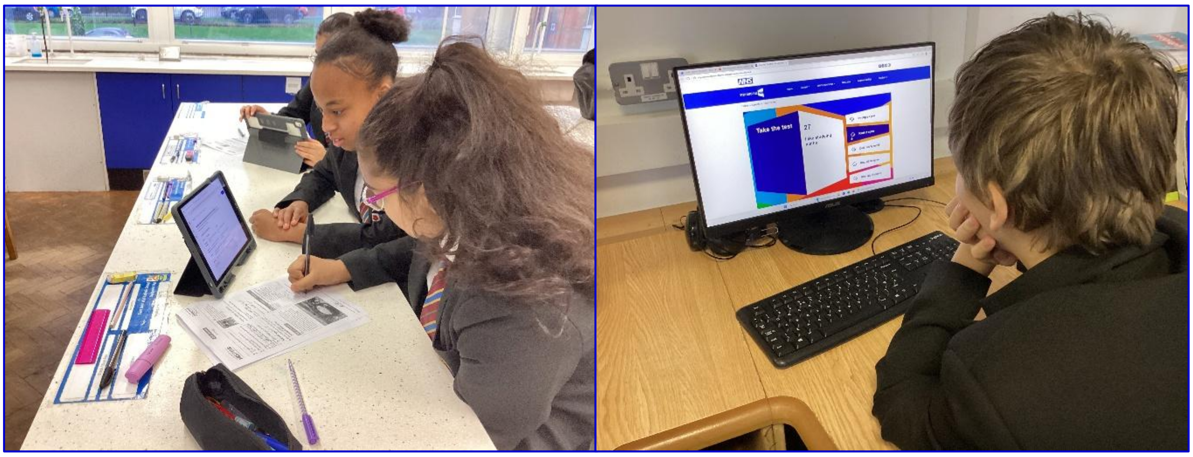
Saint John Wall Catholic School

A Catholic School For All

FORTES IN FIDE

Mission Statement

‘To educate each and every unique child in our care to hear and respond to what God calls them to be’



Cyber Security Policy

Teach me knowledge and good judgment, for I trust your commands.
Psalm 119:66

1. Introduction

Saint John Wall Catholic School is committed to safeguarding its information assets, IT systems, and the personal data of pupils, 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, pupils, governors/trustees, contractors (including peripatetic and supply staff), volunteers, visitors using school networks, and any third parties who access Saint John Wall Catholic School IT systems, services, or data (including cloud services and remote access).

3. Roles and Responsibilities

Role	**Responsibilities**
Head of Centre	*Katherine Marston* *Overall responsibility for policy implementation and cyber security strategy.*
IT Manager/Team	Mariusz Wieremiewicz *Implement technical controls, monitor systems, respond to incidents, manage access and updates.*
Data Protection Officer	Kelly Chohan Mariusz Wieremiewicz (cover) *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.
Pupils/Users	Use IT systems responsibly and report any concerns.

4. Technical Security Measures

Saint John Wall Catholic 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.

- Secure configuration and monitoring of cloud services (e.g., Office 365).
- Prompt removal of access for leavers.

5. User Account Management

- Password governance must follow NCSC Guidance:
    - https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/three-random-words
    - 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.
- 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 Paul Holden/Kelly Chohan/Mariusz Wieremiewicz immediately.

- **Dealing with Cyber/Data breaches**
- Examination data must be handled in line with the centre's data protection procedures (UK GDPR/DPA 2018) and the requirements of the relevant awarding organisation(s), including any applicable JCQ instructions/guidance.
- **Notification of breach**
  Where a personal data breach is suspected, the DPO will assess the risk and determine whether ICO notification is required (and if so, it will be made without undue delay and, where feasible, within 72 hours); affected individuals will be informed where required so they can take protective steps.
- **Evaluation and response**
  Once a Cyber/Data breach has been resolved, a full investigation of the incident will take place as per policy procedures on GDPR.

8. Compliance and Auditing

- Annual review and update of this policy
- Regular internal audits

9. Policy Review

- This policy will be reviewed annually by a member of the Senior Leadership Team and updated as necessary to reflect changes in technology, threats, and best practices.
- This policy will be ratified by Governors.

Ratified by Governors: 09/03/2026
Review Date: 09/03/2027
(This policy will remain in force beyond the review date if no updates are required)