Rockville City Police Department
GENERAL ORDER

Subject **DEPARTMENT ISSUED CELL PHONES**		Procedure **G.O. # 5 - 31**
Authorizing Signature	**Effective: 08-29-18**	**Total Pages** **3**

I. POLICY

Department-Issued Cell Phones (DICP) will be provided to all sworn Rockville police personnel who, by the nature of their jobs, have a routine and continuing business need for use while conducting official City business.

II. PURPOSE

The purpose of this General Order is to establish the uniform use of DICP's for authorized Rockville police department personnel.

III. GENERAL

A. While Maryland law prohibits the use of handheld cellular devices when operating a motor vehicle, this restriction does not apply to law enforcement and emergency services personnel acting within the scope of their official duties. However, while driving a department vehicle, personnel shall not use any cell phone to text, e-mail, or communicate in any other manner that would cause them to take their focus away from their driving responsibilities. This includes reading and/or sending messages. Department personnel may use a hands-free device (Bluetooth) while driving. The safe operation of a department vehicle will always take precedence over the use of any cell phone.

B. Personnel shall have no expectation of privacy with regard to any communication made with or stored in or through the department issued cell phone issued by the Department and shall have no expectation of privacy in their location should the device be equipped with location detection capabilities. The use of a DICP is without any expectation of privacy that the employee might otherwise have in any communication, including the content of any such communication. Communications or data reception on personal, password-protected, web-based e-mail accounts and any other services are subject to monitoring if department equipment is used.

C. In accordance with this policy, supervisors are authorized to conduct a limited administrative inspection of electronic files and downloaded applications without prior notice, consent or a search warrant, on DICP's that have been used to conduct department-related business. Administrative inspections can take place for work-related purposes that may be unrelated to investigations of employee misconduct and, as practicable, will be done in the presence of the affected employee. All such inspections shall be documented in a written report.

D. Access to the Internet is intended for official work-related business only. The Internet shall not be used for any unprofessional and/or illicit purposes.

E. Personnel will be responsible for any unauthorized financial responsibilities incurred while using the DICP, to include roaming charges and initial/recurring application fees.

IV. PROCEDURES

A. Sworn personnel will ensure the DICP is configured to receive communications while on-duty, to include special events, and while working in any department funded overtime capacity, and:

1. Ensure the phone is charged.

2. Keep the phone "on" at all times except in those circumstances where it may be considered disruptive or a distraction.

3. Keep the phone on their person(s) or close enough to their person to answer a call or text message that may be work related.

4. Respond to all calls that are work related within the members current tour of duty or the next scheduled work day.

B. The DICP is classified as issued duty gear and must be maintained and safeguarded in the same manner as all other assigned duty gear. Any loss, damage, or theft must be reported to a supervisor immediately and handled in accordance with department and City policy. Personnel may be subject to disciplinary action for any misuse, neglect, or loss of the DICP, as well as financial liability.

C. The DICP will be housed in a department issued, plain black, ruggedized case. No adornments are authorized.

D. Only department approved applications may be installed on the DICP. Personnel are prohibited from downloading and installing any social media, gaming, or utility applications on the DICP unless authorization has been obtained from the Chief of Police, or designee.

E. Personnel needing an application on their DICP for official law enforcement purposes must submit a written request to the Chief of Police or designee, via their chain-of-command identifying the application and the specific law enforcement need.

F. Photographic images viewable on the DICP home screen, or other internal screens may not be offensive or contain otherwise inappropriate images.

V. SECURITY

A. All DICP's will be required to have a 4-digit passcode. The Office of the Chief of Police or designee will maintain passcodes. Personnel changing their passcode must notify the Chief of Police via their chain-of-command immediately.

B. All DICP account information, log-on credentials and account passwords will remain under the control of the Office of the Chief of Police, or designee. Personnel are prohibited from changing, or attempting to change, any account information, log-in credentials, or account passwords without the express written consent of the Chief of Police, or designee.

C. The DICP Passcode will be set to engage after 1 (one) minute of inactivity and the "Erase Data" feature will be turned on to erase all data after 10 failed passcode attempts.

D. The DICP will not be stored unattended in public places or left in a vehicle overnight. If a DICP must be left unattended in a vehicle for short period of time, it must be concealed and out of sight.

VI. DEPARTMENT ISSUED CELL PHONE USE

A. DICP's are an augmentation to the department's communication system and not a substitute for radio communication, i.e. (car to car). DICP's are to be used as a secondary form of communication. Approved DICP usage includes, but is not limited to the following types pf communication:

1. Conveyance of sensitive or restricted information.

2. Undercover or special assignments.

3. Lengthy communication with supervisors or designee.

4. Communication beyond normal radio range.

5. Incidents in which direct communication with employee is critical.

B. Personnel are authorized to use their assigned DICP for limited personal use that does not involve long distance or roaming charges, such as:

1. Brief and infrequent phone calls to family and friends.

2. Scheduling medical and other routine personal appointments.

3. Brief communication, including long distance service while in official travel status to office, family, or friends as appropriate to convey information and communicate schedule changes.

C. Personnel are prohibited from using their DICP for the following:

1. Any call made in relation to personal gain by employees or employees' friends or relatives.

2. Any call for personal entertainment.

3. Transmission of any material in violation of any City, State or Federal law or regulation, as well as accessing or transmitting materials, other than that required for official police business, that involves the use of obscene language, images, jokes, sexually explicit materials, or messages that disparage any person, group, or classification of individuals is strictly prohibited, whether or not a recipient has consented to or requested such material.

VII. DECOMMISIONING OR DEVICE REASSIGNMENT

All data, settings and content will be removed from the DICP and restored to factory default prior to reassignment to another sworn officer, or when the DICP is decommissioned.