DEPARTMENTAL GENERAL ORDER

I-19: ELECTRONIC COMMUNICATION DEVICES

Effective Date: DD MMM YY
Coordinator: Bureau of Services

The purpose of this policy is to set forth Departmental policy on the use of Department-issued cellular phones, the use of other Department-issued electronic devices, and the use of personal cellular phones on duty. This policy includes direction on training and audit procedures.

A. DEPARTMENT-ISSUED CELLULAR PHONES

A - 1. Issuance and Control

All sworn members shall be issued a Department-issued cellular phone ("work cell phone") upon appointment to a full-time sworn position. Annuitants and reserve sworn members may be issued a work cell phone as directed by the Chief of Police or designee.

All professional staff members at the rank of supervisor and above shall be issued a work cell phone within 90 days of appointment to the Department.

The Chief of Police or designee may authorize the issue of work cell phones to members beyond those described above, including issuance of multiple phones to a single member.

Work cell phones are property of the Department and shall be issued and controlled by the Department's Information Technology Unit (ITU), with management of the device apps and settings by the City's Department of Information Technology (DIT).

A - 2. Carry Requirements for Sworn Members

All sworn members shall carry their work cell phone when they are on duty, except where this requirement would interfere with their safety or duties (e.g., undercover or plainclothes assignment), where they are precluded from carrying the phone by rule or law (e.g., court appearances), or when permitted or ordered not to by a supervisor or commander.

Sworn command officers (rank of Lieutenant and above and those who are acting in those ranks) shall have their work cell phone accessible at all times, on and off duty, with the following exceptions:

1. Where this requirement would interfere with their safety or duties (e.g., undercover or plainclothes assignment);
2. Where they are precluded from carrying the phone by rule or law (e.g., court appearances, events specifically precluding the use or carrying of cell phones);
3. When permitted or ordered not to by a higher-ranking member; or

4. While on vacation, compensatory (comp) time, or other leave and there is a substitute or acting commander available in their stead.

A - 3. Carry Requirements for Professional Staff Members

Professional staff members who are issued one shall carry their work cell phone when they are on duty, except where this requirement would interfere with their safety or duties (e.g., undercover or plainclothes assignment), where they are precluded from carrying the phone by rule or law (e.g., court appearances), or when permitted or ordered not to by a supervisor or commander.

Professional staff members at the position of manager and above (and those acting in those ranks) shall have their work cell phone accessible at all times, on and off duty, with the following exceptions:

1. Where this requirement would interfere with their safety or duties (e.g., undercover ~~or plainclothes~~ assignment);
2. Where they are precluded from carrying the phone by rule or law (e.g., court appearances, events specifically precluding the use or carrying of cell phones);
3. When permitted or ordered not to by a higher-ranking member; or
4. While on vacation, comp time, or other leave and there is a substitute, ~~or~~ acting manager, or superior available in their stead.

A - 4. On-Duty Use of Work Cell Phones

Work cell phones are ~~primarily~~ meant to allow members to conduct official department business. Work cell phones supplement the use of fixed-position office phones and allow for remote meeting support.

Formatted: Font: Bold

Members are reminded that work cell phones, because of their nexus to job-related activities, may be the subject of public records requests, subpoenas, and discovery requests.

Members are encouraged to not conduct any personal business on their work phone, and any actions taken using the phone must comply with this policy and its prohibitions (see section C for specific prohibitions). Any ~~on-duty~~ personal ~~calls or messages on~~use of a work cell phone shall be kept to a minimum and be brief. Examples include, but are not limited to:

Commented [TJ1]: Tightened up this section without overreaching

1. Calls to notify family members, physicians, etc. regarding an injury on the job; or
2. Calls to notify family members when required to work overtime without advance notice~~;~~. ~~and~~

~~3. Daily calls to speak to family members, partners, friends (or those responsible for them such as school, day care, or senior center) to check on their well-being.~~

Commented [TJ2]: Excise or talk about articulable emergencies.

