control Policy may result in disciplinary action, up to and including termination of employment or legal action, depending on the severity of the breach.