GENERAL ORDER 13.4.1

Department Issued Smart Phones

GENERAL ORDER CROSS-REFERENCE: 13.3.7

SUMMARY

This policy establishes guidance regarding the issuance process for department smartphones, the appropriate use of City provided smartphones, technology prohibitions and considerations related to smartphone use.

DISCUSSION

The Springfield Police Department provides smartphones as tools for conducting City business. Smartphones are provided to improve the ability of employees to communicate internally and with the community, thus improving service quality, efficiency and timely delivery of information.

Department issued smartphones have the potential to contain CJIS information. Therefore, the data contained on the smartphone is subject to the CJIS security policy outlined in 13.3.7. The essential premise of the CJIS Security Policy is to provide appropriate controls to protect the full lifecycle of Criminal Justice Information (CJI), whether at rest or in transit. The CJIS Security Policy provides guidance for the creation, viewing, modification, transmission, dissemination, storage, and destruction of CJI.

The CJIS Security Policy integrates presidential directives, federal laws, FBI directives and the criminal justice community's APB decisions along with nationally recognized guidance from the National Institute of Standards and Technology

The CJIS Security Policy strengthens the partnership between the FBI and CJIS Systems Agencies (CSA), including, in those states with separate authorities, the State Identification Divisions (SIB).

The CJIS Security Policy provides a secure framework of laws, standards, and elements of published and vetted policies for accomplishing the mission across the broad spectrum of the criminal justice and noncriminal justice communities.

The Department will abide by the CJIS Security Policy as well as internal CJIS policies and practice.

This General Order is not intended to supersede City Policy or CJIS Security Policy but rather to enhance the policy.

POLICY

I

DEFINITIONS

Criminal Justice Information (CJI) - 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), and case/incident history data. In addition, 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, UCN, etc.) when not accompanied by information that reveals CJI or PII.

Digital Media – Any form of electronic media designed to store data in a digital format. This includes but is not limited to memory device in laptops, computers, and mobile devices; and any removable, transportable electronic media, such as magnetic tape or disk, optical disk, flash drives, external hard drives, or digital memory card.

Evidentiary Information: Any written correspondence, photo, recording, or other information taken, created, or documented in the ordinary course of police business that either is evidence of a crime, or that is reasonably likely to lead to the discovery of further evidence of a crime, whether that information pertains to either the possible guilt or innocence of a subject. Such information should be preserved both for investigation reasons and reasons related to the resolution of any charges in the criminal justice system.

Mobile Device Management (MDM) — Centralized administration and control of mobile devices specifically including, but not limited to, cellular phones, smart phones, and tablets. Management typically includes the ability to configure device settings and prevent a user from changing them, remotely locating a device in the event of theft or loss, and remotely locking or wiping a device. Management can also include over-the-air distribution of applications and updating installed applications.

Mobile (WiFi) Hotspot — A mobile (WiFi) hotspot is a zone or area associated with a mobile device (e.g. smartphone, air card) allowing wireless connectivity to the Internet typically through a cellular connection.

Smartphones – Pocket/Handheld mobile devices (e.g. smartphones) are intended to be carried in a pocket or holster attached to the body and feature an operating system with limited functionality (e.g., iOS, Android, BlackBerry, etc.). This definition does not include tablet and laptop devices.

II

Any department member assigned a smartphone shall carry or have available that device readily accessible while on duty. In some cases, members may be required to have their phone readily accessible while off duty, depending on specific job assignments that may require a call back or availability for consultation outside of normal work hours.

The Department recognizes the technological capabilities of smartphones to document and gather information; however, phones shall not be treated or used as body worn cameras.

Messages and data created, sent, stored or retrieved via Department owned equipment including but not limited to computers, telephones, voice mail, E-mail, pagers, modems, radios and FAX machines may be reviewed and audited by authorized City personnel. Such messages and data are City property and may be considered evidentiary information. When creating, sending, storing or retrieving such messages and data, employees should not expect confidentiality and have no right to privacy from the City. Department Members should be aware that all information placed on and transactions conducted on a city-issued smartphone are subject to public records laws and rules.

III

SMART PHONE ISSUANCE & REPLACEMENT

A list of the work units and positions authorized to receive smart phones will be kept by the designated department phone coordinator. Any variance from the established list requires written or email approval from the Division Commander. Members will contact the department phone coordinator for new and replacement phone requests. The department phone coordinator will track the replacement cycle of assigned phones to determine when members can receive a replacement. Members will be issued iPhones, unless other options are approved based on specific need by the Division Commander in consultation with the Department Phone Coordinator.

Members are reminded that Department issued phones are City property: therefore, members shall utilize a phone case that is designed to protect the phone. Members may use the phone case that is issued with the phone or they may purchase a personal phone case at their own expense. Members who have phones that are eligible for an upgrade or have phones that are unable to meet the operational needs will contact the department phone coordinator.

Members will immediately notify the phone coordinator in the event a phone is lost or stolen. The phone coordinator will work with the MDM (Mobile Data Management) provider to identify the current location of the phone. When reporting a lost or stolen phone, members must communicate what kind of information was stored or handled on the phone and specify if it contained confidential or sensitive data (e.g., Criminal Justice Information System (CJIS) information, crime scene photos, etc.). Members will write a memo to their supervisor to document damage, loss or theft of a department issued phone. The phone coordinator will coordinate the issuance of a new phone. Members separating from the department will return their smart phones to the phone coordinator on or before their last day of employment.

