SUBJECT: RULE 406 – MOBILE DEVICE POLICY

Rule 406 - Mobile Device Policy, is hereby issued superseding all previous rules, special orders, memos and directives on this subject.

This rule is effective June 3, 2019.

Commanding Officers shall ensure that this order and the attached Rule are posted on Department bulletin boards.

William G. Gross
Police Commissioner
MOBILE DEVICE POLICY

1. Purpose and Scope: The purpose of this policy is to define standards, procedures and restrictions for the use of Department-issued smartphones and mobile devices. This policy applies to all employees, including contractors, who are issued a mobile device for Boston Police Department (BPD) business. Employees are not required to utilize their mobile devices while off-duty, unless functioning in an on-call capacity.

Prior to receiving a Department-issued mobile device, employees must review the regulations set forth herein and complete any training required by the Department.

2. Roles and Responsibilities: The Department will determine who shall receive a Department-issued mobile device for use in the performance of his/her duties based on Department need and availability of devices.

All employees are expected to exercise the same discretion using the mobile device as they are expected for the use of desk phones and computers.

Employees issued a mobile device do not have an expectation of privacy in anything viewed, created, stored, sent, or received on a Department-issued mobile device. All information on these devices may be subject to public records law and its regulations. Employees are reminded that all mobile devices and content on the device remain the property of the Department.

Sec. 2.1 Lost or Stolen Property: If the Department-issued mobile device or related equipment is damaged in the course of business, officers must bring the equipment to the Telecommunications Division for repair/replacement. Employees must immediately report lost or stolen equipment to the employee’s supervisor and the Telecommunications Division so that the service can be cancelled on the device. Employees are expected to protect Department-issued equipment from loss, damage or theft.

Sec. 2.2 Returning of Equipment: Upon resignation or termination of employment, or at any time upon request by the Department, the employee must produce the equipment for return or inspection. Employees who are unable to present the equipment in good working condition due to negligence or misuse within the time period requested may be required to provide the cost of a replacement.

3. Smartphone/Mobile Device Conduct: Users of Department-issued mobile devices must abide by all standards of professional behavior and conduct.
Department-issued mobile devices cannot be used to discriminate in any way based upon an individual’s race, color, national origin, religion, disability, age, citizenship status, creed, ancestry, military status, sex, sexual orientation, gender identity, genetic information or membership in any other class protected under federal or state law.

Some additional examples of conduct in violation of these standards include, but are not limited to:

a. communication of information that disparages, threatens, or harasses others;
b. knowing receipt or communication of sexually explicit material, propositions or suggestive remarks; or
c. knowing receipt or communication of aggressive material including violence, abuse, obscenities or material that promotes illegal acts.

Subsections a) through c) shall not apply to material received or sent related to an investigation or as needed in the course of an individual’s official duties.

4. Personal Use of Department-Issued Mobile Devices: The Department allows limited, reasonable, personal use of Department-issued mobile devices with the knowledge that all use of Department-issued mobile devices may be monitored and subject to Department policy and public records laws. In addition to the standards of conduct set out above in Section 3, personal use of Department-issued mobile devices must not incur a cost to the Department, disrupt the workplace, interfere with work responsibilities, or cause embarrassment to the Department. The personal use of any social media applications shall conform to Rule 102 (The Conduct and General Rights and Responsibilities of Department Personnel), and if used by an employee in the course of their job duties, shall also conform to Section 5.1 below.

Employees using a Department-issued mobile device for personal use do not have an expectation of privacy in anything viewed, created, stored, sent, or received on a Department-issued mobile device. All information on these devices may be subject to public records law and its regulations. Employees are reminded that all mobile devices and content remain the property of the Department.

5. Mobile Device Applications: Upon receipt of a Department-issued cell phone, employees may download additional applications that serve a business-related purpose.

While on duty, employees will be responsible for the information provided through Department-installed applications, as it pertains to their assignment and job description. Should any Department-installed application experience any issues or become non-functioning, it is the responsibility of the employee to notify his/her supervisor for maintenance. Supervisors shall notify the Unit responsible for the application about related issues, as soon as possible.

All employees must ensure that system software and Department-installed applications are current and updated. Users will be notified of available updates directly on the device and must follow instructions for downloading and updating the device. Users should contact the Telecommunications Division for assistance, as necessary.
Section 5.1 Department-Sanctioned Social Media Uses: The Department permits use of social media applications for work use only as it pertains to job responsibilities. The use of any social media applications shall conform to Rule 102 (The Conduct and General Rights and Responsibilities of Department Personnel). Investigatory uses are not outlined in this rule.

a. Community Outreach: Employees authorized to do so as part of their job function may use social media for community outreach and engagement, provide crime prevention tips, offer online-reporting opportunities, share crime maps and data, respond to citizen inquiries, and to promote Department events.

b. Notifications: Employees authorized to do so as part of their job function may use social media to make time-sensitive notifications including but not limited to road closures, special events, weather emergencies, missing or endangered persons, and public safety emergencies.

c. Hiring and Recruitment: Employees authorized to do so as part of their job function may use social media to recruit potential employees and/or volunteers, as well as assist in the hiring process.

6. Text Messages/Emails: Employees are reminded that all work product, including text messages, must be preserved in accordance with existing Department policy or legal requirements. In the event that text messages and/or emails are sent and/or received relative to an investigation or official duties, employees are prohibited from deleting the substance of communication from the mobile device prior to preserving the communication in another manner.

7. Camera/Video Capabilities: Department-issued mobile devices may have camera and video capabilities. Employees should be aware that any photographs and/or video taken with a Department-issued mobile device may be subject to discovery obligations and public records laws that require the production of these materials.

Methods of capturing and preserving photographs and/or video evidence on Department-issued mobile devices shall be in accordance with Rule 331 of the Department's Rules and Procedures. Officers are required to use existing procedures for video, photographic, and/or digital evidence unless authorized by a Commanding Officer. Any deviation from existing procedures shall be documented in a Form 26 and provided to the appropriate Bureau. Employees must preserve any such photographs and/or video evidence prior to deleting them from the device.

8. Terms of Acceptance: Employees who receive a Department-issued smartphone or mobile computing device will abide by the following conditions:

- The Department reserves the right to remotely configure the device. This includes remotely setting services and installing/uninstalling applications. These may include location-based services and applications running on the phone or device, such as “Find My Phone” so that a lost or stolen device can be located.
Employees must maintain a cloud-based account on the device utilizing their Department email address as the user ID. The retention of all account information and passwords is the sole responsibility of the employee.

Should an employee’s Department-issued mobile device become lost or stolen; an immediate attempt will be made, by the employee, to locate the device using a cloud-based account. The employee must be in possession of the cloud-based account password to complete this process. If the device cannot be located as a result of failure to follow this process, the replacement cost of the device may be the responsibility of the employee.

Employees who require the use of their Department-issued mobile device outside of the coverage area for work-related purposes are required to contact the Telecommunications Division in writing at least one week prior to travel to request a change to global coverage, if feasible. The Telecommunications Division will respond with approval or denial of the request.

Employees, not previously authorized to do so, who use a Department-issued mobile device outside of the existing coverage area are responsible for any data, voice roaming or other charges incurred as a result. Employees shall check with Telecommunications to identify out of coverage areas prior to travel outside of the country.

Employees who receive a Department-issued smartphone or mobile device acknowledge that the content of all text messages (SMS and other types of messages) and phone logs associated with the cellular access account supplied by the Department are and remain the property of the Boston Police Department.

Phones are to be used to increase efficiency in the performance of job duties.

William G. Gross
Police Commissioner