مدرسة الوحدة الخاصة

AL WAHDA PRIVATE SCHOOL

An American Curriculum School

IT Infrastructure & Management Policy

2025-2026

IT Infrastructure & Management Policy

1. Purpose

This policy provides a framework for the effective management, maintenance, and security of the school's IT infrastructure. It ensures that all systems support teaching, learning, operations, and communication while minimizing risk, downtime, and security vulnerabilities.

2. Scope

This policy applies to all IT systems, users, hardware, software, and digital services used by the school, including:

- Staff and student devices
- Network infrastructure
- Learning management systems (LMS)
- Cloud-based applications
- Communication platforms
- Servers and data storage systems

3. IT Infrastructure Management

3.1 Responsibilities

- **IT Manager / Director of Technology** oversees the infrastructure and ensures compliance with this policy.
- **School Leadership** ensures alignment of IT with educational goals.
- **IT Team** supports users, maintains systems, and implements updates and security measures.

3.2 Network Management

- Ensure stable and secure internet access across campus.
- Maintain separate VLANs or subnets for students, staff, and guests.

- Monitor bandwidth to support high-demand instructional activities.

3.3 Hardware Management

- Inventory all hardware annually (computers, projectors, switches, printers, etc.).
- Replace or upgrade devices on a 3–5 year cycle based on usability and support.
- Ensure devices meet minimum requirements for curriculum delivery and standardized testing.

3.4 Software Management

- Maintain licensed and approved software for curriculum and operations.
- Centralize software updates and patches.
- Ensure accessibility and compatibility across platforms used by the school.

4. IT Maintenance

4.1 Scheduled Maintenance

- Perform monthly system health checks and diagnostics.
- Schedule updates and reboots outside instructional hours when possible.
- Clean and service physical equipment (servers, routers, devices) quarterly.

4.2 Asset Management

- Maintain a digital inventory using asset tracking tools.
- Tag all equipment and assign responsibility to departments or users.
- Record and track the lifespan and usage history of each asset.

5. IT Security Standards

5.1 Data Security

- Secure all student and staff data in compliance with FERPA and COPPA.
- Use encrypted storage for sensitive files and password-protected systems.
- Implement multi-factor authentication (MFA) for staff and admin logins.

5.2 Access Controls

- Assign role-based access to systems and data.
- Immediately revoke access for staff or students leaving the school.
- Regularly audit user permissions and logs.

5.3 Network Security

- Install and maintain enterprise-grade firewalls and antivirus protection.
- Use secure Wi-Fi protocols (WPA3 or equivalent).
- Conduct annual penetration testing and vulnerability scans.

5.4 Cybersecurity Training

- Provide annual cybersecurity awareness training for all staff.
- Educate students on safe online behavior through digital citizenship programs.

6. IT Support Guidelines

6.1 Helpdesk Operations

- Maintain a ticketing system for tracking user support requests.
- Categorize requests by urgency and assign response times:
    - *Critical (e.g. network outage):* Response within 1 hour.
    - *High (e.g. exam-related issue):* Within 4 hours.
    - *Standard (e.g. device setup):* Within 24–48 hours.

6.2 Staff and Student Support

- Provide walk-in and remote support during school hours.
- Offer onboarding sessions for new staff and students.
- Maintain a self-service knowledge base for common issues and tutorials.

6.3 Vendor and External Services

- Maintain a list of authorized vendors for hardware/software support.
- Ensure third-party service agreements include SLAs and data privacy terms.

7. Disaster Recovery Plan

7.1 Backup Procedures

- Automate daily cloud backups of critical systems (student information system, LMS, financial records).
- Store backups in geographically separate locations or secure cloud environments.
- Test backup restorations quarterly.

7.2 Incident Response

- Designate an IT incident response team.
- Define steps for system failure, data breach, or ransomware attack:
    - Isolate affected systems.
    - Notify school leadership and relevant authorities.
    - Communicate transparently with stakeholders.

7.3 Recovery Time Objectives (RTO)

- **Mission-critical systems** (e.g. SIS, email): Restore within 4–8 hours.
- **Instructional systems** (e.g. LMS, classroom tech): Restore within 24 hours.
- **Non-essential systems**: Restore within 72 hours.

8. Policy Review

This policy shall be reviewed annually by the IT Manager and approved by the School Leadership Team. Updates may be made in response to technological changes or incidents.

Approved by: Duraid Al Oubaidy June 2026