Smart phone location services (i.e., GPS), allows the Department to locate a member's phone in the event that is lost or stolen. The MDM provider continually updates the last known

GPS location of a member's smart phone; however, the GPS location services function does not keep or create record of these GPS updates. The GPS location services function does not permanently store or actively track a member's smart phone GPS coordinates, nor does it create or provide GPS historical data sets*. The Chief of Police, or a designee, may authorize the phone coordinator to pull the last known location of an individual member's smart phone in a situation that the Chief of Police reasonably believes that a member is or may be in imminent danger of serious injury or death. In a criminal investigation, the investigating authority would be required to follow all applicable laws and rules regarding the seizure of records pertaining to a member's smart phone historical data. This data is not stored by the Department and is not accessible by members of the Department. In such an investigation, a court order will be obtained that authorizes the activation and monitoring of the GPS location services of a member's assigned smart phone. This court order would be required to be served to the service provider of the cellular phone and would be limited by the capabilities of the service provider. Members requesting additional functionality or applications for their smart phone will submit a memo through their chain of command explaining the reason. Members will address specific solution(s) if identified, any costs related to the solution(s), and the added benefit from the expanded functionality.

To prevent security vulnerabilities on the police network, IT will audit all phones on an ongoing basis. Any unauthorized applications found on a phone will be removed. All Department issued phones can be accessed by IT. Members should use discretion when deciding to store information on in their phones. Members should be aware that government email accounts do not automatically synchronize with smart phones unless members update their network password on both their computer workstation and Department issued smart phone.

Members who are unable to log into their smart phone after repeated attempts at passcode entry and receive a warning on the phone's screen should contact IT immediately to reset their passcode. Members in need of troubleshooting and/or technical assistance with their smart phone should contact IT. In the event that IT cannot resolve an issue, or the phone is determined to be faulty, members will contact the phone coordinator for a replacement phone.

IV

PROHIBITED ACTIVITIES

Employees are strictly prohibited from using Department issued smart phones in connection with, by way of illustration but not of limitation, any of the following activities:

- Violations of current CJIS Security Policy, which can be found on the Oregon State Police LEDS website.
- Engaging in illegal, fraudulent, or malicious conduct.
- Working on behalf of organizations without any professional or business affiliation with the City; or working on behalf of organizations with such affiliation but outside of the specific City business with them.
- Sending, receiving, or storing offensive, pornographic, obscene, or defamatory material that is not related to a member's official duties.
- Soliciting or supporting political or religious causes or beliefs.
- Annoying or harassing other individuals, including any prohibited form of harassment.

- Downloading or running materials including screen savers, music or streaming video off the web without previous authorization from their department director.
- Downloading software off the web without previous authorization from the Information Technology Department.
- Obtaining unauthorized access to any computer system.
- Using another individual's account or identity without explicit authorization of the individual, unless this is approved by the director of IT or the City Manager.
- Distributing or storing chain letters, jokes, solicitations, junk mail, offers to buy or sell goods, or other non-business material of a trivial or frivolous nature.
- Giving non-City employees or other users not authorized by a department director access to the Internet, City Network, E-mail, or computers.
- Purchasing, acquiring or installing software or hardware without previous authorization from the Information Technology Department.
- Streaming music, videos, movies or television programs not specifically related to their duties.
- Accessing personal media accounts on Department issued phones (such as iTunes, Spotify or Facebook);
- Installing Applications (Apps) not authorized by the Department.
- Disabling location services, as this allows the Department to locate a member's phone in the event that it is lost or stolen.
- Utilizing iCloud or similar cloud-based storage.
- Forwarding information related to CJI data to a personal phone.
- Connecting to public Wi-Fi
- Factory resetting or modifying a Department issued phone's operating system
- Utilizing the phone's Airplane mode function
- Utilizing the phone's Bluetooth function unless for a required purpose (AirDrop may be utilized for the transfer of non-CJI data photographs and videos)
- Enabling the phone as a mobile hotspot
- Changing the phone's screen timeout settings
- Utilizing mobile storage (media cards)
- Disabling software installed automatically by the MDM
- Personal use of department issued smartphone unless exigent circumstances arise (such as personal device being unavailable). Such use should be limited and remain brief.

III

Employees violating this policy may be subject to discipline, up to and including termination of employment. Furthermore, employees using department issued smartphones for defamatory, illegal, or fraudulent purposes also may be subject to civil liability and criminal prosecution. Any employee who knows or should have known of a violation of this policy shall inform a supervisor or command officer immediately.

It is noted that employees are also subject to the provisions of ORS 164.377, Computer Crime. Under U.S. Copyright Law, illegal reproduction of software can be subject to civil damages of as much as $100,000, per occurrence, and criminal penalties including fines and imprisonment.

VI

CAPTURING EVIDENCE FROM PHONES

All pictures and videos taken on a Department smart phone are official public records and shall be retained. Members must follow the established processes for uploading evidentiary pictures and videos from their phone to the Digital Evidence System (currently Getac). Members will direct any issues and questions regarding the process to the Digital Evidence Technician. If a member uses a phone to record images from another video recording device, the member shall ensure that the original evidentiary video footage is also obtained in accordance with normal evidence collection procedures, when practical.

Pictures, voicemail messages, voice recordings/memos and any other media or communications stored in a phone that is deemed as evidentiary information by law enforcement or judicial entities shall be retained. Members are responsible for ensuring that evidence is transitioned to the appropriate system for retention. If there are any questions about what information is defined as evidence, what systems are appropriate, or the method of transitioning information from the phone to the appropriate system, the member shall contact their supervisor.

Text messages will be automatically downloaded in real time to a CJIS compliant archiving system in order to comply with state records retention laws.

Andrew Shearer
Chief of Police