# 1710.500 MOBILE COMMUNICATIONS DEVICES PROCEDURE

## A. GENERAL

Wenatchee Valley College (WVC) mobile communications devices, and associated telecommunications contracts, and services, are managed by the technology department.

Mobile devices owned by Wenatchee Valley College or personally owned that access WVC data networks, systems, applications, services or data repositories, hosted by college systems or hosted in college managed cloud services, or third- party cloud service providers, are governed by this procedure. Applications, including cloud storage software/services, used by staff on their own personal devices are also subject to this procedure. Mobile devices purchased by Wenatchee Valley College will be automatically registered with technology department college mobile device enrollment services. Personal mobile devices that require access to college data and networks must abide by these procedures.

The following general procedures and protocols apply to the use of all mobile devices:

### 1. All mobile devices must be protected with a password, PIN code, biometric method (facial recognition, fingerprint) at the time the device is enrolled into WVC mobile device enrollment services and continue as long as the device has access to WVC data.

### 2. Mobile device passwords/PIN codes must meet the requirements outlined in the Wenatchee Valley College Access Control and Password Policy.

### 3. All college data stored on mobile devices shall be encrypted.

### 4. All mobile devices will utilize the most secure wireless encrypting standards; security and access protocols shall be used with all wireless network connections.

### 5. All mobile device users shall refrain from using public or unsecured network connections to transmit/receive college data. All mobile devices used to connect to college networks shall be registered with the appropriate mobile device management (MDM) role approved by the WVC Technology Department.

### 6. All mobile computing devices that access WVC networks shall have active and up-to-date anti-malware/virus protection and firewall protection software installed.

### 7. All mobile devices shall have locations services enabled. All lost, stolen, destroyed or compromised mobile devices or mobile devices that have been identified as threats to WVC networks or data will lose access to college data and networks.

#### a. Temporary loss – device must be remediated and meet device health baselines.

#### b. Permanent loss – employee separation, risk management assessment or other circumstances.

### 8. WVC Technology Department reserves the right to terminate access to any device without prior notification to the device owner.

### 9. All mobile devices and applications shall be kept up to date.

### 10. Operating system and application patches shall be installed within 30 days of release.

## B. USER DEVICE RESPONSIBILITIES

The following procedures and requirements shall be followed by all users of mobile devices:

### 1. WVC employees shall immediately report any lost, stolen, destroyed or compromised device in any way or form to the Wenatchee Valley College Information Technology (IT) Helpdesk.

### 2. Email the IT helpdesk at helpdesk@wvc.edu or call 509-682-6550 for assistance

### 3. Unauthorized access to a college owned or personal mobile device or unauthorized access to college data must be immediately reported to WVC IT Helpdesk.

### 4. Personal mobile devices shall not be “rooted, jail broken” or have software/firmware installed that could pose a risk to college data stored on the device.

### 5. Users shall not load illegal content or pirated software onto any mobile device accessing college networks or data.

### 6, Only WVC IT approved applications are allowed on college owned mobile devices.

### 7. College provided/approved applications will be updated on a regular basis per WVC IT policies and standards.

### 8. Device security health baselines will be enforced on all devices.

### 9. Users shall use WVC approved data sharing systems or services when sending or receiving WVC data.

### 10. Users are responsible for ensuring all important files stored on the mobile devices are backed up on a regular basis.

### 11. Users shall not modify or attempt configurations without express written authorization from WVC Technology staff.

## C. ADMINISTRATIVE RESPONSIBILITIES

The Wenatchee Valley College Technology Department staff and/or Mobile Device Management Services or their designee are responsible for the following:

### 1. Ensure employee/student personal data remains secure at all times.

### 2. Reserves the right to block personal devices that are determined to pose a threat to college networks, services and data, pending remediation by the device owner, or that violate mobile device requirements.

### 3. Reserves the right to permanently block a personal device if remediation efforts by the owner are not satisfactory, timely or technology staff determine the device continues to pose a security threat to college networks and data.

### 4. Mobile device management (MDM) enterprise mobility software will be used to enforce common security standards and configurations on devices such as:

#### a. Auto-lock with PIN or passcode enforcement.

#### b. PIN and passcode complexity enforcement.

#### c. Remote wipe enabled to lock or wipe a lost or stolen device.

#### d. Full wipe of college owned devices upon employee separation.

#### e. Partial wipe on personal devices (college data, i.e., email, teams chats, etc.).

#### f. Enforce use of secure communications protocols.

#### g. Ensure college-owned apps are maintained and up to date.

#### h. Application isolation.

#### i. Geofencing.

#### j. Device health and security baselines.

### 5. Specific configuration settings shall be defined for malware protection software to ensure that that this software is not alterable by users of mobile and/or employee-owned devices.

### 6. Annual security training is provided to users of mobile devices. The content and form of that training shall be decided by Wenatchee Valley College or designee. Periodic security reminders will be used to reinforce mobile device security procedures and other best practices.

### 7. Mobile device management software is used to manage risk, limit security issues, and reduce costs and business risks related to mobile devices. The software shall include the ability to inventory, monitor (e.g., application installations), issue alerts (e.g., disabled passwords, categorize system software operating systems, rooted devices), and issue various reports (e.g., installed applications, carriers).

### 8. Mobile device management software shall include the ability to distribute applications, data, and global configuration settings against groups and categories of devices.

### 9. Perform yearly reviews at a minimum and updates of security standards and procedures used with mobile computing devices.

### 10. Establish procedures, workflows, memorandum of understanding(s), to manage and document requests for exemptions and deviations from these procedures.

### 11. Mobile device management software shall terminate device access when an employee separates and performs a data wipe of the device(s).

### 12. Implement technical processes and measures to strictly limit and control access to sensitive data moving to and from mobile computing devices.

## D. AUDIT CONTROLS AND MANAGEMENT

### 1. Documented procedures and evidence of practices shall be available upon request for this procedure and accessible as part of WVC policies and procedures website. Satisfactory examples of evidence and compliance include:

#### a. Documented quarterly spot user checks for compliance with mobile device computing policies.

#### b. Readily available processes and procedures for staff use of mobile devices.

#### c. Configuration and support guidelines and procedures for mobile devices.

#### d. Communication and device logs of attached units showing appropriate management, compliance and monitoring protocols are in place.

#### e. Anecdotal and archival communications showing regular implementation of the procedure.

Approved by the president’s cabinet: 9/16/08, 1/6/09, 2/5/13, 4/25/23

Last reviewed: 4/25/23

Procedure contact: Technology

Related policies and procedures

 710.500 [Mobile Communication Device Policy](https://www.wvc.edu/humanresources/policies-procedures/700-technology/710.500-mobile-communication-devices.html)

 College Access and Password Policy