The American University of Paris

Bring Your Own Device (BYOD)

Number: IT008EN

Last Review Date: 09 June 2025

1. PURPOSE

This policy outlines the guidelines and responsibilities for students, faculty, and staff who wish to use personal devices to access university resources. Its goal is to facilitate the effective and secure use of personal devices within the university environment.

2. WHO IS AFFECTED BY THIS POLICY

This policy outlines the guidelines and responsibilities for students, faculty, and staff who wish to use personal devices to access university resources. Its goal is to facilitate the effective and secure use of personal devices within the university environment.

3. SCOPE

This policy applies to all members of the university community, including students, faculty, staff, and any third parties who access the university's network and resources using personal devices.

4. AUTHORIZED DEVICES

The university supports a variety of personal devices, including laptops, tablets, and smartphones. To ensure compatibility and security, the following operating systems are recommended:

- Laptops: Windows 10 or later, macOS 10.15 (Catalina) or later
- Tablets and Smartphones: iOS 14 or later, Android 10 or later

5. ACCESS TO UNIVERSITY RESOURCES

Personal devices may be used to access a range of university resources, including:

- University email
- Learning management systems
- Library databases
- Course-specific software applications
- Virtual Lab

6. SECURITY REQUIREMENTS

To protect both personal and university data, users must adhere to the following security protocols:

- Antivirus Software: Devices must have up-to-date antivirus software installed.
- Operating System Updates: Regularly update device operating systems to the latest versions.
- Password Protection: Enable strong passwords or biometric authentication on all devices.
- Network Access Control: Users may be required to register their devices with the university's IT department to gain network access.

7. USAGE GUIDELINES

When using personal devices on campus or accessing university resources, users must:

- Comply with all university IT policies and codes of conduct.
- Ensure that device usage does not disrupt the learning environment.
- Refrain from accessing, storing, or transmitting inappropriate or illegal content.

Infringement of these rules may lead to the termination of the access for the user device.

8. STAFF AND FACULTY REQUIREMENTS

Faculty and staff who use personal devices to access university resources must comply with additional security measures:

- IT Acceptable Use Policy: Staff and faculty must agree to and comply with the university's IT Acceptable Use Policy.
- University Control over Information Assets: The university reserves the right to remotely remove any university information assets or revoke access to systems from BYOD.
- Security Prerequisites: To ensure information security, faculty and staff may be required to meet specific conditions, including but not limited to:
  - Minimum operating system version
  - Firewall rules compliance
  - Active antivirus solution
  - Multi-factor authentication (MFA) for remote access

- Information Handling: University information classified as highly restricted or restricted must not be downloaded to personal devices or personal cloud storage without explicit permission from the data owner.
- Use of Secure Networks: Faculty and staff must avoid connecting to unknown Wi-Fi networks unless using a reputable VPN service or encryption protocol.
- Device Disposal and Security: When selling, transferring, or disposing of a device used for university work, all university data must be securely removed, preferably through a factory reset or data-wiping process.

9. SUPPORT AND LIABILITY

The university's IT department will provide support for accessing university resources but is not responsible for:

- Hardware or software issues on personal devices.
- Loss, theft, or damage to personal devices.
- Data loss on personal devices.

Users are encouraged to maintain regular backups of their data

10. POLICY UPDATES

This policy will be reviewed annually and updated as necessary to accommodate emerging technologies and security threats. Users will be notified of significant changes via official university communication channels.
By adhering to this BYOD policy, the university community can enjoy the benefits of personal device usage while maintaining a secure and productive educational environment.

11. RESPONSIBILITIES

The Chief Information Officer is responsible for the interpretation and administration of this policy.

12. DEFINITIONS

AUP, the University: The American University of Paris

AUP Resources: Facilities, library resources, equipment, funds, personnel, and other resources belonging to or supplied by AUP.

BYOD Device: Any equipment able to connect to the University network which is not owned and managed by the University.

IT Services: Department of Information Technology Services at AUP

User: A person expressly authorized to use University information technology resources and associated services provided by AUP.

13. APPROVALS & HISTORY

- To be reviewed in June 2026.

14. ISSUING OFFICE AND CONTACT

Chief Information Officer
Information Technology Services
69 quai d’Orsay
75007 Paris
+33 1 40 62 06 96
itservices@aup.edu