

# Electronic Device Use

University Facilities (UF)

Internal Guideline: 02.B.08.01

Effective Date: September 2014

Last Modified Date: February 2020

Approved by: Todd Barnette

The purpose of this document is to provide guidelines for the use of electronic devices (both personal and University issued) while on the job in the workplace.

Electronic Devices include but are not limited to: Cell Phones, Smart Phones, Laptops, Desk Computers, and any other devices that uses Wi-Fi, internet, intranet, landline, or over-the-air connectivity to communicate.

## University Issued Electronic Devices

---

Electronic devices are supplied to designated employees to be used on the job. The use of these devices should be limited to University business purposes. It should not serve as a personal device. These devices must be secured in an appropriate manner to prevent the accessing of the device by un-authorized people. These devices are subject to inspection, review, audits, and FOIA requests and the employee issued the device will be responsible for any information on the device and for any action or communication that occurs through that device. Employees should not consider the use or content to be protected under any privacy protection. Any personal communication which needs to be made should occur during scheduled breaks and utilizing a personal device.

## Electronic Device Acceptable Use Guide

---

**Mobile communication devices are to be used for official use just as other office equipment**, subject only to limited incidental personal use that does not increase the University's cost or violate any laws or ethical standards. Employees must reimburse the University for any incidental personal use that results in an additional expense to the University. The University Facilities Business Manager is responsible for collecting the reimbursement should there be a need. Employees should avoid making directory assistance (411) calls from a University issued mobile communication device unless the call is necessary for official business purposes and the employee has exhausted options to obtain directory information from no-cost services.

Employees have no expectation of privacy as to the use of any University issued mobile communication device. Management will have access to detailed records of mobile communication device usage from the service provider, which **will be subject to audit**.

Mobile communication devices may contain sensitive information. Therefore, employees must password protect their University issued mobile communication device and the device must be set to lock after no more than five minutes of inactivity, if such features are available on the device.

Employees should not use a University issued mobile communication device while operating a motor vehicle and must follow State Fleet Management's (SFM) Handheld Electronic Devices Directive when operating SFM leased fleet vehicles.

Use of University issued electronic devices will be monitored and usage above the average use of other employees with similar equipment and responsibilities may require supporting documentation that the device is not being used excessively for personal use.

All University issued electronic devices are subject to the Freedom of Information Act (FOIA). Any activity on these devices may become evidence in legal actions. The employee the device is issued to will be responsible for what is found as a part of the investigation.

## Prohibited Usage

---

The following examples are provided as examples of inappropriate use of University issued electronic devices but is not intended to be an exhaustive list:

- Viewing or posting personal messages on social media
- Expressing or posting comments, pictures, opinions, etc. that conflicts with the University's published position
- Streaming audio or video unrelated to work responsibilities (examples: YouTube, Spotify, etc.)
- Gaming
- Frequent or extended personal calls
- Allowing family members to use the device

## Responsibility for Device

---

- Employees are responsible for all University issued electronic devices assigned to you. Lost/missing equipment must be reported to the Director/Supervisor as soon as the loss is discovered.
- Employees will be financially responsible for any losses or damages to the equipment occurring outside normal work conditions and/or procedures.

- Employees will reimburse the University for any costs incurred during personal or unauthorized uses of cell phones.
- Employees no longer affiliated with the University Facilities are required to return all equipment prior to disaffiliation or you must pay the replacement cost for all equipment not returned.
- Employees on extended (greater than 90 days) Leave without Pay (LWOP) shall turn issued equipment in to their supervisor while on LWOP.

All University Facilities employees are subject to progressive disciplinary action when in violation of the above policy or any other University regulation that applies to the misuse of University property or equipment.

## Personal Electronic Devices

---

If you own a personal electronic device and choose to bring it to work, you must only use it during your scheduled break times. The use of the electronic device while on the job is not allowed and serves as a distraction. Emergency situations are the only exceptions to the practice. Electronic communications done in connection with University business could be subject to FOIA requests and/or discoverable through litigation.

## Special Note

---

The State of SC and the City of Clemson prohibits texting and emailing while behind the wheel. Violators are subject to fines.

Reference:

<http://www.state.sc.us/dio/docs/Mobile%20Communication%20Device%207-1-15.pdf> July 2015