Greenwood International School
Cyber-Security Policy

- Date: 16/09/2025
- Author: IT Department
- Revised by: Senior Leadership Team
- Policy Type: School Operations
- Circulation: Internal & External
- Date authorized: 09/2025
- Authorized by: The Principal
- Date of next review: 09/2026

This Cybersecurity Policy for Greenwood International School (GIS) covers essential areas of data protection, network security, user access, and incident response.

Cybersecurity Policy for GIS

1. Purpose

This Cybersecurity Policy aims to provide guidelines and procedures that help safeguard the school's information systems, data, and network resources from cyber threats, unauthorized access and misuse. It ensures that the school complies with applicable laws and regulations, upholds the privacy and safety of students and staff, and fosters a secure digital learning environment.

2. Scope

This policy applies to all students, faculty, staff, contractors, volunteers, and any other individuals who access the school's information systems, including networks, servers, computers, and mobile devices. It covers all digital data, systems, and resources owned or managed by GIS.

- ICT Labs, school-owned devices (laptops, tablets), and personal devices (BYOD).
- All platforms (LMS, student portals, emails, cloud tools).
- Networks, servers, and data stored on-premises or in cloud services.

3. Governance and Responsibilities

- Cybersecurity Committee: The Cybersecurity Committee oversees the execution of this policy and gives its reviews on a timely basis. It is composed of IT staff, administrators, and security experts.

- Information Technology Department: The IT department takes up the role of keeping the school's networks, systems, and devices secure with appropriate cybersecurity measures.

- Users: Users shall follow the policy, report suspicious activity, and undergo required cybersecurity training.
    - Report suspicious activity (phishing emails, unauthorized access) to IT via email: it@greenwood.sch.ae, mustafa.ahmed@greenwood.sch.ae, harikrishnan@greenwood.sch.ae, fadi@greenwood.sch.ae,
    - Complete mandatory annual cybersecurity training.

4. Data Protection and Privacy

- Student Data: The school follows all relevant legislation about student data privacy protection. Student information such as grades and personal information will be stored securely using encryption methods.
- Staff Data: The personal data collected from all staff members is safeguarded in accordance with the applicable privacy laws and internal rules.
- Third-Party Vendors: All the contracts involving third-party vendors that deal with sensitive school data must contain provisions about data security and compliance with appropriate laws.
    - All passwords are encrypted and can't be retrieved without admin support.
    - Access is restricted to authorized staff only.
    - Third-Party Platforms (Google Workspace, Microsoft 365).
    - Vendors must comply with GDPR/FERPA and provide annual security audits.
    - Data backups are performed daily.

5. Network Security

- Firewall Network Segmentation: The network of the school is protected with a security system and is segmented into smaller partitions so that sensitive systems are not located near general access areas.
- Wireless networks: All wireless networks are secured by strong encryption, such as WPA2. Access is strictly provided to personnel and students.
- Antivirus/anti-malware protection: Each school-owned device has updated antivirus/anti-malware software to protect against malicious threats.
- ICT Labs:
    - Segmented from the main network, lab devices cannot access administrative systems.
    - Firewalls and intrusion detection systems (IDS) deployed.
- Wireless Networks:
    - Staff/Student Wi-Fi: WPA2 encryption; separate VLANs for BYOD and school devices.
    - Antivirus: Endpoint protection enforced on all staff school devices.

6. User Access and Authentication

- User Accounts: Each user has a user account, which is used for tracking access and accountability purposes. Sharing of credentials for user accounts is strictly not allowed.
- Authentication Methods: MFA is utilized to access sensitive systems and data.
- Role-Based Access: Data and system access is restricted, where feasible and reasonable, to job roles and responsibilities with the principle of least privilege applied to reduce unnecessary access.
- Accounts:
  - Unique accounts for all users (students: *studentID@greenwood.sch.ae*; staff: *name@greenwood.sch.ae*).
  - No credential sharing, violations result in immediate account suspension.
  - Multi-Factor Authentication (MFA)
  - Required for accessing sensitive systems (School Email).
- Role-Based Access:
  - Students: Limited to LMS, reading tools, e-books, Microsoft 365 and lab resources.
  - Teachers: Access to SMS, LMS, Gmail, Microsoft 354, reading tools and e-books.
  - IT Staff: Full administrative privileges.

1. Device Management

- Device Security: Passwords or biometric authentication is required for all devices, from laptops to tablets to smartphones, and must be set to lock after a period of inactivity.
- Bring Your Own Device (BYOD): Students and staff using personal devices are bound by the school's cybersecurity policies and required to install relevant security software on their devices.
- Remote Access: The school's systems should be accessible remotely in a secure manner and should always be subjected to the same security practices as if access was on-site.
- School-Owned Devices:
  - Configured with MDM (Domain, Intune) for remote wipe, encryption, and app control.

- Auto-lock after 5 minutes of inactivity.

