

St. Mary's College Junior School



Cybersecurity Awareness Policy

Purpose

This policy aims to ensure that all members of our school community, including students, staff, and parents, are aware of and understand the importance of cybersecurity. It outlines guidelines and procedures to protect our digital systems and data from cyber threats.

Scope

This policy applies to all staff, students, contractors, volunteers and anyone with access to our systems and hardware.

Objectives

- Education and Awareness: Provide regular training and awareness programs to educate students and staff about cybersecurity risks and best practices.
- Data Protection: Ensure all data is stored securely and backed up regularly.
- Network Security: Implement robust network security measures to prevent unauthorised access.
- Incident Response: Develop a plan to handle cybersecurity incidents effectively.

Key Principles

1. User Awareness and Training:

Conduct regular cybersecurity awareness training for staff and students.

Educate students about online safety, including recognising phishing scams and maintaining privacy.

2. Password Policy:

Enforce strong, unique passwords for all accounts.

Consider using a password manager and enable multi-factor authentication (MFA) where possible.

3. Network Security:

Use a fit-for-purpose router and firewall to prevent unauthorised access.

Regularly update software and systems to protect against vulnerabilities.

4. Prevention:

Install anti-virus software on all devices and update regularly.

Discourage using USB ports unless strictly necessary.

5. Data Backups:

Create regular backups of all critical data.

Use cloud storage solutions for secure data management.

Roles and Responsibilities

- Principal: Oversee policy implementation and ensure compliance.
- ICT Coordinators: Manage ICT systems, monitor network activity, and provide technical support.
- Data Protection Officer: Ensure data protection compliance and handle data-related incidents.

Incident Response Plan

- Reporting Incidents: Establish clear procedures for reporting cybersecurity incidents.
- Response Team: Designate a team to handle incidents, including ICT staff and the school's external ICT partners GDK.
- Communication: Develop a plan for communicating with parents and stakeholders in case of a breach.

Review and Update

- This policy was adopted by the Board of Management in April 2026 and will be reviewed every 3 years or sooner if deemed necessary to ensure that it remains effective and aligned with current best practices.