Cyber Security Policy
2024 – 2025

POLICY INFORMATION	
Last review date:	September2024
Reviewed by:	IT Administrator
Next review date:	January 2026
Approved By:	Principal – Daspo Yiappos

Beirut St., Muhaisnah 4
Al Qusais Industrial Area,
Dubai United Arab Emirates
Tel: +97142543666
Website: www.oxford.sch.ae

Policy Statement

THE OXFORD School (TOS) acknowledges that cybersecurity is fundamental to protecting our students, staff, data, and infrastructure.
The school is committed to maintaining a secure digital environment where learning can thrive without disruption or fear of cyber threats.

This policy sets out the standards for safe use of technology, systems security, user responsibilities, monitoring procedures, and incident response.

Purpose:

This Cybersecurity Policy aims to:

- Protect the confidentiality, integrity, and availability of all information assets.
- Safeguard users and systems against unauthorized access, damage, or loss.
- Foster responsible use of technology by all members of the school community.

Scope:

Applies to all users (students, staff, contractors, visitors) and all digital resources including school-owned and personal (BYOD) devices connected to TOS infrastructure.

Roles and Responsibilities:

Role	Responsibilities
Principal & SLT	Overall accountability for cybersecurity measures and policy enforcement.
IT Department	Implementation of technical safeguards, monitoring, incident response.
Staff	Compliance with cybersecurity protocols; reporting breaches immediately.
Students	Adherence to Acceptable Use Policy and responsible use of devices.
Parents	Supervision of child's device usage outside school premises.

Acceptable Use of Technology

All users must:

- Use devices and internet services strictly for educational or work-related purposes.
- Avoid accessing inappropriate, illegal, or unauthorized content.
- Respect intellectual property rights; avoid software piracy or unauthorized downloads.
- Abstain from using the school network to engage in cyberbullying, harassment, or malicious activities.

Breaches may result in suspension of access rights, disciplinary action, and/or legal consequences.

Network Security and Password Policy

1.Password Requirements

- Passwords must be at least 8 characters long with a combination of uppercase, lowercase, numbers, and special symbols.
- Users must not reuse old passwords for at least 3 cycles.
- Passwords must be changed at least once every 90 days.
- Passwords must not be written down or shared.

2.Account Management

- Each user will have a unique ID and authentication credentials.
- Sharing login information or using another person's account is prohibited.

3. Device Management

4.School-Owned Devices

- Pre-installed antivirus and endpoint security software will be maintained by IT.
- Students and staff must not disable, modify, or bypass security configurations.

5. BYOD (Bring Your Own Device)

- Devices must be registered with IT before connecting to school Wi-Fi.
- Devices must have up-to-date antivirus protection installed.
- No mobile data access (SIM/eSIM) allowed during school hours, connection only via secured Wi-Fi.

TOS reserves the right to inspect any BYOD device if policy violations are suspected

6. Internet and Email Use

- Email accounts provided by TOS must be used for official communication only.
- Sending offensive, abusive, or unauthorized mass communications is forbidden.
- Access to social media sites will be restricted during academic hours unless pre-approved.
- Use of VPNs, proxies, or similar tools to bypass school filters is prohibited.

7. Data Protection and Privacy

TOS is committed to protecting personal data by adhering to UAE Data Protection laws:

- Personal information must be collected, stored, and processed securely.
- Staff must use school-approved cloud services (e.g., OneDrive, Google Drive) for storing school data.
- No personal data must be stored on unapproved external devices without IT permission.
- Sharing of personal or sensitive information via unsecured channels is prohibited.

8. Monitoring and Filtering

- TOS deploys firewall filtering, web traffic monitoring, and network access controls to ensure compliance and detect threats.
- Internet traffic on school systems may be monitored without prior notice.

  All activities conducted on school networks are subject to security auditing

9. Incident Management and Reporting

Any suspected cybersecurity incident must be reported immediately to IT Support and DSL if student safeguarding is impacted.

Incident examples:

- Virus or malware infection.
- Unauthorized access to accounts or systems.
- Phishing attacks or suspicious emails.
- Loss or theft of school-owned devices.

IT will conduct investigations, mitigate threats, and if necessary, escalate to SLT or external authorities

10. Cyber Threat Awareness and Prevention

- The school conducts regular cybersecurity awareness sessions for students and staff.
- Mock phishing tests and scenario drills will be organized periodically to evaluate readiness.
- Ongoing reminders about best practices (e.g., strong passwords, safe browsing) will be shared through internal communications.

11. Staff and Student Training

All users must participate in:

- Annual cybersecurity training covering safe technology practices.
- Induction sessions for new joiners.
- Refresher training after major incidents or significant policy updates.

12. External Access and Visitors

- Visitors requiring network access will be issued temporary guest accounts with strict controls.
- Guest network traffic will be isolated from school administrative networks.
- External vendors/contractors must sign Non-Disclosure Agreements (NDAs) before accessing sensitive systems.

13. Compliance with UAE Cyber Laws

TOS will adhere to all relevant federal laws, including:

- UAE Cybercrime Law (Federal Decree-Law No. 34 of 2021)
- Wadeema Child Rights Law (Federal Law No. 3 of 2016)
- UAE Data Protection Law

Breaches leading to criminal offenses will be reported to law enforcement agencies.

14. Breaches and Disciplinary Procedures

Breaches of this policy may result in:

- Loss of system or network access.
- Official warnings.
- Suspension or dismissal (for staff).
- Suspension, exclusion, or expulsion (for students).

Legal action in line with UAE laws

15. Policy Review

- This policy will be reviewed annually by the DGCC and updated based on evolving cyber risks, regulatory changes, and stakeholder feedback.

This Cybersecurity Policy will be:

- Reviewed annually by the IT Manager, DGCC, and Principal.
- Updated following major cyber incidents, technological changes, or amendments to UAE laws.