A - 5. International Use of Work Cell Phones

Members who are traveling outside of the United States of America for official business, and who bring a work cell phone or other work electronic device with mobile data, shall contact the ITU at least one (1) week prior to their departure date so that the device can be moved to an international data plan.

A - 6. Evidence Procedures

Electronic material (e.g., pictures, audio, text messages, electronically generated messages) potentially related to a criminal or internal investigation and recorded on work cell phones shall be handled as evidence.

A - 7. Confidentiality and Reporting of Lost Phones

Department work phones and any confidential material stored therein shall be treated as sensitive material and shall be secured at all times.

Lost or stolen devices shall be reported pursuant to DGO N-05, with an information copy to ITU.

B. OTHER DEPARTMENT-ISSUED ELECTRONIC DEVICES

B - 1. Issuance and Control

Workstation computers purchased through ITU shall be assigned to specific work spaces by the ITU. Laptop computers purchased by ITU may be issued to specific members based on assignment. Any ITU issuance of laptop computers shall be with the written approval of a Deputy Chief/Director or higher. Costs for laptop computers shall be paid from the requesting unit's funding code.

All other computers shall be issued by the unit purchasing the computer, and units purchasing computers shall pay for the computers using their funding codes. Control over programs and administration of computers connecting to the City's networks shall continue to be with DIT.

Other electronic devices, if not issued and controlled by ITU (e.g., robots, throw-phones, GPS trackers) shall be issued and controlled by the Unit/Section/Division which oversees that program, or as directed by policy.

B - 2. Work-related Use

Members may use electronic devices assigned to them or their unit for work-related functions.

Members may use the desktop or laptop computer assigned to them or their unit for appropriate personal business while on break (e.g., perusing the news). However, see section C, below, for prohibited activity.

B - 3. Devices with Specific Policies

Electronic devices with specific policies (e.g., as a result of Surveillance Technology Ordinance or Militarized Equipment Ordinance) shall be used and issued according to those policies. If any provisions in a device-specific policy conflict with this policy, the provisions in the specific device policy shall supersede this policy.

B - 4. Confidentiality and Reporting of Lost Devices

Work electronic devices and any confidential material stored therein shall be treated as sensitive material and shall be secured at all times.

Lost or stolen devices shall be reported pursuant to DGO N-05, with an information copy to ITU.

C. PROHIBITED ACTIVITY FOR DEPARTMENT-ISSUED CELL PHONES, PERSONAL CELL PHONES, AND ELECTRONIC DEVICES

C - 1. Use of Any Device to the Point of Distraction or Interference with Duty

Members shall not utilize work or personal cell phones, other telecommunications devices, or personal electronic devices to the point of distraction from their performance of duty or interference with their safety.

C - 2. Use of Cell Phones While Driving

Members shall not operate a Department vehicle while using a cell phone, whether work or personal, unless they are using a hands-free device or unless exigent circumstances exist. Use of a cell phone as a GPS navigation tool or to play work-appropriate music while driving is specifically exempted from this prohibition.

C - 3. Use of Personal Cell Phones for Department Business

Members are prohibited from using their personal cell phones or electronic communication devices for Department business except for the following:

1. Members may use city email for official business on their personal phone;

~~1.~~2. Members who have timecard approval responsibilities may approve timecards on their personal phone;

~~2.~~3. Members who do not have access to their work cell phone may make urgent work-related phone calls or text messages from their personal phones; and

~~3.~~4. Members who are not issued a work cell phone may conduct administrative work-related business (e.g., call in to the office, submit or approve timecards, etc.) using their personal cell phone.

Members shall not monitor or operate work-related social media accounts from personal cell phones (e.g., forward-facing social media accounts that represent the Department or investigative social media accounts). This

Commented [TJ3]: Added - staff expressed concerns as many use phones to navigate to calls and listen to music in their vehicles.

