St. Patrick's Catholic Primary School

Our Mission in St Patrick's is to develop each child's talents and potential in a caring Catholic community inspired by the teachings of Jesus.

Safeguarding Children in Education

Technical Security Policy

(including Access, Device and Incident Management)

At Saint Patrick's Catholic Primary School, we seek to create a unique and enabling community whereby children and staff are encouraged to journey beyond their expectations – academically, socially and spiritually – within a culture based on Gospel Values.

Purpose

This policy sets out how the school protects its technical infrastructure, systems and devices to ensure a secure and resilient digital environment. It supports safeguarding, data protection and business continuity and aligns with the DfE Digital and Technology Standards

Scope

This policy applies to:

- Staff, learners and governors
- Suppliers of third-party services and solutions
- School networks, servers and cloud systems
- School-owned devices
- User accounts and access controls
- Device configuration and management, including personal devices where permitted

Policy Statement

The school will ensure that its technical systems are managed in a way that:

- Protects users and data from unauthorised access or misuse
- Supports safe and reliable access to digital services
- Enables detection, response and recovery from technical incidents
- Is proportionate to risk and regularly reviewed

Access Control and Authentication

The school will ensure that:

- All users have unique accounts with appropriate access rights

- New user rights are allocated as part of induction
- Access is removed promptly when users leave the school
- Passwords and authentication methods reflect NCSC and DfE guidance
- Multi-factor authentication is used in accordance with DfE/NCSC requirements, particularly for privileged, administrative, remote-access and sensitive systems.
- Administrator access is restricted and monitored
- System administrators and those with global/ confidential data system access use a physical security device in addition to MFA to access systems.

System Security and Maintenance

The school will ensure that:

- Systems and software are licensed, supported and kept up to date
- Security patches are applied promptly
- Anti-virus and malware protection is in place across all systems
- Backups are taken regularly, stored securely (both locally and offsite, with rotation) and regularly tested
- Physical access to infrastructure is controlled

Device Management

The school will ensure that:

- Clear expectations exist for the use of school-owned and personal devices
- School-owned devices are centrally managed wherever practicable, allowing control over configuration, software, applications, security updates and access to content.
- Where personal devices are permitted to connect to school networks under an authorised exception, appropriate filtering and monitoring controls will apply where technically possible and proportionate.
- Where personal devices are permitted, their use is clearly authorised, risk-assessed and consistent with the school's Behaviour, Mobile Phone and Acceptable Use policies. Learners will not normally have access to personal mobile phones or equivalent smart devices during the school day, except where an authorised exception applies.
- Authorised exceptions, including those relating to medical needs, SEND, accessibility or safeguarding, are appropriately managed without weakening wider technical or safeguarding controls.
- School devices are configured securely and managed appropriately, with regular/ automatic patches and updates
- Where personal devices are permitted, expectations are clearly defined and risk-assessed
- Acceptable Use Agreements reference responsible device use
- Users receive guidance on safe and appropriate device use

Supplier Management

The school will ensure that:

- Provision of third-party services and solutions are adequately contracted and regularly reviewed
- Suppliers can demonstrate adherence to school policy and alignment with the DfE Digital and Technology Standards

Incident Management

Technical incidents will be logged, escalated and reviewed. Serious incidents will be managed in line with safeguarding and business continuity procedures.

Review and Training

Technical security arrangements will be reviewed regularly. Staff with specific responsibilities will receive appropriate training, and users will be educated on their responsibilities.

Technical controls will be reviewed in response to changes in legislation or national requirements relating to children's access to online services.

POLICY REVIEW

The Governing Body will undertake an annual review of the school's Filtering and Monitoring Policy and remedy any deficiencies or weaknesses found without delay. The names Governing Body member to contact with any concerns regarding the Technical Security Policy is Mrs. Charlotte Gilbert

Policy dated: October 2026

Date of next review: October 2027