Status Active PolicyStat ID 10432393

Origination	12/2/2014	Owner	Clint Ewell: VP-Finance & Administrative Services
Last Approved	3/5/2021	Area	5.0 Administrative Services
Effective	3/5/2021		
Last Revised	3/5/2021		
Next Review	3/4/2024		

Mobile Device, 5.33

OPERATIONAL POLICY STATEMENT

It is the responsibility of any employee of Yavapai College (YC) who uses a mobile device to access institutional data to ensure that all security protocols normally used on YC controlled systems are also applied to their mobile equipment. It is imperative that any mobile device that is used to conduct College business is utilized securely, appropriately, responsibly, and ethically. The standards in this operational policy should be seen as supplementing, and not in lieu of, other College operational policies and applicable laws.

The intent of this operational policy is to define standards, procedures, and restrictions for employees and others whom have legitimate requirements to access College data from a mobile device which connects to the College's electronic resources via any network not directly controlled by YC. This operational policy applies to, but is not limited to, all devices and associated media that align with the following device classifications:

- Laptops, tablet, and hybrid computers
- Smartphones, mobile phones
- Personal Digital Assistants
- Home or personal computers used to access College resources
- Any other mobile device capable of storing or transmitting institutional data

Protections

Access Control — YC reserves the right to limit access to its systems to any mobile device if it feels that the equipment is being used in any way that may put the institutions' systems, data, students, or employees at risk.

All College owned mobile devices must be purchased through and registered with the Information Technology Services (ITS) Department. Upon termination, College owned mobile devices must be returned to the ITS Department.

Mobile device connections from remote networks must follow the standards set forth in Operational Policy 5.32 - Remote Access.

YC reserves the right to sanitize sensitive information from the devices of terminated employees.

Security — Employees using mobile devices and related software must use secure data management procedures. Devices should be protected by a strong password or pin and employees should not disclose their passwords to anyone.

All employees utilizing mobile devices for College business must employ reasonable physical security measures. Mobile devices should be encrypted to help prevent the loss of sensitive information.

All devices should have the latest operating system patches and by free of malware and viruses.

Employees are prohibited to store sensitive data (defined in Operational Policy 5.30 — Clean Desk and Clear Screen) onto mobile devices.

In the event of a lost or stolen college-owned mobile device, it is incumbent on the employee to report the incident to the ITS Department and Campus Police. Measures will be taken to mitigate any potential unauthorized access to College data.

Incident Reporting

Yavapai College employees must immediately report any incident or suspected incidents of unauthorized data access or data loss to their immediate supervisor and the ITS Department.

Operational Policy Enforcement

Engaging in any activity that violates this operational policy can result in the loss of access privileges or other discipline.

RELATED INFORMATION

OPERATIONAL POLICY HISTORY

Adopted 12/2/2014
Revised 4/3/2018
Revised to "Operational" Policy and owner reassigned 3/5/2021

Transferred to PolicyStat 12/1/2021

Approval Signatures

Step Description	Approver	Date