Berkeley Asset Management Facilities Services

Smartphone Deployment Program

As part of the Maximo project, Asset Management/Facilities Services (AM/FS) is upgrading the currently issued Casio flip phones with Apple iPhone 6 Plus devices. Devices are issued to AM/FS staff based on role and job requirements.

Use of these devices is governed by the PPCS Code of Conduct and applicable University and Campus policies including but not limited to the following UCOP Policies:

- Electronic Communications Policy: http://policy.ucop.edu/doc/7000470/ElectronicCommunications
- BFB-IS-11: Identity and Access Management: http://policy.ucop.edu/doc/7020450/BFB-IS-11
- IS-2 Inventory, Classification, and Release of University Electronic Information: http://policy.ucop.edu/doc/7020447/BFB-IS-2

Device Issued:

- Apple iPhone 6 Plus 64GB. Included accessories: Wall Charger, USB Cable, basic earbuds
- Protective Case: Otterbox Defender Series.
  NOTE: This case is designed to provide drop, dust, screen, and scratch protection for the device. Staff are expected to keep the device in the issued case at all times. Damaged or defective cases should be reported to the CSC Manager or Real Estate IT. Alternate cases are not authorized. Departmental funds may not be used to purchase alternate cases and the employee may be held responsible for any device damage that results from the use of any alternate case.
- While devices are assigned to individual employees, the device remains the property of AM/FS. Each employee is expected to maintain the device in good working order and report any issues or problems with the device immediately. In the event of the employee's departure from the department or reassignment, the device and all accessories are to be returned immediately.
- In the event that a device is lost or stolen, the employee must report it to the AM/FS CSC Manager or Real Estate IT immediately to active Lost Mode for the device. Once the device is located, the administrator can disable lost mode. If the device cannot be retrieved, all data will be remotely wiped from the device.

Device Use

- **Communications**: The primary use of this device is for communication purposes including voice, text, email, and calendar. AM/FS also utilizes the Verizon Push to Talk (PTT) functionality for direct communication between devices.
- **Work Management**: Apps will be deployed to the device to support work, asset, and inventory management. The device and apps will be used as a tool to receive work assignments, record work and time to jobs, and complete work assignments.
- **Other Apps**: Additional apps have been deployed to the devices to support work-related activities. The list of authorized apps will be periodically reviewed and updated. Requests to install additional apps may be submitted to the Maximo Change Committee. The committee will review requests based on operational needs, compatibility, licensing, and cost requirements. To ensure that the devices are able to support the primary functions for communications and work management, employees are not authorized to install individual apps.
- **Personal Use**: Incidental personal use of the device is allowed per University policy. However, the employee may be required to reimburse the University for personal use that results in noticeable incremental costs. Personal data on University devices may be subject to public records disclosure. The University is not responsible for the loss of any personal data on the device and the employee should take care to ensure that any personal data is protected and does not interfere with the primary operations of the device.

Device Management

Prior to assignment each device will be enrolled in the departmental mobile device management (MDM) application. The MDM controls the device configuration include:

Passcode	Each device is required to have a minimum 6-digit passcode established by the user when it is assigned. If a user forgets the passcode, they should contact the CSC Manager or REIT to have the passcode reset.
Accounts	**iTunes/iCloud**: User may add personal iTunes and iCloud accounts for the use of certain services including music, news, and other personalizations; however, personal apps may not be installed from the iTunes app store. **Email**: At the time of assignment, the device will be configured to include the user's @berkeley.edu email and calendar account. Personal accounts may be added to the device; however, the user should take care to ensure that personal email storage does not interfere with the primary operations. **Wi-Fi**: At the time of assignment, the device will be configured to connect to AirBears2 using the user's individual AirBear2 key. The device may be connected to other Wi-Fi networks; however, the user must ensure that the connected networks are properly secured and do not expose the device or data to any security risks.
SimpleMDM App	The SimpleMDM app is installed on each device and reports device information. This app must be enabled at all times.
Lock Device	Provides the ability to remotely lock the device. When enabled, a message will be displayed on the device screen and the user will be required to enter the device passcode to unlock.
Lost Mode	Provides the ability for the administrator to disable the phone and identify its location. A message will be displayed on the device with instructions to return it AM/FS. Once the device is retrieved, lost mode can be disabled and the device returned to the assigned user.
App Deployment	As new apps are added to the MDM profile they will be pushed to the device. Unauthorized or restricted apps will be blocked by the MDM.
OS and App Updates	Any operating system (iOS) and app updates will be pushed to the device once they have been tested. The user may receive a prompt to complete the installation and may require device restart.
Home Screen Layout	The home screen layout is standardized for all devices and cannot be modified by the user.
Wallpaper	Both the lock screen and home screen wallpaper has been configured to support the device management and cannot be modified.