Formatted: Font: Bold

Commented [TJ4]: Explain more to the officers – what is work related? Have some examples that can guide people's understanding. Check NYPD patrol guide.

Commented [TJ5R4]: Added a few lines here

prohibition does not preclude members from engaging in non-work-related social media contacts with other members using their personal devices (e.g., being "friends" on social media, connecting over social media with other Department members regarding shared hobbies or interests, etc. Refer to DGO D-18, however, for rules around personal social media use.).

C - 4. Use of Work Cell Phones and Work Electronic Devices for Personal Business

Except for permissible brief personal use (see sections A-5 and B-2, above), work cell phones and work electronic devices shall not be used for personal business.

Without exception, no personal social media[1] accounts or applications ("apps") shall be accessed or installed on work cell phones or electronic devices (Reference DGO D-18 regarding personal social media). This does not include social media applications used for work purposes (e.g. investigative purposes or for administering and posting on the Department's public accounts).

Commented [TJ6]: Add link here

Commented [TJ7R6]: Done

C - 5. International Data Access and Charges

Members must have permission from their first-level commander to bring work cell phones or electronic devices outside of the United States of America. Members who bring a work phone or work electronic device outside of the United States of America shall be responsible for any surcharges, fees, or increased data or calling charges that result unless the device is moved to an international plan as specified in section A-5.

C - 6. Tampering with or Modifying Work Cell Phones and Work Electronic Devices

Work cell phones and work electronic devices shall not be physically modified or tampered with without express written permission from the ITU. This includes, but is not limited to, the following:

1. Removing the SIM (subscriber identity module) card from a work cell phone or device and installing it into a personally owned phone and
2. Adding or removing hardware such as RAM, disc drives, or motherboards to department computers.

This section does not limit using appropriate peripheral devices such as USB memory sticks, plug-and-play external hardware, or speakers.

C - 7. Accessing Inappropriate Material on Work Cell Phones and Electronic Devices

[1] [Policy and Publication Unit Note: This footnote is reserved for the definition of "personal social media" in DGO D-18 when that policy is finalized.]

Members are prohibited from accessing inappropriate content on their work cell phones and electronic devices when it is not within the scope of their duties – this behavior is prohibited by the Department's Manual of Rules. This includes, but is not limited to, the following:

1. Pornography (MOR 356.30).
2. Any material which violates the anti-harassment or anti-discrimination policies of the Department (DGO D-20) and/or City (Administrative Instruction 71) (MORs 356.30, 314.04).
3. Hate group, racist, or anti-government material[2] (MORs 356.30, 384.70).
4. Gambling websites or applications (MORs 356.30, 328.07).
5. Any material related to the member's outside commercial or personal financial activity (MORs 356.30, 328.07).

D. ~~AUDITING~~ INSPECTION AND AUDITING OF DEPARTMENT CELLULAR PHONES AND ELECTRONIC DEVICES

D - 1. Definitions

Inspection – inspections of work cell phones include reviewing of call logs, messaging apps, browsing history, and social media applications with the purpose of reviewing the device for policy compliance in an efficient manner. Inspections will necessarily be limited in scope and intensity but may lead the inspecting member to perform a deeper look at the phone. Inspections involve reviewing the devices and records from the device, but do not involve using a digital forensic tool.

Audit – audits of work cell phones include using a digital forensic tool to extract the entirety of the data stored on the phone, possibly including deleted data, for the purpose of reviewing the device~~s~~ for policy compliance. Audits involve an expanded scope and significantly more intensity than inspections, and will typically have a planned review to significantly sample and examine the data extracted from the device.

Search – searches are a focused attempt to find something (e.g. evidence of misconduct or criminal activity, or specific communication that could prove or disprove an allegation of misconduct) that could reasonably exist on the device. The scope and intensity of a search, and the use of digital forensic tools to conduct a search, will depend on what is being searched for.

