Cocoa Beach Police Department
Standard Operating Procedure

Effective Date: June 26, 2023	**Replaces:**	**Number:** 306.00
Subject: Mobile Device		**Re-evaluation Date:** June 26, 2025
Distribution: All Personnel	**Related Standards:**	

This order consists of the following numbered sections:

1. Purpose
2. Scope
3. Policy
4. Definitions
5. Procedures
6. References

1. PURPOSE

The purpose of this policy is to establish guidelines regarding the use of mobile devices by Cocoa Beach Police Department members. All members who have been issued a mobile device by the City of Cocoa Beach are required to adhere to the City of Cocoa Beach Employee Guide regarding cell phones or similar devices and this policy.

2. SCOPE

This policy applies to all members of the Cocoa Beach Police Department.

3. POLICY

It is the policy of the Cocoa Beach Police Department that all mobile devices shall be utilized only for official Department business and that all operations be conducted in strict conformance with applicable FBI CJIS Security policy rules/regulations, City policy, and department directives.

4. DEFINITIONS

A. MEMBERS – All law enforcement and civilian personnel appointed by, and under the command of the Chief of Police or designee.

B. CITY NETWORK - Includes the City computer network and Police Department's computer network.

C. CRIMINAL JUSTICE INFORMATION SYSTEM (CJIS) DATA - Criminal Justice Information is the abstract term used to refer to all of the FBI CJIS provided data necessary for law enforcement agencies to perform their mission and enforce the laws, including but not limited to: biometric, identity history, person, organization, property (when accompanied by any personally identifiable information (PII), and case/incident history data. In addition, Criminal Justice Information (CJI) refers to the FBI CJIS-provided data necessary for civil agencies to perform their mission; including, but not limited to data used to make hiring decisions. The following type of data are exempt from the protection levels required for CJI: transaction control type numbers (e.g. ORI, NIC, FNU, etc.) when not accompanied by information that reveals CJI or PII.

D. MOBILE DEVICE - Smartphones, other mobile/cellular phones, tablets, E-readers, portable media devices, PDAs, portable gaming devices, laptop/notebook/Ultrabook/IPad computers, and any other mobile device capable of storing enterprise data and connecting to City resources.

E. PUBLIC RECORDS - Public records means all documents, papers, letters, maps, books, tapes, photographs, films, sound recordings, data processing software or other material, regardless of the physical form, characteristics, or means of transmission, made or received pursuant to law or ordinance, or in the connection with the transaction of official business by the agency.

5. PROCEDURES

A. CITY OWNED MOBILE DEVICES

1. The use of City issued mobile devices are limited to official business only, as described herein, unless an emergency exists. A personal (second private) line on any portable electronic device is not permitted. Limited personal use that does not interfere with the member's completion of his duty, and is of no cost to the agency, is authorized.

2. Members that are issued cellular phones are required to carry them on or about their person both while on duty and off duty when subject to call. Members are required to care for issued cellular phone in a reasonable manner. Members are further required to immediately report lost or damaged cellular phone to their supervisor. Supervisors shall refer to the City Employee Guide for Mishap reporting requirements.
3. Unless authorized by the Chief of Police or designee, members will not forward the issued cellular phones to their personal cellular phones.
4. All agency cellular telephones are required to have certain management services enabled on the issued equipment. Security applications (also known as mobile device management (MDM)) which are required to meet CJIS standards are installed on issued smartphones. Users will not attempt to modify, remove, or disable these applications. Users will notify the City of Cocoa Beach I.T. Department upon discovering or learning of any errors or issues involving the security applications.
5. The use of a mobile device to capture any City related documents, pictures, or other information as part of an employee's official duty is permitted for business purposes only. Disclosure of any such information to any third party through any means, without the express authorization of the Chief of Police or designee, may result in discipline up to and including termination.
6. Text Messaging – Text messaging for business purposes will be authorized. The City's Information Technology Department will be responsible for the capture of such text messaging to ensure compliance with Chapter 119 – Public Records Law and the Florida Retention law requirements.
7. Any collection of evidence whether it be photographic, audio, video or other format with an agency issued mobile device shall conform with all other policies, directives and standard operating procedures regarding the submission of evidence.
8. Members assigned a mobile device shall set up the device using only their official agency email account. Members shall connect to their Department issued laptop for the purposes of saving files too large to email that will be saved and entered into evidence in accordance with department policies.
9. Electronic Signatures – All mobile devices that have the capability to send and receive email shall be configured with the assigned user's electronic signature.

5. **REFERENCES**

City of Cocoa Beach Employee Guide

Wes Mullins
Deputy Chief of Police
City of Cocoa Beach

Date: 06/12/2023