

BOARD POLICY

*Category: Board and General
Administrative Matters*

Electronic Communications and Computer Systems Policy

Purpose

This policy governs the use of the District's electronic communications systems: the electronic mail system (e-mail), Internet access using District owned computers, phones, including cellular phones, two-way radios, the voicemail system and facsimile machines (electronic communications systems). This policy applies to all District employees, temporary hires and/or consultants¹ (hereinafter "Users") using District equipment or accessing the District's electronic communications systems. This policy also applies to all use of equipment owned by the District whether it is located on District property, at the employee's home or in a remote location.

System Use:

Use of the District's Electronic Communications Systems and computers should be limited to District business consistent with Board Policy 168. The systems provided are not to be used in a manner that is disruptive, interferes with work or is harmful or offensive to others. All use must comply with District Policy No. 204 — Prohibiting All Forms of Unlawful Employment Discrimination, Including Sexual or Other Forms of Harassment.

Prohibited Use:

Use of Electronic Communications Systems to send messages of a threatening, harassing, obscene or profane nature is prohibited. Inappropriate use may include but is not limited to the display or transmission of sexually explicit images, messages or cartoons, or any transmission that contains ethnic slurs, racial epithets or anything that constitutes harassment or disparagement of others based on their race, national origin, color, sex, sexual orientation, age, disability, religious or political beliefs.

¹A consultant includes all outside business entities of whatever form, including independent contractors.

Adopted: 2/9/00

Users of the Electronic Communications Systems are subject to the Non-Solicitation Policy. The use of the District's Electronic Communications Systems to solicit others is strictly prohibited. Inappropriate solicitations include, but are not limited to: political, social, commercial ventures, union or religious messages or solicitations for charitable organizations.

To the extent that the electronic communications systems are used as a substitute for posted flyers (e-flyers), the General Manager's Office must approve the posting.

"Chain-mail" or "Chain messages" using the District's Electronic Communications Systems are expressly prohibited.

Privacy Interests

All data on local hard drives or the network are the property of the District. All files are subject to retrieval and review by the District at anytime, with or without consent of the user. Authorized District personnel, as designated by the General Manager, shall have unrestricted access to information stored on the District computers. This may include retrieving business information, troubleshooting hardware and software problems, preventing system misuse, including monitoring use of e-mail and the Internet and websites accessed, assuring compliance with software distribution policies and complying with legal and regulatory requests for information.

Under no circumstances can District files, or portions of files be encrypted or password protected in a way that prevents access by authorized District personnel when the user is away. This includes a ban on BIOS level passwords and all file encryption.

In order to protect the District's privacy interests in its official business messages and to maintain the integrity of its Electronic Communications Systems, the District provides Users with private password protection. The use of a password does not give the User an expectation of privacy, as the District reserves the right to access and disclose all information and messages sent over its e-mail and voicemail systems for any purpose with or without the consent of the User.

Users may not download executable files (a file that is actually a software program) from the Internet or other sources using modems or the T1 line linked to District computers.

Remote Access

Users are prohibited from attempting to access the District provided Internet service from remote locations unless authorized by the General Manager.

Security

It is the responsibility of each User to maintain the security of District Information. Computer setups (including hardware and software configuration and make-up) are the sole responsibility

Adopted: 2/9/00

of the Information Services Department. This includes, but is not limited to, operating systems, PC applications, drivers, network access, Internet access and hardware. Users, other than District authorized Information Services Department employees, may not install or uninstall any hardware or software on District computers.

The system administrator is responsible for loading all application software, operating system software and hardware (both internal and external to the machine) in a manner that is consistent with District and user department policies.

Software Piracy, Intellectual Property, Copyrights

Users must respect the property and licensing of software programs and websites.

Electronic Tampering

Unauthorized users may not attempt to gain access to another employee's computer files (including Internet and e-mail files) without the latter's express permission. However, the General Manager or his/her designee may authorize access to any District file with or without the user's permission.

Electronic snooping or tampering by any User is a violation of this policy. "Electronic snooping" is the unauthorized entry or attempted entry into files stored on another User's computer or the server, either directly or from a remote location.

Retention:

Employees should be aware that even though computer files or electronic mail may be deleted from the system, a record may remain on the computer or transmission system. All files, e-mail and voicemail may be subject to disclosure if requested through a civil or criminal subpoena or under the California Public Records Act.

Revisions

It is recognized that the area of electronic communication (e-mail, voicemail and Internet access and use) is a rapidly changing area. Therefore, the AC Transit Board of Directors authorizes the General Manager to implement this policy with appropriate Administrative Procedures as needed.

Users failing to adhere to this policy may be subject to discipline, up to and including discharge.

Adopted: 2/9/00