GLENDALE INTERNATIONAL SCHOOL

Cyber Security Policy

Version History

Ver. No.	Authors	Date	Reviewer	Next Review Date
1.0	IT Department	Aug 2023	School Board/ Governing Body	Aug 2024
1.1	IT Department	Aug 2024	School Board/ Governing Body	Aug 2025
1.2	IT Department	Aug 2025	School Board/ Governing Body	Aug 2026

1. Policy Statement

Glendale International School recognizes that cybersecurity is critical to safeguarding students, staff, information assets, and school operations. The school is committed to maintaining a secure, reliable, and resilient digital environment that supports learning, safeguarding, and effective administration.

This policy establishes clear expectations, controls, and procedures to protect Glendale's digital systems from cyber threats while enabling safe and responsible use of technology across the school community.

2. Purpose

The purpose of this policy is to:

- Protect the confidentiality, integrity, and availability of school data and systems
- Reduce the risk of cyber incidents that could disrupt learning or compromise safeguarding
- Define roles, responsibilities, and acceptable behaviour when using technology
- Ensure compliance with UAE laws and regulatory expectations for schools in Dubai

3. Scope

This policy applies to:

- All users: students, staff, leadership, contractors, vendors, and visitors
- All devices and systems:
    - School-owned devices

  - Personally owned devices (BYOD)
  - Cloud platforms, applications, and network services
- Any access to Glendale International School's network, systems, or data, whether on-site or remote

4. Cybersecurity Governance

Cybersecurity at Glendale International School is overseen through a shared governance model:

- **School Leadership Team (SLT):** Strategic oversight, risk acceptance, and escalation decisions
- **IT Department:** Implementation of security controls, monitoring, incident response, and technical compliance
- **Staff and Students:** Responsible use of systems and immediate reporting of concerns

Cybersecurity risks that may impact safeguarding, examinations, or school continuity are escalated to SLT without delay.

5. Responsible Use of Technology

All users must:

- Use school technology and internet access strictly for educational and professional purposes
- Act responsibly, respectfully, and legally when using digital systems
- Avoid accessing, creating, or sharing inappropriate, offensive, or unauthorised content
- Respect intellectual property and software licensing rules
- Refrain from cyberbullying, harassment, or malicious digital activity

Failure to comply may result in restricted access, disciplinary action, or further consequences under school procedures.

6. Common Cyber Threats

Glendale International School actively manages risks including:

- Data breaches involving student or staff information
- Phishing and social engineering attacks
- Malware and ransomware infections
- Denial of Service (DoS) attacks impacting system availability
- Security weaknesses caused by unpatched or outdated software
- Risks introduced through removable storage devices

7. Network and System Security

7.1 Network Protection

The school maintains layered security controls, including:

- Enterprise firewalls and traffic filtering
- Segregated networks for Students, Staff, and Guests
- Secure configuration of core network devices
- Encrypted communication between critical systems

7.2 Wi-Fi Security

- Separate wireless networks for students, staff, and guests
- Authentication controls applied to managed networks
- Guest access is limited and isolated from internal systems

8. Account and Access Management

- Every user is assigned a unique account
- Passwords must meet defined complexity standards
- Sharing of credentials is strictly prohibited
- Access rights are reviewed periodically and removed when no longer required

9. Device Management

9.1 School-Owned Devices

- Managed centrally by the IT Department
- Protected with antivirus and endpoint security tools
- Users must not disable or bypass security controls

9.2 Bring Your Own Device (BYOD)

- Devices must meet minimum security requirements before network access
- Updated operating systems and antivirus software are mandatory
- The school reserves the right to restrict or remove access if a device poses a risk

10. Data Protection and Privacy

Glendale International School handles personal and sensitive data in accordance with UAE Data Protection laws.

Key principles include:

- Data minimisation and role-based access
- Use of school-approved platforms for storage and sharing
- Secure handling of student and safeguarding-related information

11. Monitoring and Filtering

- Network activity is monitored to detect threats and misuse
- Web filtering is applied to support safe and age-appropriate access
- Monitoring is conducted to protect users, systems, and the school

12. Cyber Incident Management

All suspected cyber incidents must be reported immediately to the IT Department.

Examples include:

- Malware or ransomware detection
- Suspicious emails or phishing attempts
- Unauthorised account access
- Loss or theft of school devices

Incident Response Process

1. Identification and containment
2. Risk and impact assessment
3. System recovery and restoration
4. Review and corrective action

13. Awareness and Training

- Regular cybersecurity awareness sessions for staff and students
- Induction training for new staff
- Periodic reminders and practical guidance

Cybersecurity awareness is treated as part of the school's overall safeguarding and safety culture.

14. External Access and Vendors

- Visitors are issued restricted guest network access only
- Guest traffic is isolated from internal systems
- Vendors and contractors must:

- Access only approved systems
- Follow school security requirements
- Sign Non-Disclosure Agreements (NDAs) where required

15. Legal and Regulatory Compliance

Glendale International School complies with applicable UAE regulations, including:

- UAE Cybercrime Law
- UAE Data Protection Law
- Child protection and safeguarding legislation

Serious breaches may be reported to relevant authorities where legally required.

16. Breaches and Disciplinary Action

Breaches of this policy may result in:

- Suspension or removal of system access
- Disciplinary action for staff or students
- Contract termination for vendors
- Legal action in line with UAE law

17. Policy Review

This policy is reviewed annually or following:

- Major cyber incidents
- Significant technology changes
- Updates to legal or regulatory requirements

This Cyber Security Policy supports Glendale International School's commitment to safe, secure, and responsible use of technology in line with expectations across Dubai schools.