



المدرسة الهندية النموذجية الجديدة
NEW INDIAN MODEL SCHOOL
رقم التصريح التعليمي ٢٠١٨٦، هيئة المعرفة والتنمية البشرية، دبي، ا.ع.م.
Educational Permit No. 20186, Knowledge & Human Development Authority, Dubai, UNITED ARAB EMIRATES
Affiliation Nos. CBSE: 6630009, Kerala Board: 43092 (Grade 8 to 10); 15004 (Grade 11 & 12)



CYBERSECURITY POLICY

2025-2026



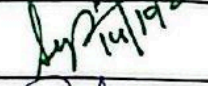
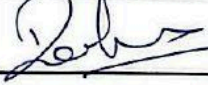
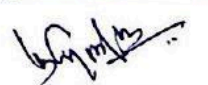
المدرسة الهندية النموذجية الجديدة
NEW INDIAN MODEL SCHOOL
رقم التصريح التعليمي ٢٠١٨٦، هيئة المعرفة والتنمية البشرية، دبي، ا.ع.م.
Educational Permit No. 20186, Knowledge & Human Development Authority, Dubai, UNITED ARAB EMIRATES
Affiliation Nos. CBSE: 6630009, Kerala Board: 43092 (Grade 8 to 10); 15004 (Grade 11 & 12)



CYBER SECURITY POLICY

Review Details	Review 1	Review 2	Review 3
Review Date	March 2025	September 2025	
Review Approved On	March 2025	September 2025	
Date of Next Review	September 2025	December 2025	
Reviewed By	Vice Principal, SLT, DEIW.	Vice Principal. SLT, DEIW	

Approved By

Ms.Supriya Sehgal	Principal	
Dr.Rohit Pramanik	Vice Principal	
Mr.Vinayachandran.M.P	Head of Inclusion	



1. Purpose

The purpose of this policy is to **safeguard the school's digital infrastructure, information systems, and data**, while ensuring the **safety and security of all users** within New Indian Model School, Dubai.

This policy provides **clear guidelines for the responsible, ethical, and secure use of school-owned digital resources**, aligning with **UAE federal regulations, KHDA standards, and international best practices** in cybersecurity and digital safety.

It aims to:

- **Protect sensitive information** from unauthorized access, loss, or misuse.
- **Ensure safe and responsible digital practices** for all students, staff, and stakeholders.
- **Prevent and mitigate cyber threats** including hacking, malware, phishing, and other forms of digital attacks.
- **Promote awareness and accountability** regarding cybersecurity responsibilities across the school community.

2. Scope

This policy applies to all members of the **New Indian Model School, Dubai community** who access, manage, or use school digital resources, including:

- **Students, teaching and non-teaching staff, administrators, and authorized external partners.**
- **All devices connected to the school network**, including desktops, laptops, tablets, mobile phones, smart boards, and IoT devices.
- **School-managed digital platforms**, such as email systems, Google Workspace/Microsoft 365, Learning Management Systems (LMS), school portals, and online assessment or collaboration tools.

This policy governs the **use, access, and management** of these resources, both **on-campus and off-campus**, ensuring safe, responsible, and secure digital practices across the school community.

3. Roles and Responsibilities

To ensure effective implementation of this Cybersecurity Policy, the following roles and responsibilities are defined:

- **Principal** – Oversees the enforcement of the policy, ensures compliance across all school operations, and approves updates or revisions as needed.
- **IT Department** – Maintains network and system security, monitors digital infrastructure, implements software updates, manages user access rights, and responds to cybersecurity incidents.



- **Teachers & Staff** – Utilize school digital resources responsibly, model safe digital practices for students, and report any observed or suspected cybersecurity incidents promptly.
- **Students** – Adhere to acceptable use guidelines, safeguard their login credentials, and immediately report suspicious activities or potential security breaches.
- **Parents/Guardians** – Reinforce responsible digital practices at home, monitor student online behavior, and support the school in promoting safe and ethical use of technology.

4. Acceptable Use

All users of New Indian Model School, Dubai digital resources are expected to follow the principles of **safe, responsible, and ethical use**.

- **Authorized Access:** Users must log in using **school-provided credentials** only.
- **Password Security:** Passwords must remain **confidential** and be updated regularly in accordance with IT guidelines.
- **Prohibited Activities:** The use of school devices, systems, or networks for **illegal, harmful, or inappropriate activities**—including hacking, cyberbullying, or accessing explicit or unauthorized content—is strictly prohibited.
- **Personal Devices:** Personal devices may connect only to the **school's secure guest network** and must comply with all security requirements and guidelines established by the IT department.

