POLICY OWNER	**Universal Private School - IT Department**
EFFECTIVE DATE	**Upon approval by the School Governing Body**
NEXT REVIEW DATE	**Within 12 months of approval (or earlier if required)**
APPROVAL	**School Governing Body & ADEK (if applicable)**

UNIVERSAL PRIVATE SCHOOL

CYBERSECURITY POLICY

(Aligned with ADEK School Digital Policy)

POLICY STATEMENT

Universal Private School (UPS), Al Ain, is committed to ensuring the confidentiality, integrity and availability of school information systems and to providing a safe digital environment for students, staff, parents and visitors. The school shall implement proportionate cybersecurity controls, safeguard personal information and respond promptly to security incidents.

This policy is aligned with the ADEK School Digital Policy (Version 1.1, September 2024), applicable UAE legislation, and the school's safeguarding and records-management responsibilities. It sets expectations for secure use of school technology; it is a governance document and does not, by itself, demonstrate that every technical control has been implemented.

PURPOSE

The purpose of this policy is to prevent unauthorised access, disruption, data loss and online harm; define responsibilities; establish minimum security standards; and support safe, continuous teaching, learning and school operations.

DEFINITIONS

Cybersecurity	Protection of networks, devices, applications, accounts and information from digital threats.
Personal Data	Information relating to an identifiable student, parent, employee or other individual.
MFA	Multi-factor authentication: a second verification factor in addition to a password.
Least Privilege	Providing users only the access needed for their approved role and duties.
Security Incident	Suspected or confirmed event that threatens the security, privacy or availability of school systems.
IDS/IPS	Intrusion detection/prevention controls that identify and, where enabled, block malicious traffic.
Confidential Data	Restricted school information, including student records, staff files, finance and health information.

1. POLICY OBJECTIVES

- Protect learning and administrative systems from cyber threats and avoidable service disruption.
- Safeguard student, parent and staff information in accordance with legal and ADEK requirements.
- Promote safe online behaviour, awareness and accountability across the school community.
- Ensure that security risks and incidents are identified, escalated, documented and reviewed.

2. SCOPE OF APPLICATION

This policy applies to all staff, students, contractors, volunteers and authorised visitors using UPS-managed networks, school-owned or approved personal devices, Microsoft 365/Teams, learning applications, financial and admissions systems, and any information processed for school purposes. The requirements apply on campus and, where relevant, during remote access or learning.

3. ROLES AND RESPONSIBILITIES

- **School Governing Body / Senior Leadership Team (SLT):** Approve the policy, assign oversight, provide resources and authorise external notifications as required.
- **IT Department / IT Manager:** Maintain security controls, review permissions and logs, manage backups, coordinate incident response and retain evidence of reviews.
- **Digital Wellbeing / Student Protection Lead:** Oversee student online safety, support safeguarding responses and coordinate awareness activities.
- **Staff and contractors:** Protect credentials, use approved systems, safeguard records and report suspicious events immediately.

- **Students and parents/guardians:** Follow responsible use guidance, protect login details and report harmful or suspicious online activity.

4. IDENTITY, PASSWORDS AND ACCESS CONTROL

- Each user shall have an individually assigned account; sharing passwords or using another person's credentials is prohibited.
- Multi-factor authentication shall be enabled for critical school services, administrator accounts and other high-risk access where supported.
- Role-based access and least privilege shall govern permissions; access must be reviewed periodically and promptly removed when roles change or users leave.
- Privileged accounts shall be limited, protected and reviewed. Exceptions require documented approval.

5. NETWORK AND INTERNET SECURITY

- UPS shall operate managed firewall controls and maintain intrusion detection/prevention capabilities, with regular review of alerts, rule changes and security updates.
- Administrative, student, guest, server, surveillance and other sensitive networks shall be segmented where appropriate, with access restricted by documented network rules.
- Web and DNS filtering shall be applied to reduce access to malicious, inappropriate or age-unsuitable content; approved educational exceptions shall be recorded.
- Wireless networks must use secure authentication. Unauthorised network equipment, hotspots and attempts to bypass filtering are not permitted.
- The IT Department shall monitor unusual network activity and investigate infected or unmanaged devices before permitting access to sensitive resources.

6. DEVICES, SOFTWARE AND PHYSICAL SECURITY

- School-managed computers, tablets, servers and interactive panels shall receive approved security patches, malware protection and secure configurations appropriate to each device.
- Sensitive devices and records shall be encrypted in transit and at rest where supported; screens shall be locked when unattended.
- Only approved software and storage services may be used for school data. Lost or stolen devices must be reported immediately.
- Servers, communications racks, networking equipment and backup media shall be accessible only to authorised personnel.

