Administrative Procedure 612

MOBILE DEVICES

Purpose

The purpose of this procedure is to govern the acquisition, usage and management of wireless devices, handheld devices, cellular phones, flash-drives, lap-tops, or other personal electronic devices for Aspen View Regional Division No.19 business use by the organization's employees. This procedure outlines appropriate standards and procedures for accessing AVRD 19 networks, systems, databases, servers and other IT infrastructure via mobile devices.

Scope

This procedure governs all AVRD employees (FTEs, PTEs, contractors, contract workers, volunteers, etc) who use division or personally – owned mobile technology to access division resources for the purpose of conducting AVRD business and operations. AVRD reserves the right to revoke remote access privileges at any time should it deem necessary to do so.

The Superintendent, in consultation with the Technical Services department, has discretion in the installation, configuration, and security measures of mobile devices and related technology.

Eligibility

Any employee requiring the use of a mobile device must receive prior approval from the Superintendent or designate.

Appropriate Use

Any Aspen View Regional Division employee who uses mobile devices and services used to conduct AVRD business must be used responsibly and ethically.

1. Aspen View owned Mobile devices should only be used only for AVRD business.

2. No Employee shall use personally-owned mobile devices or services for AVRD business without the approval of his or her supervisor and/or the Superintendent.

3. Acquisition of any mobile technology shall be done so in full accordance with AVRD's purchasing and procurement procedure.

4. As the integrity of data on mobile is the sole responsibility of the user, common-sense physical security measures should be employed at all times to prevent theft or loss. Users must report loss or theft of a device immediately to his or her supervisor, as well as the IT department.

5. All mobile device users agree to immediately report any incident or suspicion of unauthorized access and/or disclosure of corporate data or resources.

6. To ensure security of confidential information contained on mobile devices, the device will be destroyed and disposed of in accordance with AVRD's disposal procedures.

7. Email messages may be periodically monitored to ensure the service is being used appropriately. All mobile device users agree and understand that usage may also be monitored to record dates, times, duration of access and so on in order to identify suspicious activity or potential breach of security.

8. Access to all division systems and data via a mobile device shall be protected by a strong password system that complies with AVRD's password procedure. Passwords should be changed at least every sixty (60) days

9. Mobile storage devices such as flash drives, DVD's, CD's must be encrypted and password protected or not to be used to store confidential information. Mobile smart devices such as smartphones, iPads, Android devices must be passcode / password protected, encrypted (if encryption is supported) and have remote erase / wipe enabled (if remote erase is supported) or not to be used to store confidential information.

10. Mobile Device users shall refrain from sending or storing sensitive data on their devices (e.g. student data, financial data, records about individuals requiring full protection), as per privacy legislation governing AVRD.

11. All Mobile devices governed by this policy shall have pre-approved anti-virus software installed if available for the device platform.

11. Questions or concerns about this procedure should contact the Director of Business Services at (780) 675-7080.