



# DUBAI GEM PRIVATE SCHOOL

STRIVE FOR EXCELLENCE

## IT SECURITY POLICY – 2025-2026



Written by:	Ms. Parie Stoneman	Last Review:	October 2025
Position:	Principal	Next Review Date:	October 2026

## **1. Introduction**

Dubai Gem Private School is committed to providing a secure, innovative, and forward-thinking digital learning environment that supports our vision of nurturing confident, responsible, and technologically skilled learners. This policy ensures that our use of technology enhances teaching and learning, protects sensitive information, and aligns with Dubai's E33 Vision to empower a globally competitive and digitally advanced education system.

## **2. Purpose and Objectives**

The objectives of this policy are to:

- Ensure the confidentiality, integrity, and availability of all digital and IT systems.
- Promote safe, ethical, and responsible use of technology among staff, students, and parents.
- Integrate Artificial Intelligence (AI) and emerging educational technologies to improve student engagement and outcomes.
- Build digital capacity through continuous professional development (CPD) for all staff.
- Comply with KHDA's Digital Framework, UAE Data Protection Law (Federal Decree-Law No. 45 of 2021), and international best practices followed by British schools.
- Support E33 goals by fostering digital fluency, innovation, and data-driven decision-making.

## **3. Scope**

This policy applies to:

- All staff, students, parents, and visitors using school-owned devices, systems, or networks.
- All third-party service providers and educational technology partners.
- All data stored, processed, or transmitted through Dubai Gem Private School systems.

## **4. Governance and Leadership**

- The IT Manager oversees system security, compliance, and maintenance.
- The Digital Learning Lead coordinates training, integration of technology into teaching, and AI tools.
- The SLT ensures alignment with KHDA inspection requirements and E33 priorities.
- Annual audits will be conducted to assess compliance, risk, and impact.

## **5. Data Protection and Privacy**

- Personal and academic data are stored securely with restricted access and encryption.
- The school adheres to UAE Data Protection Law and UK GDPR standards.
- Parents, staff, and students will be informed of how data is used and protected.
- Data sharing with external partners (e.g., Alpha ERP, Microsoft Teams, Google Workspace for Education) will occur only undersigned data processing agreements that meet privacy regulations.

## **6. Network and System Security**

- The school employs Sophos Endpoint Detection and Response (EDR) across all devices for real-time protection.
- Segregated networks for staff, students, and guests ensure safe access.
- Firewalls, multi-factor authentication (MFA), and encryption protocols are mandatory for sensitive systems.
- Network logs and activity will be continuously monitored for anomalies or breaches.
- Routine penetration testing and backup reviews will be conducted.

## **7. Acceptable Use and Online Safety**

All users must:

- Access systems only for authorised academic or administrative purposes.
- Avoid sharing passwords or accessing inappropriate content.
- Report any security breach or suspicious activity immediately to the IT Department.
- Uphold the school's values of dignity, integrity, and respect in all online interactions.
- Understand that AI tools (e.g., ChatGPT, Copilot, adaptive learning platforms) must be used ethically, ensuring transparency and originality.

## **8. Digital Teaching and Learning**

Dubai Gem Private School encourages technology integration to transform teaching and learning through:

- Blended and AI-supported learning models (e.g., adaptive platforms, data analytics, virtual labs).
- Teacher-led technology innovation projects to enhance creativity and digital literacy.
- Student digital portfolios to evidence learning progress.
- Continuous evaluation of impact on attainment, progress, and engagement through digital tools.
- Embedding digital citizenship and AI ethics within the curriculum.

## **9. Professional Development (CPD)**

- Staff will participate in annual digital competency training, aligned with KHDA and E33 frameworks.
- Workshops will focus on cybersecurity awareness, AI literacy, edtech integration, and digital assessment tools.
- CPD will be tracked to demonstrate measurable impact on teaching and student outcomes.
- Designated Digital Champions will mentor colleagues and share best practices.

## **10. Software and Device Management**

- Only authorised and licensed software may be installed on school devices.
- Automatic updates and patch management must be enabled.
- The IT department maintains an approved software inventory.
- Regular reviews of third-party apps (Google Workspace, Microsoft Teams, Seesaw, Alpha ERP, etc.) ensure data security compliance.

## **11. Incident Response and Reporting**

- All security incidents, breaches, or suspicious activity must be reported to the IT Manager immediately.
- The school maintains an Incident Response Plan that outlines:
  - Containment and mitigation procedures.
  - Notification of affected individuals and KHDA (if required).
  - Documentation and post-incident analysis to prevent recurrence.

## **12. Monitoring, Evaluation, and Impact**

- The IT team will monitor compliance with this policy through audits, log analysis, and usage reports.
- The SLT will evaluate digital learning impact via:
  - Lesson observations.
  - Student outcomes and engagement metrics.
  - Staff confidence and skill surveys.
- Findings will feed into the School Improvement Plan (SIP) and Digital Strategy Roadmap.

## **13. Policy Review**

This policy will be reviewed annually or when new regulations or technologies emerge. Reviews will consider updates from KHDA, Dubai Digital Authority, and the UAE Cybersecurity Council. All amendments will be communicated to staff, students, and parents.