7. PERSONAL DATA PROTECTION AND CONFIDENTIALITY

- UPS shall collect only necessary data for legitimate educational, safeguarding and administrative purposes and maintain transparent notices and consent procedures where required.
- Student, parent, staff, medical, financial and academic records shall be classified, secured and shared only with authorised parties for approved purposes.
- Personal data must not be transmitted through private email, public links, personal messaging services or unapproved AI tools and external applications.
- Records shall be retained, accessed, corrected and securely disposed of in accordance with school records rules, applicable laws and ADEK requirements.
- Sharing with ADEK or authorised third parties shall follow the applicable legal basis, approvals, contractual safeguards and disclosure procedures.

8. CLOUD SERVICES, TEAMS AND THIRD-PARTY PROVIDERS

- School-approved accounts shall be used for Microsoft 365, Teams and educational platforms; public sharing, external guests and meeting permissions shall be restricted as appropriate.

- New learning applications, suppliers and cloud services shall undergo a documented security, privacy and safeguarding review before use.
- Third-party agreements shall address confidentiality, access, incident notification, data handling and backup or recovery responsibilities.

9. BACKUP, RECOVERY AND CONTINUITY

- Critical systems, configurations and records shall be backed up on a planned schedule, with secure copies isolated from the production network or stored offline as appropriate.
- Recovery procedures shall be tested periodically, and responsibilities for restoration shall be documented.
- Continuity arrangements shall prioritise student safety, communications, teaching, admissions and essential administrative services during disruption.

10. RESPONSIBLE USE AND DIGITAL SAFEGUARDING

- Students shall access school technology for educational purposes under age-appropriate supervision and comply with acceptable-use and anti-cyberbullying expectations.
- Taking, sharing or publishing student images, recordings or personal information requires the relevant approvals and safeguards.
- Staff shall receive cybersecurity guidance, and students shall be taught how to identify phishing, unsafe links, privacy risks, scams and harmful content.

11. SECURITY MONITORING AND ASSURANCE

- The IT Department shall maintain appropriate asset inventories, access records, configuration records, incident logs and evidence of security checks.
- System and network monitoring shall be necessary, proportionate and restricted to authorised personnel, respecting privacy and records retention rules.
- Vulnerability checks, access reviews and backup recovery tests shall be documented, with identified risks assigned corrective actions.

12. CYBERSECURITY INCIDENT RESPONSE

All suspected phishing, malware, compromised accounts, loss of devices, unauthorised access, data disclosure or online safeguarding incidents must be reported immediately to the IT Department and relevant school leadership. Staff must not independently erase evidence or disclose incident details externally.

- **1. Identify and log:** Record the time, affected users or systems, possible data exposure and immediate safety concerns.
- **2. Contain:** Isolate affected devices or accounts where necessary, preserve evidence and avoid unnecessary disruption.
- **3. Investigate and recover:** Determine the impact, remove the cause, restore trusted services and verify recovery.
- **4. Notify appropriately:** Escalate through SLT and follow ADEK and other applicable reporting duties. External communication is restricted to authorised channels.
- **5. Learn and improve:** Maintain an incident record, actions taken, approvals and lessons learned; update controls and train staff where required.

13. REGULATORY COMPLIANCE AND EXTERNAL COMMUNICATION

UPS shall comply with applicable ADEK rules, UAE data protection requirements and cybercrime legislation. In accordance with the ADEK School Digital Policy, cybersecurity incident communications outside the school shall be controlled by authorised leadership and directed to the involved service provider and ADEK, subject to applicable legal reporting obligations. Public statements and responses to external enquiries shall not be issued by individual staff members.

14. TRAINING, ENFORCEMENT AND REVIEW

- Appropriate awareness shall be provided to new staff and students, refreshed regularly and updated in response to significant threats or incidents.
- Non-compliance shall be handled proportionately under UPS staff, student protection and behaviour procedures, with emphasis on safeguarding and fair process.
- SLT and the IT Department shall review this policy at least annually and after major incidents or changes in law, ADEK guidance or school systems.

REFERENCES

- ADEK School Digital Policy, Version 1.1 (September 2024), especially Sections 1, 4, 5, 6 and 7.
- ADEK School Records Policy and Student Protection / Safeguarding requirements (as applicable).
- UAE Federal Decree-Law No. 45 of 2021 concerning the Protection of Personal Data.
- UAE Federal Decree-Law No. 34 of 2021 on Combatting Rumours and Cybercrimes.
- UPS Student Admission Policy (May 2025) and UPS Attendance Policy and Guide (internal policy references).

UPS ADOPTION NOTE

Universal Private School maintains this Cybersecurity Policy as part of its internal policy framework. The effective date and review date are recorded below. The School Principal oversees implementation, and the IT Manager coordinates technical cybersecurity controls, reviews and incident handling. The policy is supported by separate data-protection, responsible-use, and incident-response procedures and is subject to applicable ADEK and UAE requirements.

POLICY ADMINISTRATION

EFFECTIVE DATE	06 August 2026
REVIEW DATE	06 August 2026
SCHOOL PRINCIPAL	Dr Mays Rababah
IT MANAGER	Eng. Ghaith Shawqi