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.

1. **DEPARTMENT-ISSUED CELLULAR PHONES**
   1. **Issuance and Control**
      1. 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.
      2. All professional staff at the rank of supervisor and above shall be issued a work cell phone within 90 days of appointment to the Department.
      3. 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.
      4. 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).
   2. **Carry Requirements for Sworn Members**
      1. 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.
      2. 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.
   3. **Carry Requirements for Professional Staff Members**
      1. 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.
      2. 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 available in their stead.
   4. **On-Duty Use of Work Cell Phones**
      1. 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.
      2. Members are encouraged to not conduct any personal business on their work phone. Any on-duty personal calls or messages on a work cell phone shall be kept to a minimum and brief. Examples include, but are not limited to:
         1. Calls to notify family members, physicians, etc. regarding an injury on the job;
         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.
   5. **International Use of Work Cell Phones**
      1. 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.
   6. **Evidence Procedures**
      1. 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.
   7. **Confidentiality and Reporting of Lost Phones**
      1. Department work phones and any confidential material stored therein shall be treated as sensitive material and shall be secured at all times.
      2. Lost or stolen devices shall be reported pursuant to [DGO N-05](https://public.powerdms.com/OAKLAND/tree/documents/472), with an information copy to ITU.
2. **OTHER DEPARTMENT-ISSUED ELECTRONIC DEVICES**
   1. **Issuance and Control**
      1. 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.
      2. 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.
      3. 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.
   2. **Work-related Use**
      1. Members may use electronic devices assigned to them or their unit for work-related functions.
      2. 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.
   3. **Devices with Specific Policies**
      1. 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.
   4. **Confidentiality and Reporting of Lost Devices**
      1. Work electronic devices and any confidential material stored therein shall be treated as sensitive material and shall be secured at all times.
      2. Lost or stolen devices shall be reported pursuant to [DGO N-05](https://public.powerdms.com/OAKLAND/tree/documents/472), with an information copy to ITU.
3. **PROHIBITED ACTIVITY FOR DEPARTMENT-ISSUED CELL PHONES, PERSONAL CELL PHONES, AND ELECTRONIC DEVICES**
   1. **Use of Any Device to the Point of Distraction or Interference with Duty**
      1. 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.
   2. **Use of Cell Phones While Driving**
      1. 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.
   3. **Use of Personal Cell Phones for Department Business**
      1. 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;
         2. 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. 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.
      2. Members shall not monitor or operate work-related social media accounts from personal cell phones.
   4. **Use of Work Cell Phones and Work Electronic Devices for Personal Business**
      1. 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.
      2. Without exception, no personal social media[[1]](#footnote-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).
   5. **International Data Access and Charges**
      1. 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.
   6. **Tampering with or Modifying Work Cell Phones and Work Electronic Devices**
      1. 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.
      2. This section does not limit using appropriate peripheral devices such as USB memory sticks, plug-and-play external hardware, or speakers.
   7. **Accessing Inappropriate Material on Work Cell Phones and Electronic Devices**
      1. 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 includes, but is not limited to, the following:
         1. Pornography.
         2. Any material which violates the anti-harassment or anti-discrimination policies of the Department (DGO D-20) and/or City ([Administrative Instruction 71](https://public.powerdms.com/OAKLAND/tree/documents/579540)).
         3. Hate group, racist, or anti-government material.
         4. Gambling websites or applications.
         5. Any material related to the member’s outside commercial or personal financial activity.
4. **AUDITING OF DEPARTMENT CELLULAR PHONES AND ELECTRONIC DEVICES**
   1. **Right of Department to Inspect Work Cell Phones and Electronic Devices at Any Time**
      1. The Department may inspect work cell phones and work electronic devices at any time. Such inspections shall not be arbitrary, capricious, or harassing, and shall not be based on personal bias or animus.
      2. Inspections of work cell phones or electronic devices by supervisors or commanders outside of planned/ordered audits or investigations shall be documented in a memorandum to the Captain of Internal Affairs, no matter the outcome of the inspection.
   2. **Integrity Unit Inspections of Work Cell Phones**
      1. The IAD Integrity Unit shall conduct a quarterly inspection of no less than four (4) randomly selected[[2]](#footnote-2) 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.
   3. **Department Searches of Work Cell Phones and Electronic Devices**
      1. The Department may search work cell phones and work electronic devices when there is reasonable grounds for suspecting that the search will reveal evidence of work-related misconduct or criminal misconduct.
   4. **Internal Record Keeping and Asset Management**
      1. 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)
   5. **Inspection and Audit Responsibilities**
      1. 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.
      2. The Department’s Office of Inspector General (OIG) shall be responsible for conducting audits on adherence to this policy.
   6. **Audit Frequency**
      1. The Department’s Office of Inspector General (OIG) 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.
5. **TRAINING**
   1. **Academy and Initial Hire Training**
      1. 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.
      2. 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.

By order of

LeRonne L. Armstrong

Chief of Police Date Signed: \_\_\_\_\_\_\_\_\_\_\_\_\_

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.] [↑](#footnote-ref-1)
2. 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. [↑](#footnote-ref-2)