[2] Reference the definition in DGO D-18 of extremist content: Content that advocates for, celebrates, or otherwise furthers the cause(s) of extremist political, racial, or gender-based positions or groups that espouse violence, a denigration, "othering", or subjugation of another person or people based on the actual or perceived race, color, religion/religious creed, national origin/ancestry, sex, age, marital status, personal appearance, sexual orientation, gender identity or expression, family responsibility, homelessness, physical and/or mental disability, matriculation, political affiliation, pregnancy, medical condition, military or veteran status, or status in any other group protected by federal, state or local law or the putting down of persons for personal attributes or political beliefs.

Commented [TJ8]: Cite and refer back to MOR sections – each of these.

Commented [TJ9]: Bringing language from Social Media policy (which had

Commented [TJ10]: Need some definitions here, especially around inspection, audits, searches

Commented [J11R10]: Added

Formatted: Font: Bold

Formatted: Font: Bold

Formatted

Formatted: Indent: Left: 0", First line: 0"

~~D - 1.~~D - 2. Right of Department to Inspect Work Cell Phones and Electronic Devices at Any Time

The Department may inspect or audit ~~,~~ work cell phones and work electronic devices at any time. Such inspections or audits ~~,~~ shall not be arbitrary, capricious, or harassing, and shall not be based on personal bias or animus.

Supervisors and commanders may conduct inspections of the work phones of members in their chain of command. Inspections of work cell phones or electronic devices by supervisors or commanders outside of planned or ~~/~~ordered inspections, audits, or investigations shall be documented in a memorandum to the Captain of Internal Affairs, no matter the outcome of the inspection.

D - 3. Department Work Cell Phone Inspection Plan

Bureau Threshold Inspections

1. BRM will complete a written inspection plan within 180 days of this policy being signed, and will review the plan at least every two (2) years subsequently.
2. The BRM inspection plan will utilize thresholds based on data points such as:
   - **a.** Number of citizen complaints which are associated with misconduct
   - **b.** Uses of force
   - **c.** Amount of data used during the review period

   To develop a list of at least twenty-five (25) members assigned a work cell phone per Bureau.

   From the list for each Bureau, the BRM shall, at the beginning of each quarter (January, April, July, and October) randomly select[3] at least four (4) per Bureau and send the names to the respective Bureau Deputy Chief or Director.

   The Bureau Deputy Chief or Director shall direct the work cell phones of the members on the list **inspected** (see definition in section D-1) by supervisors or commanders in the Bureau.
3. Random inspections pursuant to thresholds shall be done by a member at least one rank higher than the member to whom the phone is assigned.
4. Violations of this policy noted during the inspections shall be reported and handled pursuant to DGO M-03.

[3] Random selection shall be accomplished by using a random number generator, with a minimum of 1 and a maximum of 25, where the numbers generated will correspond to the row or column upon which the member's name exists in the spreadsheet or data ~~collection tool~~array.

Commented [TJ12]: Check this here along with D-3

Commented [J13R12]: Made this inspection and audit, kept searches the same.

Commented [TJ14]: DGO N-12: An examination that focuses on a specific task, activity, or event in order to ensure compliance with a policy, procedure, rule, or directive.

VS

Audit: A methodical, extensive and detailed examination or analysis. An audit is more general in nature than an inspection and may involve reviewing a previous inspection or conducting a new one.

Formatted: Underline

Formatted

Formatted: Font: Bold, Underline

Formatted: Font: Bold

Formatted: Font: Bold

Formatted: Font: Bold

Formatted: Font: Bold

Formatted: Font: Bold

Formatted: Indent: Left: 1", No bullets or numbering

Formatted: Indent: Left: 1", No bullets or numbering

Formatted: Font: Bold

Formatted: Font: Bold

Formatted

Formatted: Font: Bold

Formatted: Font: Bold

5. The inspections ~~must~~shall be completed by the end of the quarter (March, June, September, December), and the results of these inspections shall be documented in the monthly management report (or in a memorandum to the Assistant Chief of Police with an information copy to IAD for sections that do not complete monthly management reports). If the member randomly selected is unavailable for the entirety of the quarter (e.g., on military leave, on injury leave, etc.) this shall be noted in the report or memorandum.

