



**City of Fort Bragg**  
**Administrative Regulation No. M-3**

**MOBILE COMPUTING DEVICES**

**I. OBJECTIVE**

Mobile computing devices, including laptop computers, smart phones, and digital tablets offer employees the benefits of enhanced productivity and convenience. At the same time, the portability of these devices increases the risk of loss and the compromise of data and information and can blur the lines between personal and business use. This document sets forth the City's policy for mitigating risk and establishing the accountability of staff for these mobile assets and specifies procedures for purchasing and use. Furthermore, this Administrative Regulation is intended to supplement other City personnel and administrative policies that govern rules of conduct and performance in the workplace, including but limited to the Use of Electronic Systems and Social Media Policy.

**II. PROCEDURES**

**1. Purchasing and Distribution – Tablets**

a) Purchases can be handled in one of two ways:

- o Option 1 – City Purchase. Under this option, the City will purchase a Wi-Fi enabled tablet, stylus, protective case/stand, and City required apps for each Councilmember and Department Manager who elects to use a tablet for City business. The tablet shall be City property. Councilmembers and Department Managers may take the device home and use it anywhere they conduct City business and such use is subject to City policies on the personal use of City equipment. Councilmembers and Department Managers are responsible for the general care of any City-issued equipment. Any tablet or accessory that is broken, damaged, or fails to work properly must be presented to the IT Department for evaluation. Councilmembers and Department Managers must return the tablet and any City-issued accessories to the Human Resources Department at the end of their service on the City Council or upon separation of service from the City. A Councilmember and Department Manager who is unable to present the device in good working condition within 24 hours shall bear the full cost of the replacement or repair of the City-owned device.
- o Option 2 – Individual Purchase with or without Financing Provided by the City. Under this option, individual Councilmembers and Department Managers may select a tablet and accessories of their choosing, subject to the specifications established by the City, either using their own funds or with financing provided by the City through the City's Equipment Purchase Loan Program. This option is designed for those who are not comfortable being personally responsible for City equipment or who would like to use the device for purposes other than City business. The City will provide assistance with setting up the tablet for City business; however other hardware and software support will not be provided and are the responsibility of the user.

**2. Purchasing and Distribution – Laptops and Projectors**

The IT Department will acquire all City-issued laptops and projectors based on established specifications for use in City business. Councilmembers and employees needing to utilize a laptop or projector for City business should contact the IT Department to check out the



**City of Fort Bragg**  
**Administrative Regulation No. M-3**

appropriate items. Items are checked out for specific tasks and must be returned at the designated date. If an item is lost, broken, damaged, or fails to work properly, the IT Department must be notified within 24 hours. If an item is stolen while away from the office, a police report should be obtained and submitted to the IT Department for follow up.

**3. Purchasing and Distribution – Cell Phones**

- a) Cell phones are available for Department Managers, Police Officers, Community Service Officers, Mid-Management and Public Works personnel for City business related use. Other employees needing cell phones for City business may be authorized by the City Manager on a case-by-case basis dependent on job duties and responsibilities.
- b) Purchases can be handled in one of two ways:
  - o Option 1 – City Purchase. Under this option, the City will purchase the cell phone and protective case for the authorized individual and select, pay for and administer the cell phone plan. The cell phone shall be City property. Users will be allowed to take the device home or use it anywhere they conduct City business; however, such use is subject to City policy on the personal use of City equipment. Users are responsible for the general care of any City-issued equipment. If the cell phone or accessory is broken, damaged, or fails to work properly it must be presented to the IT Department for evaluation. Users must return the cell phone and any City-issued accessories to the Human Resources Department while on a leave of absence that exceeds one month (unless an exception is granted by the City Manager) and upon separation of service. An employee who is unable to present the device in good working condition within 24 hours shall bear the full cost of the replacement or repair of the City-owned device.
  - o Option 2 – Individual Purchase. This option is only available for staff classified as Exempt for payroll purposes. Under this option, an authorized individual would be allowed to select a cell phone and accessories of their choosing, subject to specifications established by the City, using their own funds. This option is designed for employees who do not feel comfortable being personally responsible for City equipment or who would like to use the device for purposes other than City business. The City will provide assistance with setting up the cell phone for City email; however other hardware or software support will not be provided and are the responsibility of the user.

**4. Monthly Access, Usage and Data Charges**

- o A Employees whose job classification requires access to a cell phone and email during non-working hours, who own their own cell phone and have entered into a contract for cellular and data service: the City will provide a monthly stipend of \$40 per month. This stipend is intended to cover all cell phone services, including texting and internet connectivity. Stipends are fully taxable however other employee deductions such as retirement are not affected by the stipend. Stipends will be paid on the first pay check of each month.
- o Employees and Councilmembers who are authorized to use a Tablet device will receive a monthly stipend of \$20 to cover the cost of access required as a result of their position with the City. This stipend is intended to cover all data services. Stipends are fully taxable however other employee deductions such as retirement



**City of Fort Bragg**  
**Administrative Regulation No. M-3**

- are not affected by the stipend. Stipends will be paid on the first pay check of each month.
- Stipends will be suspended for the duration of an extended leave of one month or more unless an exception is granted by the City Manager.
  - Employees receiving a cell phone stipend are required to enter into and maintain a current contract with a cellular/data provider.
  - Employees receiving a cell phone stipend are required to sign an user agreement verifying that they have a current contract and that they understand the privacy limitations of using a City-owned or -funded mobile computing device.
  - Employees and Councilmembers receiving a tablet stipend are required to sign an user agreement verifying that they understand the privacy limitations of using a City-owned or -funded mobile computing device.
  - Stipends will cease upon separation of service from the City.