5. Data Protection & Privacy

New Indian Model School, Dubai is committed to **protecting the personal and sensitive data** of students, staff, and the school community in accordance with **UAE data protection laws and KHDA guidelines**.

- **Secure Storage:** Personal data of students and staff must be **stored securely** and accessed **only by authorized personnel** for legitimate purposes.
- **Data Sharing:** School data, including personal or confidential information, must **not be shared with third parties** without prior approval from authorized school leadership.
- **Cloud Services Compliance:** All cloud-based platforms and services used by the school must **comply with UAE federal data protection regulations**.
- **Data Backup:** The IT Department will maintain **regular backups** of critical systems and data to prevent loss and ensure business continuity.

6. Network & System Security

To ensure the integrity, availability, and confidentiality of school digital resources, all systems and networks must adhere to the following security standards:



- **Security Tools:** Firewalls, antivirus software, and intrusion detection systems must be **enabled, properly configured, and regularly updated.**
- **Authorized Software:** Only **approved and authorized software** may be installed on school-owned devices.
- **External Storage Devices:** All external storage media, including USB drives, must be **scanned for malware and viruses** before use on school devices.
- **Remote Access:** Any remote access to school systems must occur through **secure VPN connections** and comply with IT department protocols.

7. Cyber Safety & Awareness

New Indian Model School, Dubai is committed to **promoting a culture of cyber safety and responsible digital behavior** across the school community.

- **Training & Education:** The school will conduct **regular training sessions** for staff and students on safe internet use, phishing awareness, and responsible digital citizenship.
- **Cyberbullying & Online Harassment:** Incidents of cyberbullying, online harassment, or any form of digital misconduct will be **addressed promptly under the school's disciplinary framework.**
- **Parental Engagement:** Parents and guardians will be engaged through **workshops and awareness programs** to support safe and responsible digital practices at home.
-

8. Incident Response

To ensure timely and effective handling of cybersecurity incidents, the following procedures apply:

- **Reporting:** All cyber incidents—including phishing attempts, malware infections, unauthorized access, or other suspicious activities—must be **reported immediately** to the IT Department.
- **Investigation & Mitigation:** The IT Department will **investigate, contain, and mitigate** the incident, ensuring that all actions are **thoroughly documented** for accountability and future reference.
- **Escalation:** Serious or high-risk breaches will be **escalated to school leadership** and, where required, reported to **relevant UAE authorities** in compliance with federal regulations and KHDA guidelines.

9. Monitoring & Compliance

To maintain the security and integrity of its digital environment, New Indian Model School, Dubai implements the following measures:

- **Network Monitoring:** The school reserves the right to **monitor the use of its digital resources and network** for security purposes, including detecting unauthorized access, policy violations, and potential threats.



- **Policy Compliance:** All users are expected to adhere to this Cybersecurity Policy. **Violations may result in disciplinary actions**, which can include suspension of digital access, corrective measures in accordance with school policy, or legal action if mandated under UAE law.

10. Review

This Cybersecurity Policy will be **reviewed annually** by the **IT Department in collaboration with the Senior Leadership Team** to ensure:

- Alignment with **current UAE federal cybersecurity regulations** and KHDA standards.
- Adaptation to **emerging cyber threats** and best practices in digital safety.
- Continued effectiveness in **protecting the school's digital infrastructure, data, and users**.

All updates or revisions will be **communicated promptly** to staff, students, and relevant stakeholders.

Policy development committee

Sl. No	Name	Designation
1	Dr. Rohit Pramanik	Vice Principal
2	Mr. Vinayachandran. M. P,	Head of Inclusion
3	Ms. Rishana R.V	School Counsellor
4	Ms. Merin Paul	School Counsellor
5	Mr.Rakesh. K. Nair	IT Administrator



المدرسة الهندية النموذجية الجديدة NEW INDIAN MODEL SCHOOL

رقم التصريح التعليمي ٢٠١٨٦، هيئة المعرفة والتنمية البشرية، دبي، ا.ع.م.
Educational Permit No. 20186, Knowledge & Human Development Authority, Dubai, UNITED ARAB EMIRATES
Affiliation Nos. CBSE: 6630009, Kerala Board: 43092 (Grade 8 to 10); 15004 (Grade 11 & 12)

