



# CALIFORNIA ENTERPRISE DEVELOPMENT AUTHORITY

a CALED sponsored organization

## POLICY AND PROCEDURE

### MOBILE ELECTRONIC DEVICE AND USE POLICY

Adopted by the CEDA Board of Directors, November 15, 2018

#### I. PURPOSE

The purpose of this policy is to establish guidelines for the authorization, and appropriate business use of Mobile Electronic Devices ("MEDs") by the California Enterprise Development Authority ("Authority") employees. MEDs include cellular telephones, personal digital assistants, smartphones, air cards, tablets, or laptops. As used herein, the term "employee" or "employees" shall include employees hired directly by the Authority as well as employees of the California Association for Local Economic Development who perform work for the Authority pursuant to a written agreement. The Authority acknowledges the necessity of these devices as an integrated technology used for data as well as voice communication and provides this policy to contain costs, ensure departmental and personal responsibility and accountability, and to prevent improper use.

#### II. SCOPE

MEDs are used for the purpose of conducting Authority business when it is necessary for an employee to be accessible via telephone and/or email.

#### III. POLICY

There are two MEDs options available to employees (see A & B below). The Chair has the authority to approve an employee's MED request while taking into consideration the option that is most appropriate given the business need.

##### A. Authority-Provided MEDs

1. Authorized employees may elect to receive an Authority provided MEDs.
2. The Authority is responsible for purchasing and maintaining Authority-provided MEDs. Employees shall coordinate with the Chair in order to receive an Authority-provided MEDs.

3. Authority provided MEDs are intended to be used solely for Authority business with de minimis personal use.
4. Records and communications related to Authority business that are stored on an Authority provided MEDs may be subject to disclosure per a California Public Records Act request.
5. Records and communications related to Authority business made, received, or retained on Authority provided MEDs are subject to the Authority's record and retention policies and procedures.

**B. Personally Owned MEDs**

1. Employees may elect to use a personally owned MED for business use, however, the Authority will not be responsible for any cost associated with purchasing and maintaining personally owned MEDs. However, the Authority may provide reimbursement for service costs when approved in advance by writing.
2. The use of an employee's personal MEDs for Authority business is voluntary and allowing access to the Authority's network from a personal MEDs is granted for the employee's convenience.
3. Employees electing to use a personally owned MED are responsible for all replacement and repair costs for their MEDs. The Authority assumes no liability for loss or damage to any personally owned MEDs.
4. Employees shall use good judgment when selecting a personally owned MED for Authority business use and when selecting a service provider, taking into consideration service area (coverage), Authority standards, policies and procedures.
5. Employees using a personally owned MED shall maintain an active and functional MED and shall report any loss of functionality of the device to their supervisor within one (1) business day. Supervisors shall report the loss of functionality to the Chair within one (1) business day.
6. Records and communications related to Authority business on an Authority approved personally owned MED or a personally owned MED used to conduct Authority business, may be subject to disclosure per a California Public Records Act request.
7. Records and communications related to Authority business made, received, or retained on a personally owned MEDs are subject to the Authority's record and retention policies and procedures.

#### **IV. PRIVACY**

When using an Authority provided MEDs, or when conducting Authority business on personally owned MEDs, the Authority cannot and does not imply, extend, or guarantee any “right to privacy” for voice calls and/or electronic communications including, but not limited to, call detail records, logs, voice mail messages, data storage, text messages, emails, address books, and the tracking of physical location.

#### **V. REVIEW OF DEVICES IN RESPONSE TO A CALIFORNIA PUBLIC RECORDS ACT REQUEST**

Upon receipt of a written California Public Records Act (“CPRA”) request, Authority management will identify employees who may have responsive documents. Those employees are required to search for documents in response to a CPRA request in good faith. The employee’s search will include Authority devices and accounts and any personal accounts and devices the employee uses to conduct Authority business. The employee alone will be responsible for searching his or her personal accounts and devices. To comply with the law and to protect the privacy of its employees, the Authority will take the following steps:

1. Identify the employee(s) who may have documents relevant to the request.
2. Communicate the scope of the request to those employees.
3. Request that the employee(s) search his or her personal files, accounts, and devices for materials responsive to the request.
4. If an employee(s) wants to withhold documents that could be potentially responsive to the request, the employee shall submit an affidavit to the Authority and a reviewing court, if applicable, that states why the documents are a personal record and not a public record.