Integrity Unit Random Audits

1. The IAD Integrity Unit shall conduct a quarterly audit of no less than two (2) randomly selected[4] work cell phones, with the audits conducted in accordance with Integrity Unit operating procedures. The results of these audits shall be documented in a quarterly memorandum to the IAD Commander.

~~D - 2. Integrity Unit Inspections of Work Cell Phones~~

~~The IAD Integrity Unit shall conduct a quarterly inspection of no less than four (4) randomly selected[5] work cell phones, with the inspections conducted in accordance with Integrity Unit operating procedures. The results of these inspections shall be documented in a quarterly memorandum to the IAD Commander.~~

~~D - 3.~~D - 4. **Department Searches of Work Cell Phones and Electronic Devices**

In addition to inspections and audits, as detailed above, ~~T~~the Department may also search work cell phones and work electronic devices when there ~~is~~ are reasonable grounds for suspecting that the search will reveal evidence of work-related misconduct or criminal misconduct.

~~D - 4.~~D - 5. **Internal Record Keeping and Asset Management**

The ITU shall keep a record of issued work cell phones. This shall include, but is not limited to:

1. Phone number, if applicable
2. Device serial number or identifying number
3. Member assigned the device(s)

[4] Random selection shall be accomplished by using a random number generator, with a minimum of 1 and a maximum of the number of the total lines in the work phone record mentioned in D-4, and matching the first two (2) (or as many numbers need to be generated to gather the requisite number of phones to be inspected) random numbers generated to the row of the work phone record mentioned in D-4.

[5] ~~Random selection shall be accomplished by using a random number generator, with a minimum of 1 and a maximum of the number of the total lines in the work phone record mentioned in D-4, and matching the first four (4) (or as many numbers need to be generated to gather the requisite number of phones to be inspected) random numbers generated to the row of the work phone record mentioned in D-4.~~

Formatted: Font: Bold

Formatted: Underline

Formatted: Font: Bold, Underline

Formatted

Formatted

Formatted: Font: Bold

Formatted

Commented [TJ15]: Does this conflict with D-1? Does D-1 need to say search? Check with OCA here.

Does this create a limitation on the ability to search that we aren't really under?

Commented [TJ16R15]:

~~**D - 5. Inspection and Audit Responsibilities**~~

~~Supervisors and chain of command shall be responsible for conducting inspections of work devices pursuant to D-1. Additionally, the Internal Affairs Division (IAD) Integrity Unit may conduct inspections beyond those specified in D-2 pursuant to their procedures.~~

~~The Department's Office of Internal Accountabilty~~Accountability ~~(OIAG) shall be responsible for conducting audits on adherence to this policy.~~

~~**D - 6. Audit Frequency**~~

~~The Department's Office of Inspector General~~Internal Accountability ~~(OIAG) shall conduct an audit of work cell phone and/or work electronic device use and adherence to this policy at least once every two (2) years.~~

E. TRAINING

E - 1. Academy and Initial Hire Training

Upon graduating the Basic Police Academy, the Training Division shall provide training for the new police officers on the provisions of this policy and the appropriate use of work cell phones and electronic devices.

All professional staff and sworn members who join the Department outside of the Basic Police Academy process shall review and sign off on this policy via PowerDMS within 90 days of their appointment to their position.

Commented [TJ17]: Baltimore Gun Trace TF report recommendation – train people on why this policy exists (examples and consequences)

Commented [J18R17]: Note here for training.

By order of

LeRonne L. Armstrong
Chief of Police

Date Signed: _____

Formatted: Indent: Left: 0", First line: 0", Space After: 0 pt

Formatted: Centered