**5. Training and Support**

- a) Support services for the various devices are provided as follows:
- Email support – IT Department, during regular business hours.
  - Smart Phone and Cell Phone tied to current City vendor contracts – Assistant to the City Manager, during regular business hours.
  - Tablets – IT Department, during regular business hours. For iPads additional free support is available at the “Genius Bar” in any Apple retail store. This includes help with basic usage, general tech support, and free-to-the-public classes.
- b) Training on tablets is available from the IT Department during regular business hours, including:
- Hardware and software
  - Cloud storage and backup
  - Wireless syncing

**6. Security**

All City owned mobile computing devices, including cell phones, and employee owned mobile computing devices covered by a City-funded stipend, must be configured and secured so that the risk of inappropriate access to stored information is minimized and internal threats are mitigated. Employees and Councilmembers should have no expectation of privacy on any device used for City business. Email sent and received from a City email account is stored on the City’s Network and as such is subject to review without notice, pursuant to the City’s Information Technology Use Policy and Personnel Rules and Regulations.

**a) User Responsibilities**

- **Passwords** – Employees and Councilmembers are responsible for creating and maintaining strong passwords, safeguarding those passwords so as to prevent theft or hacking, and being able to recall or access passwords as needed to update computer software, mobile device apps, etc. in order to stay current with all security updates. Passwords shall not be shared with anyone.
- **Damage prevention** – Employees and Councilmembers are responsible for protecting their mobile devices to the fullest extent possible from breakage, damage, and theft, and promptly reporting any loss or damage to the IT Department.



**City of Fort Bragg**  
**Administrative Regulation No. M-3**

Appropriate safeguards including activating the "Find My iPhone/iPad" feature, and purchasing protective films, cases, or sleeves as needed for the employee's working conditions.

- **Syncing of devices** – Cell phones and tablets will be set up to automatically sync calendars, contacts and email. Those who use tablets will need to transfer any created or annotated documents the appropriate file storage folder on the City's file server in order for the document to be backed up.
- **Altering** – Mobile computing devices owned by the City must not be altered (Jailbreaking) in any way.
- **iTunes** – iTunes shall not be installed on any City-owned computers. Users may create and maintain their own personal iTunes account on their home computers, which requires the use of a personal credit card. City credit cards may not be used for iTunes purchases without the prior approval of the City Manager.
- **Purchases** – Employees who purchase apps or 3G wireless access for business purposes must obtain prior approval from the City Manager and, if approved, may submit a request for reimbursement to the City Manager for approval.
- **Continuing education** – Users shall stay current with policy changes, app recommendations, etc. by reading information disseminated through the City's Intranet or email.

**b) IT Department Requirements**

Configuration and encryption of mobile devices must meet standards defined by the IT Department. The IT Department will manage any security policies pushed to mobile devices, ensure that such policies are in place, and provide instructions for connecting to the Exchange Server.

- **Authentication** – Each mobile computing device must have an alphanumeric login enabled. The password must contain letters and numbers. SSL encryption must be active on each mobile computing device.
- **Loss or Theft** – In the event that a mobile computing device is lost or stolen, the owner must immediately contact the Assistant to the City Manager or the IT Department to report the incident. An inventory of programs and data should be included with this report. IT will support the user by either walking them through the operation of "wiping" the device via Outlook Web Access or doing so immediately through the Exchange Server.
- **Third Party Applications** – If a third-party program does not meet internal testing requirements for stability and/or security, it will be removed from any City-owned mobile computing device. The City does not support any third-party email applications, such as Yahoo or Gmail accounts.
- **Antivirus** – Virus scanning programs, updated regularly, may be required on all mobile computing devices.
- **Remote security management** – the following parameters must be allowed and enabled to be set on each device.
  - All parameters of the password, such as length, complexity, expiration and history
  - Ability to block certain applications
  - Internet sharing control
  - Browser access via proxy



**City of Fort Bragg**  
**Administrative Regulation No. M-3**

- Encryption must be enabled (on all phones carrying City data)

