مدرسة ايليت الانجليزية ش.ذ.م.م
Elite English School L.L.C

IT Security Policy

Governing Authorities:
Knowledge and Human Development Authority (KHDA)
Ministry of Education (MOE), United Arab Emirates

Review Cycle: Yearly
Last Review: February 2026
Next Review: February 2027

---

1. Introduction

Elite English School Dubai is committed to providing a secure, innovative, and resilient digital learning environment that supports high-quality teaching, learning, and school operations.

Technology plays a vital role in enhancing educational outcomes, communication, and school efficiency. This policy ensures that all digital systems are used safely, responsibly, and securely, while protecting sensitive information and safeguarding all members of the school community.

The policy aligns with:

- KHDA Digital Learning Framework
- UAE Federal Decree-Law No. 45 of 2021 (Personal Data Protection Law)
- UAE Cybersecurity Strategy
- Dubai Economic Agenda (E33)
- Best practice standards followed by British curriculum schools

---

2. Purpose and Objectives

The objectives of this policy are to:

- Ensure the **confidentiality, integrity, and availability** of all IT systems and data.
- Protect personal, academic, and operational information from unauthorised access.

- Promote **safe, ethical, and responsible use of technology** by staff and students.
- Support the secure use of **Artificial Intelligence (AI)** and emerging technologies.
- Develop strong **digital literacy and cybersecurity awareness** across the school.
- Ensure compliance with all KHDA, UAE, and international data protection regulations.
- Support innovation and digital transformation aligned with **Dubai E33 goals**.

---

3. Scope

This policy applies to:

- All staff, students, parents, contractors, and visitors using school IT systems.
- All school-owned devices including laptops, tablets, servers, and network equipment.
- Personal devices accessing the school network (where permitted).
- All digital platforms, cloud services, and educational technologies approved by the school.
- All data created, stored, processed, or transmitted by Elite English School Dubai.

---

4. Governance and Leadership

Responsibility for IT security is shared across the school:

- **IT Manager**
    - Oversees network security, infrastructure, system maintenance, and incident response.
    - Ensures technical compliance with cybersecurity standards.
- **Digital Learning Lead**
    - Supports safe integration of technology and AI into teaching and learning.
    - Coordinates digital innovation and staff training.
- **Senior Leadership Team (SLT)**
    - Ensures compliance with KHDA inspection requirements.
    - Oversees strategic alignment with school improvement priorities and E33 objectives.
- **Annual Audits**

- Regular internal reviews and risk assessments will be conducted to ensure effectiveness and compliance.

---

5. Data Protection and Privacy

Elite English School Dubai is committed to protecting personal data.

- All personal and academic data is stored securely with controlled access.
- Encryption is used where appropriate for sensitive data.
- Access rights are role-based and reviewed regularly.
- Data is processed lawfully, fairly, and transparently.
- The school complies with:
  - UAE Personal Data Protection Law (PDPL)

Data sharing with external service providers (e.g. MIS systems, learning platforms, cloud services) occurs only where:

- A signed Data Processing Agreement (DPA) is in place.
- Providers meet required data protection and security standards.

Parents and staff will be informed about how data is collected, stored, and used.

---

6. Network and System Security

To protect digital infrastructure, the school implements:

- Secure firewalls and intrusion prevention systems.
- Endpoint protection and anti-malware software across all devices.
- Segregated networks for:
  - Staff
  - Students
  - Guests
- Multi-factor authentication (MFA) for sensitive systems.
- Secure password management protocols.
- Regular system updates and patch management.
- Automated data backups with routine restoration testing.

- Monitoring of system logs and network activity to detect potential threats.

---

7. Acceptable Use and Online Safety

All users must:

- Use school systems only for authorized educational or operational purposes.
- Keep usernames and passwords confidential.
- Not attempt to bypass security controls or filters.
- Avoid accessing, creating, or sharing inappropriate content.
- Treat others respectfully in all digital communication.
- Report any suspected breach, loss of device, or unusual activity immediately.

Use of AI tools (such as generative AI platforms) must:

- Be ethical, transparent, and age-appropriate.
- Support learning rather than replace original thinking.
- Comply with the school's AI and Academic Integrity expectations.

---

8. Digital Teaching and Learning

Elite English School Dubai promotes purposeful technology use to enhance learning through:

- Blended learning models.
- Adaptive learning platforms and data-informed instruction.
- Secure online collaboration tools.
- Student digital portfolios and learning evidence.
- Responsible integration of AI to support differentiation and engagement.

Digital citizenship, online safety, and AI ethics are embedded within the curriculum and pastoral programme.

---

9. Professional Development (CPD)

To strengthen digital capacity:

- All staff participate in annual cybersecurity and digital safety awareness training
- The training includes:
    - Cybersecurity awareness
    - Safe data handling
    - AI literacy and ethics
    - Effective use of educational technology
- Training impact is monitored through practice, feedback, and student outcomes.

---

10. Software and Device Management

- Only authorized and licensed software may be installed on school devices.
- All devices must allow automatic updates and security patches.
- The IT Department maintains:
    - An approved software register
    - Asset tracking records
- Third-party platforms are reviewed regularly for:
    - Educational value
    - Data protection compliance
    - Security risk

---

11. Incident Response and Reporting

All security incidents must be reported immediately to the IT Department.

The school maintains a formal **Incident Response Plan**, which includes:

- Immediate containment and risk mitigation.
- Investigation and documentation.
- Notification of affected users where required.
- Reporting to KHDA or relevant authorities when necessary.
- Review and improvement measures to prevent recurrence.

---

12. Monitoring, Evaluation and Impact

The effectiveness of this policy is monitored through:

- System audits and security reviews.
- Usage monitoring and access reports.
- Staff and student feedback.
- Review of digital learning impact on progress and engagement.

Findings contribute to:

- The School Improvement Plan (SIP)
- Digital Strategy and Development Roadmap

---

13. Policy Review

This policy will be reviewed annually or sooner if required due to:

- Changes in legislation or KHDA guidance
- New technologies or cybersecurity risks
- Recommendations from inspections or audits

All updates will be communicated clearly to staff, students, and parents.