

OFFICE OF THE CHIEF OF POLICE

ADMINISTRATIVE ORDER NO. 6

August 4, 2022

SUBJECT: CELLULAR TELEPHONES – REVISED AND RENAMED

PURPOSE: The purpose of this Order is to update the Department policy regarding the use and request for Department-issued cellular devices.

PROCEDURE: Department Manual Section 3/566, *Cellular Telephones*, has been revised and renamed, "*Cellular Devices*." Attached is the revised Department Manual section with the revisions indicated in italics.

AMENDMENT: This Order amends Section 3/566 of the Department Manual.

AUDIT RESPONSIBILITY: The Commanding Officer, Audit Division, shall review this directive and determine whether an audit or inspection shall be conducted in accordance with Department Manual Section 0/080.30.



MICHEL R. MOORE
Chief of Police

Attachment

DISTRIBUTION "D"

**DEPARTMENT MANUAL
VOLUME III
Revised by Administrative Order No. 6, 2022**

566. CELLULAR DEVICES.

Requests for Department-issued Cellular Devices. Requests for Department-issued cellular devices (e.g., iPhone Operating System [IOS], Android smartphones, tablets, smartwatches, and laptops) shall be submitted through Information Technology Division's (ITD) Computer Service Desk Portal, located on the Department's Local Area Network (LAN) page. The requestor's commanding officer shall review all requests and determine if the issuance of a Department-issued cellular device is in the Department's best interest before approving the request. Final approval for the issuance of cellular devices shall be the responsibility of the Commanding Officer, Information Technology Bureau. As the Department's cellular purchasing agent, Information Technology Bureau is the owner and administrator for the cellular contracts. Information Technology Bureau shall ensure that contracts and contract extensions are executed in a timely manner and participate in negotiating the pricing, service level, and terms of the cellular services contract.

Department Property. Cellular devices issued by the Department are Department property. Therefore, employees shall comply with Department requests to make the Department-issued cellular devices available during personnel complaints or other administrative investigations.

Use of Department-issued Cellular Devices. The use of Department-issued cellular devices has proven to be an effective supplemental method of communication with members of the Department and community. It is not intended to replace the Department's radio communications network. The use of Department-issued cellular devices should not interfere with an employee's duties or City business. Those assigned a Department-issued cellular device shall utilize these devices for conducting Department business, and exercise caution and good judgment on when and how to use them.

Employees accessing City and Department data, including email, with Department-issued cellular devices are required to adhere to all City and Department policies and guidelines related to confidentiality of information. Employees may use the camera, video and audio recording feature of the cellular devices, in accordance with Department policy. In addition, with the Department's unlimited data and messaging plan, personal phone calls and text messages are permitted on Department-issued cellular devices, provided that such use does not interfere with the performance of the employee's official duties.

Furthermore, Department-issued cellular devices shall not be used for unprofessional communications such as disseminating material or messages that are defamatory, sexually oriented, threatening, hateful or bigoted, or for promoting any political, religious, or personal business interests. In addition, the use of the Department-issued cellular devices (e.g., making or posting comments, likes, tweets, memes, statements, videos, screenshots, shared links, hashtags, and animated graphics) shall be consistent with the Law Enforcement Code of Ethics and the Department's Core Values and may be subject to review by the Department. If the Department becomes aware of words or conduct that violate Department policies or Core Values, disciplinary action may be initiated and may result in discipline and/or removal from the Department.

DEPARTMENT MANUAL
VOLUME III
Revised by Administrative Order No. 6, 2022

***Use of Personal Cellular Devices.** If an employee utilizes a personal cellular device for Department business, the data, communications and images related to Department business may be available for search pursuant to a search warrant.*

Employees are reminded of Department Manual Section 3/566.10 which explains Department expectations when utilizing personal devices during investigations, and Office of the Chief of Police Notice of November 4, 2020, "Invasion of Privacy: First Responders..." which highlights the California law prohibiting non-official use of certain photographs, and Manual Section 3/405, which emphasizes the confidential nature of Department records, reports, files, documents, photographs, images, etc.

