


Intelligence & Technology		
	Mobile Devices	Order 17.104

A. Purpose

City-issued mobile devices are provided to Tempe Police Department employees to allow for improved methods of communication, as well as for obtaining evidence and intelligence.

B. Policy

Any mobile device issued to an employee will be used in accordance with this General Order, as well as any and all other applicable City of Tempe or Police Department policies (i.e., passwords, cell phone usage, data usage, social media, etc.).

C. Definitions

- Mobile Device – Any handheld computing device with an operating system and can run various types of application software. A smartphone or tablet is an example of a mobile device.

D. General Considerations

1. City-issued mobile devices are for official business; however, it is understood that incidents may occur and result in incidental personal usage.
2. Information generated on, processed by, or stored in a City's mobile device, as well as all related billing records, may be required to be produced to a member of the public pursuant to the Arizona public records law (ARS 39-121 through 39-122) or pursuant to court order.

3. Personal mobile devices will not be used for business purposes.
4. All City issued mobile devices require a password.

E. Procedures

1. Employees will be provided training upon deployment of new mobile devices, including review and acknowledgement of this policy.
2. Mobile devices are assigned to individuals or work groups based upon demonstrated need.
3. If assigned a City mobile device, the employee must have the device turned on during their assigned work shift and/or standby time or as required by position.
4. The designated Mobile Device Coordinator will monitor Department inventory and conducts annual inventory for audit purposes.
5. Employees will take reasonable precautions to ensure their mobile device is not lost or stolen.
6. Employees will not remotely wipe their mobile device.
7. A lost mobile device must be reported to a supervisor immediately. The supervisor must have a Communications Supervisor remotely wipe all of the information on the device.
8. Requests to replace a damaged/lost mobile device must be submitted through an employee's direct chain of command to the Bureau Manager.
 - a. Damaged/lost mobile devices will be replaced by a device of the same make and model.
 - b. Department upgrades will occur on a regular basis and shall not be requested by individual employees.

9. Mobile Data Management System

- a. The purpose of the mobile data management system is to allow the City to protect assets, supply apps to users, and remove data and devices from the network if they are lost or stolen.
- b. All mobile devices must be managed through the City's mobile data management system/software.
- c. A user will not remove the mobile data management software from the device. If the mobile data management software is removed, the phone will be locked and all information removed from the device.
- d. A user will have five (5) attempts to unlock their device with a password. Upon the sixth attempt, the device will be locked and all information will be removed from the device.
- e. The mobile data management software will not be used to track cellphone locations without exigent circumstances.

10. Mobile Device Apps

- a. Any apps added to a City phone must be added through the corporate 'app store' available in the mobile data management system.
 - 1) A wide array of apps will be available for download to employees, and others will be pushed out to users automatically.
 - 2) This process must be used as it will allow the Department to transfer apps from one phone to another when an individual leaves the Department or moves to another assignment.
- b. To request a business related app be added to the corporate 'app store', simply send the request to tempepd_vpp@tempe.gov.

11. Apple iOS and ID Account

- a. Mobile devices running Apple iOS (to include, iPads and iPhones) must be affiliated with an Apple ID account to allow installation of mobile applications and use of the 'Find My iPhone' feature. Employees issued a City owned mobile device which requires affiliation to an Apple ID account will be required to create and maintain an Apple ID account that utilizes their City of Tempe (work) email address ending in tempe.gov domain. The employee will be responsible for maintaining access to the Apple ID account and the associated password.
- b. City owned Apple devices may not be affiliated to any personal Apple ID account.
- c. Personally owned Apple devices may not be affiliated to the employees City Apple ID account.
- d. Employees who are issued more than one City owned mobile device that requires an Apple ID account affiliation may associate both (iPhone and iPad) devices to a single account to facilitate data sharing and syncing between the devices. Both devices may be associated to the same work email address with a tempe.gov domain.

12. Department Issued Equipment

- a. Employees who are issued a mobile device will be required to have a protective case provided by the Department at all times. Replacement cases will be provided by the Department. Contact the Mobile Device Coordinator.
- b. Employees can purchase additional car and/or wall chargers for their mobile device and submit for uniform reimbursement. Employees, who receive a stipend in lieu of reimbursement, will be required to purchase the chargers from their stipend allocation.