

Article 3      Miscellaneous

- Sec. 3.1      Credit Union Membership. All District employees are eligible to join the San Diego County Credit Union (SDCCU) with payroll deductions provided at no cost to the employee. This benefit is optional and may be entered into at any time by the employee. Membership forms are available through the Finance Department.
- Sec. 3.2      Deferred Compensation. All District employees have the option to participate in a deferred compensation program whereby a portion of the employee's salary is set aside tax free to accumulate toward future retirement.
- Sec. 3.3      Payroll Deductions and Employee Association Dues. Employee Association dues, and payroll deductions, such as credit union, United Way and dependent life insurance deductions, as may be properly requested and lawfully permitted, shall be deducted by the District from the salary of each employee who files with the District a voluntary written authorization requesting that such deduction be made. Remittance of the aggregate amount of all dues and other proper deductions made from the salaries of employees shall be made by the District directly to the designated organization.
- Sec. 3.4      Separability and Savings. If any portion of this employee's manual, or the application of such portion to any person or circumstance, shall be invalidated by judicial or legislative action, the remainder of this manual, or the application of such portion to persons or circumstances other than those as to which it is invalidated shall not be affected thereby, and shall remain in full force and effect.
- Sec. 3.5      Telephone Use. District telephones may be used for employees' personal calls on a de minimis basis only. If it should become necessary for an employee to receive or place a personal call, the conversation should be kept as brief as possible. The employees do not have a right, nor should they have an expectation, of privacy while using District telephones for personal calls or receiving voice mail of a personal nature.
- Sec. 3.6      Personal Equipment Purchase and Education Program. All District full or part-time regular employees, who have completed their probationary period, are eligible to participate in the Personal Equipment Purchase and Education Program whereby loans are made by the District to employees to purchase career related equipment or provide funding for career related educational purposes and are repaid through payroll deductions. Employees participating in the Program must make their own arrangements with schools (see Administrative Code Section 7.3(h), or vendors. The District will not recommend a vendor or otherwise be involved in an equipment purchase. A detailed description of the Program is available from Human Resources.

Sec. 3.7 Acceptable Use of District Computer Systems and Data The sole purpose of the District computer systems and connections to the Internet, external e-mail via the Internet, and internal e-mail is the timely and efficient processing and communication of information directly related to District business interests. In addition, internal electronic mail (e-mail) provides a vehicle for work related communication between employees via their computer workstations and mobile devices.

"District computers" are defined as including, but not limited to, the District mainframe, network server, all computer workstations and mobile devices, peripheral equipment and connections to the Internet throughout the District facilities. "Electronic mail" (e-mail) is defined as a method of electronic communications between employees or with outside sources which exist as an aide in conducting the day to day business functions of the District. E-mail communication is to be considered confidential but it is not private. The District's communications media policy is further outlined as follows:

- (a) All District computer systems, including all information contained therein, electronic mail and Internet access, are the sole property of the District and may be used only for business purposes. Subject to approval of the department head, District computers may be used for de minimis personal use, but any such use is subject to this section.
- (b) District computer systems may not be improperly used. Improper use may include but is not limited to connecting to the Internet and downloading information unrelated to District business such as creating, accessing, printing or distributing documents or messages to others that may adversely affect employee morale, or are derogatory, defamatory, harassing, obscene, or otherwise inappropriate or unrelated to conducting District business functions. Files or messages on another employee's system shall not be accessed for any purpose without authorization from a Department Head. The improper use of the District computer systems is considered an extremely serious offense, violation of District policy and is subject to discipline up to and including termination.
- (c) The District reserves the right to monitor the computer systems for any reason, including but not limited to the right to review, audit and disclose all matters sent over and/or stored in electronic mail or any computer software or system without the employee's knowledge or consent.
- (d) Under some circumstances, communications sent by e-mail may be subject to disclosure under the Public Records Act or during litigation. Be advised that if the system is improperly used to create an inappropriate file and the file is later deleted that it may not be fully eliminated from the system and could be re-captured. Employees are duly warned not to compromise themselves or any computer software or system(s) on District property.

Sec. 3.8

Mobile Devices. Mobile Devices (MDs) include cellular telephones, personal digital assistants, smartphones, air cards, laptop computers, tablets, and other devices having integrated technology used for data and/or voice communications. MDs provided by the District are to be used for the purpose of conducting District business when it is necessary for an employee to be accessible via telephone and/or e-mail, and to access District data remotely while away from the office with de minimis personal use.

- (a) Department Heads have the authority to approve an employee MD request as appropriate given the business need. The Information Technology (IT) Department is responsible for purchasing and maintaining District provided mobile devices.
- (b) Employees using District provided MDs to access e-mail and the Internet will abide by the acceptable use provision in Section 3.9(b) regardless of the location where the MD is being used.
- (c) MDs 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 District security policies.
- (d) Employees are expected to protect their District-issued mobile devices from theft, damage, abuse, and unauthorized use. Employee will protect the device with a password and keep this password confidential. The device will not be shared with other individuals or family members. If the device is lost or stolen, the user will notify the District's IT Department within one hour, or as soon as possible after noticing that the device is missing. The IT Department will attempt to lock and disable the device upon notification.
- (e) Employees shall not attempt to download and/or install any software or apps on a District provided mobile device without prior approval by the Information Technology Department.
- (f) Personally owned mobile devices should not be used to conduct District business except on a very limited basis when the District provided mobile device is not functioning or is not available. Employees shall not download/transfer or store sensitive District business data/documents to any personal or non-District owned device at any time.

Article 3      Miscellaneous (Cont'd.)

Sec. 3.8      Mobile Devices (Cont'd)

- (g) When using any mobile device, including any personally owned device, to conduct District business, the District 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 message, e-mails, and address books. To the extent that employees wish that their private activities remain private, they should avoid using District provided mobile devices for limited personal use. By acceptance of the District provided device, employees imply their consent to disclosing and/or monitoring of device usage, including the contents of any files or information maintained or passed through that device.
- (h) Employees are expected to maintain device usage within the mobile device plan parameters. Due to voice and data plan usage limits on the mobile device, employees should opt to use the wired phone at their desk to make and receive calls, and use their office workstation to access the Internet.
- (i) California state law prohibits talking on a mobile 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 a District vehicle or a personal vehicle while on District business shall be solely responsible for costs resulting from such actions. Employees will abide by and stay apprised of all state and federal laws relating to the use of mobile devices.
- (j) Personal mobile devices, including MDs owned by a third party visiting or doing business at the District, are not allowed to connect to any District-managed computer systems, communication networks, or wireless access points without prior authorization by the IT Department. Upon request only, visitors to the District may use wireless access points specifically set up for guests that provide access to the Internet, but not to any internal District network.

Sec. 3.9      Use of Virtual Private Network (VPN). Remote access to District’s network via VPN is approved by Information Technology Department based on District’s business need. Users may only use District approved devices and configured VPN client software to access District VPN.

Per Ordinance No. 2014-05 Adopted 8/4/14 [Sec. 3.8]

Per Ordinance No. 2014-05 Adopted 8/4/14 [Sec. 3.9]