

Cyber Security Policy

St Michael's Catholic Grammar School



Founded by the Sisters of the Poor Child Jesus, in the trusteeship of St Michael's Catholic School Trustee and a member of the Loreto Education Trust.

Approved by: Headteacher (Head of Centre)

Date: October 2026

Next review due by: October 2027

Contents

1. Introduction	2
2. Scope	2
3. Roles and responsibilities	3
4. Technical Security Measures	3
5. User Account Management	4
6. Staff training and awareness	4
7. Incident Response Plan	4
8. Compliance and Auditing	4
9. Policy Review	4
10. Links to other policies	4

1. Introduction

St Michael's Catholic Grammar School is committed to safeguarding its information assets, IT systems, and the personal data of students, staff, and stakeholders from cyber threats. This policy sets out our approach to cyber security, outlines roles and responsibilities, and ensures compliance with relevant UK legislation, including the Data Protection Act 2018, UK GDPR, and Keeping Children Safe in Education guidance.

2. Scope

This policy applies to [all staff, students, governors, and any third parties] who have access to St Michael's Catholic Grammar School's IT systems and data.

3. Roles and Responsibilities

Role	Responsibilities
Head of Centre	Overall responsibility for policy implementation and cyber security strategy.
IT Manager/Team	Peter Zeelie (and Connect Systems) Implement technical controls, monitor systems, respond to incidents, manage access and updates.
Data Protection Officer	Neil Hinnem Ensure compliance with data protection law, advise on data handling, and oversee data breaches.
All Staff	Follow this policy, complete annual training, report incidents or concerns promptly within the centre.
Governors	Oversee and review cyber security arrangements and policy compliance.
Students/Users	Use IT systems responsibly and report any concerns.

4. Technical Security Measures

St Michael's Catholic Grammar School implements the following security measures, scaled to our size and needs:

- Firewalls and network security controls.
- Anti-virus and anti-malware software on all devices.
- Regular software updates and patch management.
- Secure data backup and tested recovery procedures.
- Encryption for sensitive and personal data.
- Multi-factor authentication (MFA) for critical systems and remote access (implemented 2027-27)
- Secure configuration and monitoring of cloud services (e.g., Office 365, Google Workspace).
- Prompt removal of access for leavers.

5. User Account Management

Password governance must follow NCSC Guidance:

- o <https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/three-random-words>
- o <https://www.ncsc.gov.uk/collection/passwords/updating-your-approach>

Access control and permissions are based on job roles and reviewed regularly.

Accounts are promptly disabled when users leave.

Account activity is monitored and audited.

6. Staff Training and Awareness

All staff must complete annual cyber security training and annual refresher training.

- o Phishing awareness and social engineering defence training.
https://www.ncsc.gov.uk/section/education-skills/cyber-security-Centres#section_17.

Records of cyber training must be retained for all staff and be available for inspection.

7. Incident Response Plan

All staff members must report any suspected security incidents or concerns to the Schools' Business Manager immediately.

- a. Steps for identifying and reporting incidents: Alert SBM ASAP
- b. Incident response team: SLT
- c. Communication plan for stakeholders – Depends upon issue and extent, could be governors, parents, students, staff, National Cyber Security Centre (NCSC).
- d. Include referral to awarding organisation(s) (if applicable)
- e. Post-incident review process: Conduct a review to identify lessons learned and update procedures if necessary.

8. Compliance and Auditing

Annual review and update of this policy and periodic auditing by SBM

9. Policy Review

This policy will be reviewed annually by the SBM and updated as necessary to reflect changes in technology, threats, and best practices.

This policy will be ratified by the headteacher

10. Links to other policies

This policy links to the following policies and procedures:

Economic and Business Continuity Policy