PROCEDURE MANUAL

ARIZONA WESTERN COLLEGE			**PROCEDURE 223.016**
			Page 1 of 5
			Last Revision Date: 04/13/2026
			Effective Date: 05/06/2025
			Last Review Date: 04/13/2026
Section:	Technology	**Subject:**	Personal Device Usage

PURPOSE

The purpose is to outline the procedure Arizona Western College's (AWC) Information Technology Services & Support (ITSS) takes for Bring Your Own Device (BYOD). This procedure establishes guidelines for using personally owned computing devices on the AWC network, ensuring the protection of intellectual property, sensitive data, and college-licensed software. AWC recognizes the prevalent use of personal Mobile Devices for college business and has instituted this procedure to regulate such activity. Employees, Students, volunteers, contractors, etc. must comply with these guidelines to mitigate the risk of security breaches, and safeguard College Data and Technology Resources.

SCOPE

This procedure covers all College employees, Students, volunteers, contractors, utilizing personally owned devices for college-related activities, including portable computers, storage media, mobile devices, and IoT (Internet of Things) devices. Exceptions may be granted per relevant procedures. It sets minimum security standards for personal devices accessing college resources, excluding college-owned devices. Users are responsible for configuring their devices, accepting liability for any damage or charges incurred, and ensuring compliance with this procedure.

PROCEDURE

For all personal devices, whether utilized for college business or personal use, it is mandated that all individuals must adhere to the following guidelines:

- **Compliance with Acceptable Use Procedure**: All personal device use must adhere to the College's Acceptable Use Procedure. 223.001
- **Data Backup Responsibility:** Users are responsible for backing up their personal data. AWC bears no responsibility for the maintenance, backup, or loss of data on BYOD devices.

ARIZONA WESTERN COLLEGE			**PROCEDURE 223.016**
			Page 2 of 5
			Last Revision Date: 04/13/2026
			Effective Date: 05/06/2025
			Last Review Date: 04/13/2026
Section:	Technology	**Subject:**	Personal Device Usage

- **Physical Security Measures**: Owners must secure their devices physically to prevent theft or loss.
- **Reporting Lost or Stolen Devices**: In the event of a lost or stolen device containing college data, prompt reporting to ITSS is mandatory.
- **Adherence to Security Requirements**: Devices must meet the specified security requirements for accessing college resources.
- **Network Disruption Prevention:** Personal devices must not cause disruption to the Campus Network or College Information System.
- **Disruptive Device Handling:** AWC ITSS reserves the right to block devices causing disruption.
- **Network Authentication**: Authentication is obligatory for device access to the college network.
- **Prohibition of Personal Devices as Servers or Networking Devices:** Personally owned devices must not function as college servers or networking devices.
- **Generative AI:** Users shall not input, process, or generate College data using artificial intelligence tools in ways that bypass security controls, expose sensitive information, or violate College policies.

RESPONSIBILITIES

Participants utilizing personal devices to access college resources are responsible for safeguarding sensitive data and ensuring compliance with relevant Federal and State Regulations, along with AWC policies and procedures. This includes configuring devices for connectivity, accepting liability for any damages or legal consequences resulting from device activities, and taking ownership of transactions conducted under their authentication. The college is not responsible for maintenance, backup, or loss of data on personal devices, or for the security of such devices in cases of loss, theft, or damage. Any suspected or confirmed data breach involving a personal device must be reported immediately to ITSS in accordance with the Incident Response Procedure (223.017).

ARIZONA WESTERN COLLEGE			**PROCEDURE 223.016**
			Page 3 of 5
			Last Revision Date: 04/13/2026
			Effective Date: 05/06/2025
			Last Review Date: 04/13/2026
Section:	Technology	**Subject:**	Personal Device Usage

SECURITY CONTROLS

- **Active Access Protection:** Utilize an active form of access protection such as passcode, passphrase, facial recognition, or fingerprint to secure the device.
- **Anti-virus Software:** Ensure that anti-virus software is installed and running Real-Time Scanning, and regularly scan the device to prevent, detect, and remove malware.
- **Supported Operating System:** Use a supported operating system that is regularly patched and updated to ensure the latest security measures are in place.
- **Prohibited Modifications:** Devices that have been Jailbroken, Rooted, or subjected to any other method of altering built-in protections must not be used to access college resources.
- **WPA2 and AES Support:** Devices must support wireless security (WPA2 and AES) encryption protocols to connect to AWC Wi-Fi systems.

DEVICES

The College will not reimburse employees for business calls or Internet usage made on non-College devices. Employees that feel that they need to use a cellular phone or have mobile internet service for college business must follow the procedures to acquire a college device.

Personal mobile devices can be utilized if the employee is willing to fund and support the device. If the device is configured to use the College network, or retrieve employee email, the employee acknowledges that College policy requires that any computer/device connected to the network is subject to the State of Arizona Public Records Law. (That means, that during a security audit, a list of remote users could be requested, and if deemed that those users connected to State resources from non-state devices that equipment may be susceptible to search and/or seizure in accordance with applicable laws.) Employees must understand that any personal device used for business communications is subject to remote wipe of all contents by the College Information Security Officer (ISO), if deemed a security issue. All efforts will be made to communicate with the employee before this action takes place.

ARIZONA WESTERN COLLEGE			**PROCEDURE 223.016**
			Page 4 of 5
			Last Revision Date: 04/13/2026
			Effective Date: 05/06/2025
			Last Review Date: 04/13/2026
Section:	Technology	**Subject:**	Personal Device Usage

College email, data and other business-related communications are the property of the College regardless of where they are stored and the mobile devices used for business communications are subject to search and/or seizure at any time, and there is no guarantee or expectation of privacy for any communications or data (personal or otherwise) stored on the device used for business communications.

SUPPORT

ITSS will provide software application support only if the software is deemed necessary for job functions. Examples of support services that will not be provided include, but are not limited to:

- **Troubleshooting Performance and Hardware Issues:** Assistance with device performance or hardware problems will not be provided.
- **Hardware Installation:** Installation of new or replacement hardware is not within the scope of support services.
- **Unsupported Software and Services:** Troubleshooting software applications or cloud services not offered or supported by AWC will not be provided.
- **Operating System Updates and Software Installation:** The department will not install Operating System updates, patches, or software applications unless they are required for job functions.
- **Data Backup and Migration:** Backing up device data or migration to another device is the responsibility of the user.
- **Third-Party Email Clients/Accounts:** Support for third-party email clients or accounts is not provided.
- **Malware Removal:** The removal of malware, spyware, or viruses is not covered under support services.

PROCEDURE MANUAL

ARIZONA WESTERN COLLEGE			**PROCEDURE 223.016**
			Page 5 of 5
			Last Revision Date: 04/13/2026
			Effective Date: 05/06/2025
			Last Review Date: 04/13/2026
Section:	Technology	**Subject:**	Personal Device Usage

HISTORY

IT Reviewer Name	Update Date	AWC Reviewer	Approval Date
Scott Estes, Tyler Vodehnal, Mercedes Soto	2/4/2025	Dr. Daniel Corr	05/06/2025
Scott Estes, Tyler Vodehnal	02/04/2026	Dr. Reetika Dhawan	04/13/2026