Walters State Community College

Faculty and Staff Mobile Device Data Policy

Introduction:

The purpose of this policy is to provide guidance for the appropriate use and configuration of mobile devices as necessary to protect the Walters State(WSCC) network and information from unauthorized access or disclosure. Mobile devices incorporate features traditionally found in a personal computer (PC). Their smaller size and affordability make these devices a valuable tool in a wide variety of applications; however, these devices are also subject to increased risk of loss, breakage, theft, and unauthorized use.

This policy applies to all faculty and staff who utilize a mobile device, owned by WSCC or the individual, to access the WSCC network, or to retrieve or store sensitive college information. Vendors, contractors, or other users who use mobile devices to access the WSCC network, or to retrieve or store sensitive college information may also be subject to this policy.

For the purposes of this policy, the following definitions apply:

A mobile device includes any device that is portable and capable of collecting, storing, transmitting, or processing electronic data or images. Examples include, but are not limited to, laptops or tablet PCs, personal digital assistants (PDAs), media players such as iPods™ and "smart" phones such as Blackberries™, digital photo cameras, and video cameras. This definition also includes storage media, such as USB hard drives, memory sticks or flash drives (also known as "thumb drives"), Secure Digital or Compact Flash cards, CD-R or DVD-R media, and any peripherals connected to a mobile device.

A personal mobile device includes any mobile device that is not owned or issued by Walters State, but is used to access the WSCC network to retrieve or store sensitive college information.

Sensitive college information includes, but is not limited to:

- **Personal identity information (PII):**

  Includes Social Security Numbers, credit card numbers, bank and other financial institution account numbers, health insurance plan identification numbers, driver's license numbers, dates of birth, and other similar information associated with an individual student or employee which can potentially be used to uniquely identify an individual and that if misused, might enable assumption of that individual's identity ("identity theft") to compromise an individual's personal or financial security.

- **Protected health information (PHI):**

  Includes health information that is defined in federal and state laws, and Tennessee Board Regents and WSCC policies and guidelines.

- **Student record information:**

  Includes academic, personal, and financial information based on student status or history and maintained or stored by the college.

Guidance for the Use of Mobile Devices:

Security and Protection

The user and/or owner of any mobile device used to access the WSCC network is responsible for protecting the device and any college data retrieved, accessed, or stored by the device.

Suggested methods of security and protection are:

- **Use of encryption and passwords**:

  All data owned by the college should be encrypted where and when possible and secured by a password.

- **Network Shared Drives:**

  WSCC provides protected network shared drives to store institutional information. Shared drives are secured and only allow authenticated users access, which can be limited to one or multiple users. The use of shared drives also fosters collaboration in a secured environment. Shared drives should be used to distribute sensitive data instead of using e-mail and/or other portable options.

- **Virtual Private Networks (VPN):**

  WSCC provides VPN options for connection to the institutional network when connecting remotely. The use of VPN software provides secure and encrypted connections to all institutional data.

- **Tracking and Recovery software:**

  All portable computers (laptops and tablets) owned by the college should incorporate tracking software to enable the identification and retrieval of the item in the event of loss or theft. WSCC encourages owners and users of personal mobile devices to incorporate tracking software on these devices, particularly if used to access the WSCC network or to retrieve or store sensitive college information.

- **Physical protection:**

  Owners and users must exercise due care in physically protecting mobile devices from loss, theft, or damage. This would include using security locks when possible and ensuring that the item is not vulnerable to loss, theft, or unapproved access.

- **Device identification:**

  Mobile devices owned or issued by Walters State must comply with the college's inventory policies. WSCC encourages owners and users of personal mobile devices to copy identifying information and store it in a secure location.

- **Virus protection:**

  All mobile devices owned by the college should run, when possible, the college's centrally managed security software to allow for protection from viruses, spyware, and other known and unknown security issues. WSCC encourages owners and users of personal mobile devices to install and configure antivirus and other security software to fully protect access to institutional sensitive information.

- **Disable unused services:**

  To reduce the risk of unauthorized access, wireless, infrared, Bluetooth or other connection features on any mobile device should be turned off when not in use.

- **Storage of passwords:**

  The unencrypted storage of usernames and passwords on mobile devices should be avoided.

Access and Storage of Sensitive College Information:

The following represent “best practices” for anyone utilizing a mobile device; however, all mobile devices, including personal mobile devices, used to access or store sensitive college information must meet the following requirements.

- **Access and use of sensitive information appropriately:**

  Unencrypted sensitive information should not be stored on mobile devices. Users needing access to the college network from mobile devices should utilize secure VPN access. This will allow users to securely access documents without storing them on the mobile device.

- **Use of personal devices to store sensitive information:**

  Sensitive college information should not be stored on personal mobile devices. Sensitive documents and correspondence accessed via e-mail should be removed from mobile devices as quickly as possible. It is the responsibility of the user to insure no sensitive data is stored on the device that is locally or remotely accessing any college network, data, or system.

- **Use of USB drives:**

  The use of unencrypted USB drives, known as "thumb drives” or “flash drives", and portable hard drives for the storage of sensitive college information is prohibited.

- **Physical protection:**

  Mobile devices used to access or store sensitive college information must not be left unattended and, where possible, must be physically locked away or secured. Additionally, any portable media; e.g. portable hard drives or CD-R or DVD-R disks used for backup of systems containing sensitive college information must be stored securely in locked drawers, cabinets, or other secure enclosures.

- **Exclusivity of use:**

  Any mobile device that stores sensitive college information must not be shared with any unauthorized user.

- **Protection of information:**

  Reasonable care must be taken when using mobile computing facilities in public places, meeting rooms, or other unprotected areas, either on or away from the college’s premises, to avoid the unauthorized access or disclosure of information stored on or accessed by the device.

Termination of college relationship:

All college-owned mobile devices must be returned to the Information and Educational Technologies Helpdesk office upon termination of the assigned user’s relationship with the college. In addition, any software applications purchased by the college and installed on a personal mobile device must be removed by the user. Sensitive information must be removed from the personal mobile device upon termination of the assigned user’s relationship with the institution.

Report any loss, suspected misuse, or theft:

Owners or users of mobile devices are required to report the loss, suspected misuse, or theft of any mobile device immediately to Campus Police and the Information and Educational Technologies (IET) Helpdesk. This provision includes personal mobile devices that store sensitive college data.