#### **VI. RESPONSIBILITY AND ACCOUNTABILITY**

##### **A. Appropriate MEDs Use**

1. Employees using Authority provided MEDs to access email will abide by and remain apprised of changes to all Authority policies, including the Authority’s Electronic Media Policy as it pertains to Authority email access and use.
2. MEDs should not be used to store confidential and/or sensitive data. Since these devices can be lost or stolen, employees shall ensure that these devices are used in full accordance with Authority security policies.

3. In California, state law prohibits talking on a cell phone without a hands-free device while driving. In addition, state law prohibits writing, sending, or reading text-based communications on a mobile device while driving a motor vehicle. An employee who is issued a ticket or fine as a result of violating either of these laws while operating an Authority vehicle or a personal vehicle on Authority business shall be solely responsible for costs resulting from such actions.
4. Employees shall not use Authority provided or Authority approved personal MEDs in any way as to violate federal, state, or local laws including, but not limited to, the public meeting requirements of the Brown Act. Employees shall not use Authority provided or Authority approved personal MEDs in any way that would violate an Authority policy.
5. Employees shall not use Authority-provided MED's for personal business or any other purpose not related to District business.
6. Employees shall not use the Authority-provided or Authority-approved personal MED's to deliberately propagate any virus or other hostile computer program or file, to disable or overload any computer system or network, or to circumvent any system intended to protect the privacy or security of another user.

**B. Consequences of Misuse**

1. The Authority expects that its employees will use MEDs in an ethical and appropriate manner and in accordance with Authority policies. Employees shall refrain from using sexually explicit language, abusive language or profanity when using MEDs for Authority business.
2. Excessive misuse or abuse of Authority provided MEDs may result in employee reimbursement for charges, loss of the use of the device, and/or disciplinary action.
3. The Authority reserves the right to terminate an employee's MEDs privilege to use Authority provided or personally owned MEDs at any time for any reason.

**VII. SECURITY**

Regardless of the MED option that is chosen (Authority Provided MEDs or Personally Owned MEDs), all MEDs connected to the Authority network are required to have anti-virus software installed.

Applications on MEDs are required to be updated when updates become available. The MEDs' operating system and firmware are also required to be updated when the MEDs indicate that updates are available.

Employees using a personally owned MED are required to update the MDM when updates become available. If the MDM cannot be updated on the device, the employee shall contact the Chair immediately or access to Authority information and applications will be removed from the MEDs.

Upon termination of employment, or a determination by the employee or the employee's Department Head that the employee no longer has a need to access the Authority network via a personally owned MEDs, the Chair shall be notified to remove all Authority data from the employee's MED.

### **VIII. DEFINITION(S)**

Mobile Electronic Devices ("MEDs") include any communication device that provides for voice and/or data communications between two or more parties including, but not limited to, a cellular telephone, a text message device, a personal digital assistant, a smartphone, an air card, tablet, or laptop that utilizes a cellular signal to provide Internet access.

### **IX. FORM(S)**

#### **Mobile Electronic Device/Use Application**

All Authority employees are required to read and familiarize themselves with the Mobile Electronic Device and Use Policy and the Electronic Media Policy. Because changes or modifications may be made to these policies as technology evolves, it is each employee's responsibility to periodically review the policies to ensure compliance with the most current requirements.

I acknowledge receipt of this policy and understand and agree that I am bound by its contents. I further acknowledge that if an MEDs is required by my position, the Authority shall provide an Authority owned MED. If I elect to use my personally owned MED for business use, I understand that I may be authorized to receive a MED allowance to defray a portion of the cost of the MED to be used for Authority business, but I acknowledge that the Authority is not responsible for any overages resulting from the use of a personal plan for Authority business. If I am not eligible to receive a MED allowance for use of my personally owned MED, I understand that the Authority shall not be responsible for any cost associated with purchasing, using and maintaining it. Similarly, I acknowledge that the Authority assumes no liability for loss or damage to a personally owned MED:

---

Employee Signature

---

Date