

POLICY TITLE: Cell Phone and Wireless Communication Device Policy
POLICY NUMBER: 3305

3305.1 Purpose:

The use of cell phones and wireless communication device technology is an integral part of our daily business and personal activity. Cell phones, PDA's, pagers, texting, etc., provide instant communication and information where one may transact business almost anywhere in the world. These devices are tools to enhance employee productivity, provide safety/security while traveling, and provide a higher level of service to the citizens of our community. This policy is provided as an effort to maximize efficiency, enhance safety, and ensure communication devices are used properly.

3305.2 Policy:

In recognition of communications technology, it is the District's goal to enhance the efficiency and effectiveness of communication, ensure safe work practices when using cell phones while driving or performing work-related activities, to comply with State law which prohibits drivers from using a cell phone unless they are also using a hands-free device, to provide standards and clarification for cell phone or other wireless communication device use, and to provide for the conditions of use of District issued devices. Texting (writing, reading, or sending) while operating a motor vehicle is prohibited.

3305.3 Scope:

The procedures provided for in this Policy apply to all employees, officials, or volunteers using cell phones or other communication device(s) for conducting District business.

3305.4 Definitions:

- A. District Related Business: Activities that directly or indirectly support the business of the District.

3305.5 Procedures:

- A. Cell phones and other communication devices may be issued to employees to enhance the efficiency and effectiveness of communications in conducting District Related Business. In addition, personal cell phones and other devices may be authorized for use by employees to enhance the efficiency and effectiveness of communications in conducting District Related Business.
- B. Employees must agree to the terms and conditions set forth in this policy to be issued a District device or able to use their own device for District Related Business.
- C. Use of District issued devices is contingent upon continued District employment and the device shall remain the sole property of District.
- D. Employees shall report and submit damaged or defective equipment to their immediate supervisor who will report it to their Department Head or the General Manager.
- E. Cell phones or other devices assigned to management or personnel that are on-call or expected to be available beyond normal work hours are to carry and be accessible by the device for District Related Business.
- F. The District will not actively intercept electronic communications, without legal authority.
- G. The District maintains the right to limit or deny the use or possession of personal cell phones during work periods when said possession is determined to be a distraction, infringes on established employee safety standards, or becomes a detriment to employee productivity.

3305.6 Use of Devices:

- A. Use of a District provided cell phone for commercial profit or secondary employment is prohibited.
- B. Phones should be set to "silent" or "vibrate" if not turned off to avoid distraction to other employees or the public in appropriate places. This provision also applies to personal (non-District issued) cell phones carried by employees.
- C. Regardless of phone ownership, employees with cell phones equipped with cameras are prohibited from using the camera in a manner that violates the privacy of co-workers or the public.
- D. Employees shall limit making personal calls on their cell phone, personally owned or District provided, during work hours. Personal calls are to be kept to a minimum on District provided cell phones; any use must be de minimis in nature (i.e., that the use is so small that the accounting for it is unreasonable or administratively impracticable).
- E. Cell phones or other wireless devices provided by the District are only for non-compensatory purposes.
- F. Employees are prohibited from accessing certain websites during work hours/while connected to the District's network at the discretion of the supervisor or General Manager.
- G. Devices may not be used at any time to:
 - Store or transmit illicit materials
 - Store or transmit proprietary information belonging to another company
 - Harass others
 - Engage in outside business activities

3305.7 Use of Cell Phone While Operating a Vehicle:

Regardless of the ownership of a cell phone or other electronic device, State law prohibits the use of cell phones while operating a vehicle unless the telephone is specifically designed and configured to allow hands-free listening and talking, and is used in that manner while driving. Also, it is illegal to "write, send, or read a text-based communication" while operating a motor vehicle. (California Vehicle Code Section 23123 and 23123.5).

