



ST. MARY'S *Catholic High School, Dubai*

CYBER SECURITY POLICY

2025-2026

St. Mary's Catholic High School, Dubai

At St. Mary's Catholic High School, Dubai, we believe that every child has the right to learn in a safe and caring environment without fear of being bullied. By having a written policy outlining the definition of Cyber- Bullying in all its forms, we believe that we are taking the first and most essential steps to tackling bullying and ensuring the school creates a safe learning environment where risk of harm is minimized and students feel socially and emotionally secure.

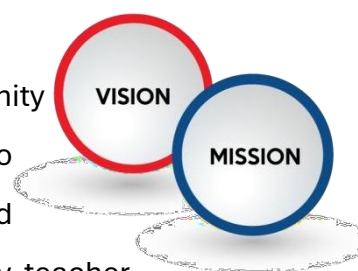
As with all the policies of the school, we believe that our stated mission and vision for the next five years underlies the ethos of the school and underpins everything that the school stands for,

MISSION STATEMENT

We serve with compassion to develop a deep sense of integrity, mutual respect and tolerance within the Marian family so that the uniqueness of each person is celebrated, allowing them to holistically develop as successful learners and responsible citizens.

VISION:

Within the next 5 years, we envision ourselves as a school community that consistently strives to develop highly independent learners who confidently showcase innovation through meaningful reflection and purposeful collaboration. We aim to achieve this by ensuring every teacher inspires students through effective questioning and feedback to reach their highest potential in a culturally diverse society.



Objectives:

This policy has been developed in order to ensure that all stake holders including the students, teachers, senior leadership team and other members are well versed and aware of how to report cyber-bullying and what to do in the event that cyber-bullying is reported. The school also makes it clear that cyber-bullying is not tolerated and when dealing with cyber-bullying there is a clear message that the offender will be firmly dealt with.

Cyber Security Policy

1. Introduction

In today's digital age, technology plays a vital role in teaching, learning, administration, and communication at **St. Mary's Catholic High School, Dubai**. While digital technologies provide significant educational and operational benefits, they also introduce cyber security risks that must be effectively managed.

This Cyber Security Policy establishes the principles, responsibilities, and controls required to protect the school's digital environment. The policy supports student wellbeing, safeguarding, and responsible digital citizenship while ensuring the confidentiality, integrity, and availability of information systems.

This policy aligns with the **Knowledge and Human Development Authority (KHDA) guidelines**, applicable **UAE laws and regulations**, and recognized international cyber security best practices.

2. Purpose

The purpose of this policy is to:

- Protect student, staff, and school data from cyber threats
- Ensure safe and responsible use of digital technologies
- Support safeguarding and wellbeing of students
- Prevent, detect, and respond to cyber security incidents
- Ensure compliance with KHDA expectations and UAE regulations

3. Scope

This policy applies to:

- All students
- All teaching and non-teaching staff
- School leadership and management
- Contractors, vendors, and third-party service providers

It covers:

- School-owned devices and infrastructure
- Personal devices accessing the school network
- Cloud-based platforms and learning systems
- Wired and wireless networks
- Data stored, processed, or transmitted by the school



4. Policy Framework and Alignment

This policy is informed by:

- KHDA Wellbeing and Safeguarding Framework
- UAE Cyber Security best practices
- NESAs (National Electronic Security Authority) principles
- ISO/IEC 27001 Information Security Management guidance
- Child online protection standards



5. Governance, Roles, and Responsibilities

5.1 School Management

- Approve and oversee cyber security policies
- Ensure adequate resources and support
- Promote a culture of cyber safety and compliance

5.2 IT Department

- Implement and maintain cyber security controls
- Monitor systems and network activity
- Manage vulnerabilities and cyber incidents
- Report security posture and risks to management

5.3 Staff

- Use school systems responsibly and securely
- Protect login credentials and sensitive information
- Complete required cyber security training
- Report suspected cyber security incidents immediately

5.4 Students

- Follow the Acceptable Use Policy
- Use technology safely, ethically, and respectfully
- Report cyberbullying or online safety concerns



6. Cyber Security Monitoring and SOC Operations

St. Mary's Catholic High School uses **CDC-ON**, a Security Operations Centre (SOC) platform, to enhance cyber security monitoring and threat detection across the school network.