- BYOD (Students/Staff):
  - Mandatory installation of GIS-approved antivirus.
  - Devices without security software are blocked from the network.
  - ICT Lab Computers: software installations require IT approval.

BYOD Minimum requirements

- Windows 10 or later, macOS 12+, Android 11+, iOS 15+.

8. Cybersecurity Awareness and Training

- Training Program: Regular cybersecurity training shall be imparted to all students, staff, and faculty to increase awareness about online safety, protection of data, and identification of phishing and other cyber threats.

- Acceptable Use Agreement: All users must sign an acceptable use agreement that outlines the expectations of the school for responsible and secure use of school devices and networks.

- Annual Training:
  - Topics: Phishing simulations, secure use of school platforms, password hygiene.
  - Students: Integrated into ICT curriculum (spotting fake emails).

- Acceptable Use Agreement:
  - Signed digitally by all users via the school portal before accessing any systems.

9. Incident Response and Reporting

- Incident Reporting: All cybersecurity incidents should be immediately reported to the IT department, including potential breaches, malware infections, and suspicious activity.

- Incident Response Plan: The school shall have an Incident Response Plan that prescribes procedures to be followed for containment of the cyber incident, investigation, notification, and remediation.

- Data Breach Notification: If a data breach occurs involving sensitive personal information, then the school shall notify the affected persons in compliance with relevant laws.

- Reporting:
  - Immediate notification to IT via email (it@greenwood.sch.ae, mustafa.ahmed@greenwood.sch.ae, harikrishnan@greenwood.sch.ae, fadi@greenwood.sch.ae,) or hotline (050 7575 832 - 050 3733 977).

- Response Plan:
  - Containment: Isolate affected systems (e.g. disconnect lab devices).
  - Investigation: Logs reviewed from platforms and network traffic.
  - Notification: Parents/staff are alerted within 48 hours of a confirmed data breach.

10. Compliance and Monitoring

- Compliance with Regulations: The School follows the relevant laws and regulations.

- Security Audits: The organization conducts regular security audits and assessments regarding security of systems and their compliance with this policy.

- Monitoring and Logging: The school monitors the network traffic and user activity for potential unauthorized access, cyber-attacks, or other security events. Activities are logged for security purposes.

- Logging:
  - All user activity on (greenwood.sch.ae) platforms monitored; logs retained for 90 days.

11. Enforcement and Disciplinary Action

- Non-Compliance: For any violation of this policy, disciplinary actions such as suspension or termination of access to the school's network, suspension from school activities, or termination of employment may be imposed, depending upon the severity of the violation.

- Legal Consequences: In cases of intentional violation of the policy and damage to systems or data of the school, users may be held liable under the law, which could include criminal prosecution.

- Violations:
  - Students: Loss of device/network access; disciplinary action.
  - Staff: Suspension or termination based on severity.
- Legal Action:
  - Deliberate breaches (e.g., hacking lab systems) reported to UAE authorities.

12. Review and Updates

- This Cybersecurity Policy will be reviewed annually or as needed to account for changes in technology, regulations or the school's needs. Changes in the policy will be communicated to all users.
  - Reviewed annually or after major IT changes (e.g., new platform adoption).
  - Updates communicated via email and the school portal (greenwood.sch.ae).

13. Network Security

- Wireless networks can be upgraded to WPA3 as devices allow, starting with staff networks. Legacy WPA2 devices will be phased out and upgraded/replaced.
- DNS filtering will be applied to block malicious and inappropriate sites for student networks.

14. User Access and Authentication

- MFA should be mandatory for all staff email accounts and SMS portal.

(Easy integration for SSO logins via Authenticator apps - Microsoft Authenticator, Google Authenticator, etc.)

15. Cybersecurity Acceptable Use Checklist (Do's and Don'ts)

Do's

- Use only your assigned school account.
- Create strong passwords and enable MFA.
- Report suspicious emails or activity to the IT department immediately.
- Lock your device when unattended.
- Keep your personal devices updated.
- Use school Wi-Fi networks responsibly and for educational purposes only.
- Respect privacy of others' data.

Don'ts

- Don't share your password with anyone, even friends.
- Don't install unauthorized software on school devices.
- Don't access inappropriate or malicious websites.
- Don't attempt to bypass school firewalls or restrictions.
- Don't plug in unknown USB drives or devices.
- Don't store school data on personal cloud accounts.
- Don't ignore update notifications, always apply them.
- Don't use VPNs on your devices.

Acknowledgment

By using the school's information systems, all users accept responsibility for complying with the requirements of this Cybersecurity Policy.

IT Department Contact Information:
it@greenwood.sch.ae, mustafa.ahmed@greenwood.sch.ae, harikrishnan@greenwood.sch.ae, fadi@greenwood.sch.ae,
Emergency Security Hotline: 050 7575 832 - 050 3733 977