

APPROPRIATE/ACCEPTABLE USE POLICY (AUP)

ATHENA EDUCATION

1. Overview and Scope

This Appropriate/Acceptable Use Policy (AUP) defines the acceptable use of all ATHENA EDUCATION-owned or –managed technology resources, ensuring lawful, ethical, and secure practices. It applies to all students, faculty, staff, contractors, and affiliates, covering:

- Hardware: Desktops, laptops, tablets, mobile devices, servers, networking equipment, audiovisual devices, security cameras, printers, copiers, and related cabling.
- Software & Services: Operating systems, licensed applications, open-source tools, cloud/SaaS platforms, learning management systems, email, file storage, collaboration portals.
- Connectivity: Wired, wireless (Wi-Fi), VPN, intranet, and external internet access.
- Digital Communications: Email, instant messaging, official social media accounts, and collaboration tools.

This policy is reviewed annually to align with UAE regulations (e.g., Federal Decree-Law No. 45 of 2021 on Data Protection) and modern educational practices.

2. Definitions

- Acceptable Use: Utilizing ATHENA EDUCATION's IT resources in alignment with its educational mission, legal requirements, and this policy.
- IT Resources: All hardware, software, networks, and services owned, leased, or managed by ATHENA EDUCATION.
- User: Any individual with authorized access credentials, including students, staff, faculty, and third-party personnel.

3. General Responsibilities

1. Account Security: Users must protect all credentials, never share passwords, and use unique accounts.
2. Device Care: Keep devices updated with approved security patches; lock or log off when unattended; report loss or malfunction immediately.
3. Data Protection: Do not transfer personally identifiable or confidential data via unapproved methods or portable media.

4. Software Licensing: Install only properly licensed software; unauthorized copying or distribution is prohibited.

5. Antivirus & Updates: Maintain current antivirus/anti-malware software and system updates on all devices.

6. Email & Attachments: Exercise extreme caution with unknown email attachments; refrain from forwarding chain letters, spam, or malicious content.

4. Bring Your Own Device (BYOD)

Personal devices may connect to Athena Education's network only if they:

- Run current antivirus and anti-malware protection.
- Have fully patched and supported operating systems.
- Install Athena Education's Mobile Device Management (MDM) client, allowing policy enforcement and remote wipe.

Unauthorized personal networking equipment (e.g., routers) is prohibited.

5. Acceptable Use of Internet and Network

- Permitted: Academic research, coursework, administrative tasks, and collaboration using approved tools.
- Prohibited: Accessing or distributing illegal, copyrighted, or harmful content; cyberbullying, harassment, hate speech; running unauthorized servers or network scanners; denial-of-service or other disruptive attacks.
- Remote Access: Use institution-approved VPNs; ensure encrypted connections.

6. Academic Honesty and Plagiarism

- Academic Honesty: Users must create original work and cite sources properly in assignments, projects, and publications.
- Plagiarism: Presenting another's ideas or words without attribution—whether copied verbatim or paraphrased—is prohibited.
- Consequences: Violations lead to disciplinary actions as per the Athena Education Student Handbook, up to dismissal.

7. Copyright and Intellectual Property

- Legal Compliance: Adhere to UAE Copyright and Related Rights Law (Federal Law No. 38 of 1992, as amended) and international IP laws.
- Use of Materials: Obtain licenses or permissions before copying, sharing, or distributing copyrighted texts, images, audio, video, or software.
- Fair Use/Educational Exemption: Limited reproduction for teaching and research is permitted with proper attribution and restricted distribution to enrolled users.

8. Modern IT Practices for UAE–Based Schools

1. Cloud & SaaS: Use only providers storing data within UAE or compliant jurisdictions; enforce encryption at rest/in transit and robust access controls.
2. IoT & Smart Classrooms: Isolate IoT devices on dedicated VLANs; schedule regular firmware and security updates.
3. Data Classification & Privacy: Classify data as Public, Internal, or Confidential; enforce multi-factor authentication and role-based access for Confidential data.
4. Social Media & Branding: Official accounts must adhere to brand guidelines; include disclaimers that personal opinions do not represent Athena Education.

9. Prohibited Activities

Without exception, users must not:

- Violate IP rights (e.g., install pirate software, share unlicensed media).
- Introduce malicious code (viruses, worms, rootkits).
- Bypass security controls or authentication mechanisms.
- Engage in fraudulent or defamatory communications.
- Conduct unauthorized network or security scans.
- Harvest or solicit email addresses for spam or harassment.

10. Enforcement, Monitoring & Reporting

- Monitoring: Athena Education reserves the right to monitor network traffic, device logs, and application usage for compliance.
- Reporting: Suspected violations should be reported to the IT Helpdesk or Compliance Office; confidentiality is maintained when possible.
- Discipline: Non-compliance may result in suspension of access, academic/employment disciplinary actions, or legal proceedings.

11. Acknowledgment

I, the undersigned, have read, understand, and agree to abide by the terms of Athena Education's Appropriate/Acceptable Use Policy (AUP). I acknowledge that violations may lead to disciplinary or legal action.

Name: _____ Date: _____

Signature: _____