



POLICY TITLE:
Electronic Device Policy Commissioners and Exempt Employees (Participants)
ADOPTED BY BOARD OF HARBOR COMMISSIONERS:
November 26, 2018
EFFECTIVE DATE:
This Administrative Policy is effective upon approval by the Board of Harbor Commissioners.
BACKGROUND/PURPOSE
This purpose of this Policy is to outline the use of District-issued electronic devices, including but not limited to cell phones, tablets and laptops, by participants, including the safe use of these devices by participants while performing their work function and while driving.
AUTHORIZATION
<p>(1) Under Harbor and Navigations Code section 6070, the Board of Harbor Commissioners is authorized to adopt all necessary ordinances for the regulation of the District, including, but not limited to, ordinances to provide for the protection and safety of persons or the property of persons using District facilities, and persons and property in and upon waters subject to the jurisdiction of the District, and adjacent property owned or controlled by the District.</p> <p>(2) Participants are permitted minimal and incidental use of District-issued electronic devices, pursuant to Government Code 8314(b)(1) and Penal Code section 424(c).</p>
PROCEDURE
The CEO & Port Director, upon the advice and consent of the General Counsel, shall approve and monitor the issuance and use of District-owned devices, including cellular phones.
GENERAL INFORMATION AND GUIDELINES
<p>1. <u>Issuance and Ownership of Cellular Devices.</u> The Oxnard Harbor District (“District”) may issue and pay for employee-enabled cellular phones, tablets, and wireless cards (hereafter “Device(s)”) consistent with this Policy.</p> <p>2. <u>Eligibility.</u> Commissioners and exempt District employees may obtain a District-owned, employee-enabled Device pursuant to the terms and conditions of this Policy by filling out and submitting a request to the District IT department. As responsibilities and functions are subject</p>

to change, the District will periodically review the eligibility of Participants using District-issued Devices.

3. Ownership. The District shall be considered the owner of all Devices paid for by the District.

4. Activation. Upon submission of a District enrollment form and being issued a Device by the District, Participants may opt to use their own personal Apple ID, and/or the District assigned Apple ID.

5. Expenses – Covered. Participants will be issued a District-owned Device on a District-provided plan (“Plan”). Monthly business-related voice and data charges will be covered by the Plan. The District’s Plan includes unlimited data and wireless, and Participants will not be charged for business-related data or wireless charges. Additionally, the Plan will cover incidental usage of the District-owned device, including personal voice and data charges provided there is no additional cost to the District. The District will not cover the cost of any expenses incurred by the Participant that are not directly related to the District’s business.

6. Expenses – Not Covered. Participants may use District devices for personal use provided there is no additional cost to the District. The Plan does not cover, and Participants will be responsible for, the following expenses incurred on a District-owned Device (“Participant Charges”):

- A. Any charges not included in the Plan (e.g., directory assistance calls, international roaming charges, Talena, games, ring tones, etc.);
- B. Additional memory, portable power supply, or upgrading to a larger device, unless the memory or upgrade is directly related to the Participant’s job duties within the District;
- C. Additional device accessories (e.g., higher quality headphone, etc.) or charges incurred for downloading games, ring tones, or any other non-District-related features.

Participants will be responsible for these charges.

7. Impermissible Uses. The following activities are absolutely prohibited on any District-owned device:

- Gambling
- Visiting and downloading material from pornographic websites
- Campaigning - political activity
- Online activities that are connected with any type of outside work or commercial activity, including any trading

8. International Travel. International Plans must be activated in advance of travel to avoid excessive roaming charges and to ensure the availability of data services. The participant must provide the IT Department with sufficient advance notice of plans to travel abroad to allow time for an International Plan to be added during your scheduled travel date(s). The participant is required to contact the IT Department in advance of traveling outside of the country with a District-issued Device so that International services can be activated.

9. Device Management Policy. The District shall use a Mobile Device Management (MDM) software system that allows the IT Department administrative control over District-issued Devices. This system allows for management of passwords, remote connection settings, increased device security, control of allowed applications, and location of lost or stolen devices. This software may not be removed or tampered with.

A. Download of applications may be restricted, or applications may be removed, if those applications are considered inappropriate, unrelated to District business, or they are considered a threat or significant risk to the District's network environment.

B. From time to time, Participants may be asked to present their device to the IT Department for a software update or receive instructions on how to download and update themselves. Participants must promptly comply with these requests.

C. Devices are used as convenience and productivity enhancing tools. Due to their somewhat volatile nature, the data on these devices is considered as transient, convenience copies. However, if there is a record on the District-owned device that needs to be retained, Participants are required to retain the record on a District-file system pursuant to the District's Records Management Policy.

10. Security Requirements. All Participants using District-issued devices must comply with the following security procedures:

A. Devices must be password protected;

B. Devices must lock after five incorrect password attempts; and

C. Devices must "time out" and require a password after a fifteen-minute period of inactivity.

11. Professional and Conscientious Use. All Participants are required to be professional and conscientious always when using District-owned phones.

12. Confidential Discussions. Participants should not use cell phones to discuss confidential or sensitive information, as cell phone conversations are not secure.



13. Loss or Theft. In the event of a loss or theft of a District-issued device(s), Participants must immediately notify the District IT Department. The District retains the right to correct any such incident in order to protect the integrity of District's systems and data. The District reserves the right to perform a remote reset/wipe of any District-owned device at any time.

14. No Expectation of Privacy. Participants shall retain no expectation of privacy in any discussion or text message sent or received on a District-owned Device(s).

15. Driving. The District requires strict adherence to state laws concerning the use of cellular phones while driving. For the safety of the District's employees, it is required that Participants use hands-free devices while driving and using a District-owned Device. Employees are expressly prohibited from checking, sending or receiving emails or text messages while driving. These requirements apply at all times when driving a District issued vehicle and at any time when driving on District business, even if the representative or employee uses his or her own vehicle. Failure to adhere to this Policy is grounds for discipline, up to and including termination.

16. Accounting Control. Copies of all reviewed Device bills shall be maintained by the District's Finance Department. Additional audits of these bills shall be carried out on a periodic basis by Finance Department staff to ensure adherence to this Policy.

17. Insurance. All District-owned Devices shall have insurance at all times in case of loss or damage.

18. Discontinued Use. Upon separation of employment or upon a Participant no longer qualifying to receive a District-owned device(s), the device(s) is/are to be returned to the District. With approval of CEO & Port Director, participants can purchase discontinued devices(s) at current documented market value.

19. Penalties. Any District Employees who violates this Policy may be disciplined, up to and including termination as appropriate, in accordance with this Policy. Further, any such violation of this Policy may be punishable by an individual's loss of the right to use any District-owned Device as described herein. In addition, violations of this Policy may be referred for criminal prosecution, if appropriate.

RELATED POLICIES AND PROCEDURES:

District Policy #208.1- District Driving Policy