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.

Per Ordinance No. 99-4 Adopted 6/21/99 [Sec. 3.1]
Per Ordinance No. 2011-07 Adopted 6/6/11 [Sec. 3.2]
Per Ordinance No. 2014-05 Adopted 8/4/14 [Sec. 3.5]

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.

Per Ordinance No. 2014-05 Adopted 8/4/14 [Sec. 3.7]

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.

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

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.

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

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. Use of VPN is subject to the following requirements and standards:

(a) Remote access to District's network via VPN must be approved by Information Technology (IT) Department based on District's business needs. Access is provided and maintained for authorized users only.

(b) Approved employees may only use District approved devices and properly configured VPN client software to access District VPN. Employees using VPN shall abide by the Acceptable Use of District Computer Systems and Data policy.

(c) Authorized third parties may only use VPN for the purpose and duration of their contract with the District. Each third-party user must use their own individual login credential, and access shall be strictly limited to resources they need to access for the contracted task. VPN access privilege shall be immediately revoked at the cessation of the business need or at the end of the contract, whichever comes first.

(d) VPN shall not be used to conduct personal business unrelated to District business.

(e) Users of non-District owned equipment must configure and maintain the equipment with of up-to-date and fully functioning endpoint security software, up-to-date version of the operating system, and use a device password, pin code, lock screen, biometric authentication, or other strong authentication method to secure the equipment.

(f) Any user (authorized employees and authorized third parties) connecting to VPN must be individually authenticated via at least two separate authentication methods. Examples of this include a strong password combined with a code or prompt on the user's mobile phone, a hardware token in user's possession, or the user's biometric signature. Password sharing or circumventing the multi-factor authentication by authenticating another user on their behalf is strictly prohibited.

(g) It is the responsibility of any user with VPN privileges to ensure that unauthorized users are not allowed access to District's internal networks. If the device that is connected to VPN is left unattended, access to the device must be locked, or it must be disconnected from VPN.

(h) If the device used to connect to VPN has been tampered with, breached, infiltrated, or compromised by an unauthorized party, or if the user's credentials may have been exposed, the user must discontinue its use immediately and contact the IT Department as soon as possible.

(i) If an active VPN connection is no longer needed, the user shall sign out from all District network resources and disconnect from VPN.

Per Ordinance No. 2026-10 Adopted 7/21/26 [Sec. 3.9 (a-i)]
Per Ordinance No. 2014-05 Adopted 8/4/14 [Sec. 3.9]

Sec. 3.10 Use of Artificial Intelligence (AI). This policy outlines the acceptable use of AI systems and generated content in the District.

I. Definitions

1) AI is a field of computer science dedicated to creating systems capable of performing tasks that typically require human intelligence, such as reasoning, learning, problem-solving, perception, and understanding language. Instead of relying on explicit programming for every action, traditional AI systems rely on algorithms and large datasets to detect patterns, generate predictions, and gradually improve their performance.

2) Generative AI produces entirely new content—such as text, images, music, videos, or software code—based on a user's prompt or request.

II. Purpose and Scope

The District supports the appropriate, beneficial, and safe use of AI. This policy establishes standards and guidance for all employees to help ensure that the District's core principles are protected. While AI can enhance productivity and improve the level of service provided to our customers, it is important to recognize that AI lacks human intuition and judgment and may produce errors. AI should be viewed as a tool to assist employees, with the responsibility for final decisions remaining with the user.

Any AI use by the District shall conform to the following five key principles (from Department of Homeland Security Directive 139-08):

1) Lawful and Mission-Appropriate: Any AI use must comply with the Constitution, laws, and District policies, protecting privacy, civil rights, and civil liberties.

2) Mission-Enhancing: AI use must be purposeful to improve the District's operational, administrative, and support functions.

3) Safe, Secure, and Responsible: AI use must address risks and benefits, protect privacy and civil rights, and be tested rigorously to avoid biases and ensure effectiveness, accuracy, and security.

4) Trustworthy: AI use must be transparent and explainable, with public disclosures and traceable, auditable outputs.

5) Human-Centered: AI design and deployment must consider the impact on users and those affected, incorporating feedback from communities and stakeholders.

Therefore, all District employees, partners, contractors, and volunteers who operate on behalf of the District and use District-provided AI solutions, as defined below, shall:

(a) Review and adhere to the District's AI policy.

(b) Collaborate closely with the District's IT Department to carefully assess AI applications, programs, and tools to ensure they meet safety and security standards before being purchased and implemented. Prior to procuring or using an AI tool, fully understand its capabilities, limitations, and potential impact. Dedicate time to training in order to understand the AI tool's functionalities and best practices for its use.

(c) Review and verify all content produced by AI tools before using it in any work. The employee—not the AI—is always fully responsible for the final output. Do not rely solely on AI tools for decision making. Use them to complement, not replace, human judgment. Never rely on AI to create District official documents or review legal or regulatory issues without expert human review.

(d) Seek independent sources to verify the information provided by an AI tool and take reasonable steps to ensure that the facts and sources it provides are accurate and trustworthy. Examine prompts and outputs for signs of bias and discrimination, and take appropriate steps to mitigate their inclusion when feasible. Verify facts, figures, and sources provided by an AI system independently. Never assume they are accurate.

(e) Evaluate high-risk uses carefully before implementation. This includes, but is not limited to, using AI solutions to (1) automatically make health, financial, or life opportunity decisions; (2) manage essential services or critical infrastructure for the District without human oversight; (3) perform real-time and covert biometric identification or process the data collected from such systems, excluding identification as required for law enforcement purposes under expressed authority by applicable law; (4) manage employment and worker systems (HR systems), such as tools used for recruitment, applicant screening, or systems used for employee work management, performance, or behavior that could result in discipline or termination; and (5) systems that are known to cause significant or irreversible environmental damage.

(f) Never use insecure or publicly accessible AI tools to process or discuss sensitive, confidential, or private information. This includes protected health information (PHI) and personally identifiable information (PII) as defined by the Health Insurance Portability and Accountability Act (HIPAA), law enforcement sensitive information, and proprietary District data. Do not use District data to train public AI solutions that are not governed by the District's standard contractual terms, as this could increase security and legal risks and potentially lead to a data breach. Ensure that all interactions adhere to legal and organizational data privacy and confidentiality standards.

(g) Never use digitally generated or altered images of any individual without their consent, or of any subject with the intent of causing harm to District employees or members of the public. Never use District-provided AI solutions to generate or process socially inappropriate or harmful content regardless of its intended purpose.

(h) Do not use District-provided AI solutions for self-gain, personal business, or private use.

(i) Credit all images and videos produced by Generative AI solutions to the respective AI tool. Whenever possible, attributions and citations to the District should be embedded directly in the image or video (e.g., through a digital watermark). If AI-generated text is significantly used in a final product, proper attribution to the relevant AI solution is required.

(j) Report to their supervisor and the IT Department if staff becomes aware of an instance where an AI solution has caused harm either through direct action or due to the system being compromised.

(k) Follow the laws and current procedures and District policies for records retention and disclosure, including records produced by an AI solution. This includes records of inputs, prompts, and outputs in a manner consistent with the District's records management and public disclosure policies and practices.

Per Ordinance No. 2026-10 Adopted 7/21/26 [Sec. 3.10 Section Added]