Through CDC-ON:

- Network and system activity is continuously monitored
- Cyber threats and vulnerabilities are identified proactively
- **Monthly cyber security reports** are generated
- **Vulnerability alerts and notifications** are received in real time

These alerts enable the IT team to **immediately investigate, remediate vulnerabilities, and reduce risk**, ensuring a proactive and responsive cyber security posture.

7. Data Protection and Privacy

- All personal and sensitive data is classified as confidential
- Data access is restricted on a need-to-know basis
- Personal data is protected against unauthorized access, loss, or disclosure
- Secure storage and approved platforms are used for data processing
- Data handling complies with KHDA requirements and UAE data protection laws



8. Access Control and User Authentication



- Unique user accounts are issued to staff and students
- Strong password standards are enforced
- Multi-Factor Authentication (MFA) is implemented where applicable
- Access rights are reviewed periodically
- User access is revoked promptly upon leaving the school

9. Device and Network Security

- School-owned devices are secured with:
 - Antivirus and endpoint protection
 - Automatic operating system and software updates
 - Firewalls and secure network configurations are maintained
 - Staff and student networks are logically separated
 - Internet content filtering is enabled to protect students from harmful content
-

10. Acceptable Use of Technology

- School systems are to be used for educational and administrative purposes only
- Users must not:
 - Access or distribute inappropriate material
 - Bypass security controls
 - Install unauthorized software or hardware
- Monitoring of systems and internet usage may be conducted to ensure safety and compliance

11. Student Online Safety and Safeguarding

- The school promotes responsible digital citizenship
 - Students receive guidance on:
 - Online safety and privacy
 - Respectful digital communication
 - Cyberbullying awareness
 - Cyberbullying or misuse of technology is addressed through safeguarding and disciplinary procedures
- 
- A green rectangular sign with rounded corners and a yellow pushpin at the top right. The sign contains the text "Be smart on the internet" in a bold, white, sans-serif font. To the right of the sign is a cartoon illustration of a laptop with a yellow screen and a red cord, with a white computer mouse on the cord.



12. Incident Management and Reporting

Cyber security incidents include, but are not limited to:

- Data breaches or data loss
- Malware or ransomware attacks
- Phishing or social engineering attempts
- Unauthorized access to systems

All incidents must be reported immediately to the IT Department.

Incident response includes:

- Identification and containment
- Investigation and documentation
- Communication with school leadership
- Recovery and preventive measures



13. Backup and Disaster Recovery



- Regular backups of critical systems and data are performed
 - Backups are stored securely
 - Disaster recovery procedures are tested periodically
 - Business continuity plans are maintained to minimize disruption
-

14. Third-Party and Vendor Security

- Third-party service providers must comply with school security requirements
 - Access to systems is limited to business needs
 - Data protection and security obligations are included in contracts
-

15. Training and Awareness

- Staff receive regular cyber security awareness training
 - Phishing and threat awareness information is shared periodically
 - Students receive age-appropriate digital safety education
 - Parents are encouraged to support cyber safety at home
-

16. Compliance, Monitoring, and Enforcement

- Compliance with this policy is mandatory
 - Systems may be monitored to ensure security and safeguarding
 - Breaches of this policy may result in disciplinary action
 - Regular reviews and audits are conducted
-

17. Policy Review and Maintenance

This policy will be reviewed **annually** or following:

- A significant cyber security incident
 - Regulatory or KHDA updates
 - Major changes to school systems or infrastructure
-

Approved by: School Management

Next Review Date: June 2026