**7. Use of Cell Phones, Smart Phones and Tablets**

- a) California Vehicle Code Section 23123 prohibits all drivers from using a handheld wireless device while operating a motor vehicle unless using a "hands-free device." Vehicle Code Section 23123.5 further prohibits all drivers from using an electronic wireless communications device to write, send, or read a text-based communication.
- b) Employees making or receiving telephone calls, emails or texts while on-the-job on cell phones or tablets shall not do so while driving unless the vehicle and/or device is equipped with a hands-free device.
- c) Any employee who is charged with a traffic violation resulting from the use of their personal or City issued cell phone or tablet while driving on-the-job shall be solely responsible to the extent allowed under the law for all liabilities that result from such actions.
- d) Cell phones and tablets issued to an employee by the City are primarily for work-related communications. The employee acknowledges that he/she has no expectation of privacy in the use of or in the material content contained within such device and the employee expressly agrees that the City may at any time retrieve, audit and disclose the contents of all communications originating from or received by a City owned device including, but not limited to e-mails, voicemails, text messages and web addresses.
- e) Use of a cell phone or tablet for personal conversations is restricted to non-duty time, such as breaks, lunch, etc. Supervisors have the authority to restrict or prohibit use of devices at any time on-the-job when they believe such situations may create a distraction or safety hazard to the employee, coworkers, contractors, the general public and City or private property.

**8. Compliance with Brown Act and Public Records Act**

- a) The use of mobile computing devices, including, but not limited to, laptop computers, cell phones, smart phones, tablet computers, and similar devices, by members of the City legislative bodies subject to the Brown Act during the public meeting of the body shall be limited as prescribed in this policy and applicable law.
- b) Use of mobile computing devices by members of the City legislative bodies subject to the Brown Act during public meetings of the body shall comply with the requirements of all applicable laws and City policies, including the requirements of Article I, section 3, subdivision (b), paragraph 1 of the California Constitution, the California Public Records Act (Government Code §§ 6250-6276.48), the Ralph M. Brown Act (Government Code §§ 54950-54963), and due process rights of interested parties in City legislative body proceedings.
- c) Members of City legislative bodies subject to the Brown Act may not use mobile computing devices at public meetings of the body in any manner or for any purpose prohibited by law or City policy. In particular, but without limitation, electronic communications and data devices may not be used at public meetings by City legislative body members in any of the following ways:
  - In violation of the requirements of the Ralph M. Brown Act, such as by sharing communications among a majority of the legislative body privately and separate from the public discussion at the meeting.



**City of Fort Bragg**  
**Administrative Regulation No. M-3**

- o In violation of the requirements of the California Public Records Act, such as by transmitting to a majority of the legislative body information connected with a matter subject to consideration at the meeting, which information is not available to the public.
- o In violation of due process rights of interested parties at adjudicatory hearings, such as by consideration of information not a part of the hearing record, or by use of an electronic communications or data device so as to result in inattention to the record and/or proceedings before the body.
- d) In addition to the restrictions on the use of electronic communications and data devices by City legislative body members under the Ralph M. Brown Act, the California Public Records Act, and the due process guarantees under the U.S. and California Constitutions, members of the City legislative bodies subject to the Brown Act may not, during a meeting of the body, receive electronic communications from, or send electronic communications to, any person (including, but not limited to, members of the public, City staff, other legislative body members, and parties to City proceedings).
- e) All writings (documents, emails, etc.) produced, received, or stored on electronic communication and data devices are subject to release under the Public Records Act, including records on devices owned by the employee.

**9. Privacy**

Users of mobile computing devices for City business shall have no expectation of privacy or confidentiality with respect to their usage or in the content materials contained within those devices, regardless of ownership. As a condition for the use of City-issued device the employee agrees that the device is issued for work-related activities only and, that the City may, at any time without prior notification to the employee, review, audit, and disclose text messages, emails, and voicemails originating from or received by City owned device. As a condition of the acceptance of a City provided cell phone or tablet stipend or the use of a personal mobile computing device for City business purposes, the employee agrees that the City may, at any time without prior notification to the employee, review, audit, and disclose text messages, emails and voicemails originating from or received by a personal mobile computing device related to City business.

**III. RESPONSIBILITY**

It is the responsibility of each employee to follow the procedures outlined in this Administrative Regulation.

**IV. DEFINITIONS**

1. "Mobile computing device" means any laptop computer, cell phone, smart phone, digital tablet, or similar device.
2. "Authorized employee" means City Council Member, Department Director, and any employee authorized by the City Manager.
3. "City Computer Network" means computers and other hardware including Cell Phone and Tablets interconnected by communication channels that allow sharing of resources and information established and maintained by the City for the exclusive purpose of conducting City business.<sup>1</sup>



**City of Fort Bragg**  
**Administrative Regulation No. M-3**

4. "Jailbreaking" is the act of overcoming limitations in a computer system or device that were deliberately placed there for security, administrative, or marketing reasons; also the description and set of technical instructions necessary to achieve a specific jailbreak or a software item designed to achieve a jailbreak.

Approved by City Manager

*[Handwritten Signature]*  
(Signature)

1.23.13  
(Date)

Made a part of the City's Administrative Regulations  
binder and distributed to all City staff

8-1-13  
(Date)