***Safety of Department-issued Cellular Devices.** Employees shall be responsible for the security of Department-issued cellular devices and the information stored into them. Therefore, employees should carry the device with them and never leave a smartphone unattended in a public place. Employees are also required to maintain their smartphones and ensure they are charged, accessible and on alert (ringer or vibrate mode) while on-duty. If a Department-issued cellular device is lost and/or stolen, it shall be immediately reported to a Department supervisor. Additionally, Messaging/Mobile Services Section (MMSS), ITD, shall be notified as soon as possible at (213) 486-0330, or off-hours via the Department Operations Center at (213) 484-6700, as remote wiping and/or resetting of the device may need to be performed. Employees are also required to document lost and/or stolen Department-issued cellular devices on an Investigative Report, Form 03.01.00, and have it approved by a supervisor.*

To comply with the requirements set forth by the Federal Bureau of Investigation on the accessibility of Criminal Justice Information Services (CJIS), detailed on Section 5.13.2 of the CJIS Security Policy, cellular devices running a limited feature operating system (e.g., IOS and Android), shall be enrolled in the Department's Mobile Device Management (MDM).

***Mobile Device Management and GPS Tracking.** The Department will only use MDM GPS tracking capabilities for a lost and/or stolen device to obtain the approximate location of the device. To accomplish this, a message will be sent to the IOS device's home screen to notify the employee the device is locked, placed in lost mode, or if the device is reported lost/stolen. Lost mode can only be disabled by the MDM. Once disabled, the device will require the employee to re-enter their information to unlock the device.*

***Non-Budgeted Cellular Devices.** Cellular devices obtained and maintained through the Forfeited Assets Trust Fund or with funds from grants, gifts, private sources, or any source other than the ITD are deemed non-budgeted cellular devices. Requests for these cellular devices shall be routed through ITD's internal approval cycle. Such requests shall also include the source of funds for the purchase, installation, maintenance, and monthly bill. The concerned commanding officer shall ensure that applicable procedures are followed.*

DEPARTMENT MANUAL
VOLUME III
Revised by Administrative Order No. 6, 2022

Phone Operating Systems and Personal Apple Identifications. *Employees who choose to use personal Apple ID accounts on Department mobile devices are cautioned that the contents on Department devices are subject to the course and scope of Department administrative investigations.*

Training Coordinators. *Each division will be responsible for designating a Training Coordinator who will serve as the primary liaison between ITD and his or her division for all cellular phone related matters.*

Information Technology Division (ITD) *will assist the Training Coordinators in each division by providing information on standards, Department/employee responsibilities, porting numbers, device recommendations, security, and other related issues.*

Emergency Command Control Communications System Division (ECCCS) *will coordinate all necessary signal augmentation in police facilities with cellular services and ensure adequate signal strength. If a building has been augmented and is experiencing inadequate signal strength or poor call quality (dropped calls, poor reception, etc.), the Training Coordinator shall open a service request ticket via the ITD Computer Service Desk Portal.*

Return of Department-issued Cellular Devices. *Employees shall return their Department-issued cellular devices when the device is no longer required for their work assignment, pursuant to a court order, and/or upon separation from the Department. The Training Coordinator shall be responsible for collecting smartphones from employees departing from the Department. In addition, the Training Coordinator should ensure that the device is wiped via the mobile device manager and cellular inventory is updated to remove the departing employee from the inventory record. A factory reset does NOT remove the account or update the inventory records. If assistance is required to do this, the employee shall open a service ticket via the ITD Computer Service Desk Portal.*

Salvage of Cellular Devices. *Prior to salvaging any cellular device, all telephone numbers and any other information stored should be removed by restoring the device to its manufacturer's settings through a device factory reset. In addition, all identifying information, including employee names, division names, numbers, etc., shall also be removed from the cellular device, accessories, and batteries.*