- A. There are two exceptions to the law regarding the use of cell phones while operating a vehicle:
 - i. Emergency services personnel are exempt from this law when operating an authorized emergency vehicle;
 - ii. The law does not apply to persons using their cell phone to contact law enforcement or public safety agencies for emergencies.
- B. Cell phone use (including texting): Except for A above, employees shall not operate cell phones and other wireless devices that may distract from safely operating a motor vehicle. Using cell phones or other devices while driving leads to increased risk of accident and liability to the District.
- C. Employees who are charged with traffic violations resulting from using mobile devices while driving are solely responsible for all liabilities that result.
- D. To limit risk to the District and employees, the following guidelines are provided for employees to use while on District Related Business:
 - i. Use a hands-free device if you must make or receive a call while driving.
 - ii. Making and completing calls before proceeding to your destination is preferred.
 - iii. Safely pull over or park before initiating a call when practical.
 - iv. Allow voice mail to handle your incoming calls and return them at your convenience in a safe place.
 - v. Suspend conversations during hazardous driving conditions or situations.
 - vi. Taking notes or looking up phone numbers while driving should not be done.

3305.8 Support for District Issued Devices:

- A. District issued devices must receive all available security updates and have security updates enabled.
- B. Connectivity issues are supported by IT; employees should not (unless instructed by IT) contact the device manufacturer or their carrier for operating system or hardware-related issues.
- C. IT will make provisions and configure standard apps, such as browsers, office productivity software and security tools, before allocating them to the user.
- D. Mobile Device Management (MDM) software will be installed on the District issued device. This software will monitor emails, text messages, and photos, along with the location of the device.
- E. Two factor authentication shall always be used when available.
- F. Family and friends of employees are prohibited from using the allocated District issued devices.
- G. The district will load anti-virus software onto the devices.

3305.9 Security:

- A. To prevent unauthorized access, District issued devices must be password protected using the features of the device and a strong password is required to access the company network.
- B. District issued devices must be set up to automatically lock the screen and must have a password or other screen lock protection (password, fingerprint, facial recognition or pattern, or at least 6 digit PIN).
- C. After five failed login attempts, the device will lock.
- D. Device must be running an unmodified firmware/operating system from the device manufacturer or cellular carrier that has not been "jail broken"/no root access.
- E. Employees are automatically prevented from downloading, installing, and using any app that does not appear on the District's list of approved apps.
- F. Cellphones and tablets belonging to employees that are for personal use only are not allowed to connect to the District's network.
- G. Employees' access to District data is limited based on user profiles defined by IT and automatically enforced.
- H. The District issued device may be remotely wiped if 1) the device is lost, 2) the employee terminates his or her employment, 3) IT detects a data or policy breach, or a virus or similar threat to the security of the District's data and technology infrastructure.

3305.10 Privacy:

- A. No employee should expect privacy except that which is governed by law. District has the right, at any time, to monitor any communications that utilize District's networks in any way. This includes, but is not limited to, data, voicemail, telephone logs, Internet use, network traffic, etc. Management reserves the right to review, retain, or release personal and/ or company-related data on mobile devices to government agencies or third parties during an investigation or litigation. No employee shall knowingly disable any network software or system identified as a monitoring tool.
- B. At any time, the employee may be asked to produce the District issued device for inspection. The purpose of these inspections is to ensure that the employee is following company policy.

3305.11 Responsibility:

- A. Supervisors are responsible for determining an employee's need for a District provided cell phone or other communication device. In doing so, the supervisor will analyze the business necessity for such use before distribution. Supervisors shall inform employees of the purpose of cell phone

communication while performing District Related Business, ensure the employee understands this policy, and enforce compliance with this policy.

- B. Each supervisor shall manage the administration of the contract for cell phone service for each District provided cell phone assigned in their department, including maintaining an inventory of cellular equipment and number of users. Cell phone contracts may be centralized for cost savings and the assigned Department will have review authority.
- C. Employees shall review and adhere to this policy. Using a District cell phone or other wireless communication device is a privilege and not a right. The General Manager may revoke the use of a District cell phone or other device at any time with or without cause.
- D. Data, including any retained voice message, text, e-mail, etc., on the communications device is not to be considered private and may be reviewed at any time by the District with or without notice to the employee

3305.12 Responsibility for Review:

The policy will be reviewed at least once every 3 years by the General Manager and Board of Directors.