

<h1 style="text-align: center;">POLICY MANUAL</h1>	Date Adopted:        May 23, 2001
Classification: GENERAL ADMINISTRATION	Date Last Amended:
Subject:            Electronics Communications Policy	Approved By:

**I.    Purpose and Procedure:**

The purpose of this policy shall define appropriate employee use of the Fresno Metropolitan Flood Control District owned, operated and maintained technology resources (including, but not limited to, hardware, software, e-mail, Internet/on-line access and telephone voice mail).

The District's technology resources are made available to District staff to assist them as tools to perform work assignment. Technology resources include the telephone, voicemail, any hardware, software, e-mail and Internet connection tools it deems necessary in fulfilling the duties required to provide service to the District's constituents.

Users are expected to cooperate with each other to promote the most effective use of computing resources, and to respect each other's work even though it is in electronic rather than printed form. Individuals will be held accountable for their actions involving the use of technology resources. Failure to comply with this policy and the following guidelines for acceptable use of technology resources may result in loss of

<h1 style="text-align: center;">POLICY MANUAL</h1>	Date Adopted:        May 23, 2001
Classification: GENERAL ADMINISTRATION	Date Last Amended:
Subject:            Electronics Communications Policy	Approved By:

specific or all technology based access privileges and disciplinary action, up to and including termination.

**II. Confidentiality:**

The District seeks to protect the confidentiality of District records stored on its computer systems. Rules prohibiting theft or vandalism apply to software and data as well as to physical equipment. All software, data, reports, messages and information stored on local and network hard drives, as well as other products created using the District technology resources are the property of the District and access to them must be authorized. The District reserves the right to set up protocol and access rights as it deems necessary to all technology resources.

**III. Internet Content:**

Due to the nature of the Internet, at this time there is not a way to completely safeguard Internet content activity. The District reserves the right to use available technology to screen out information that may be offensive; since new sites are added daily, this technology cannot block all sites that may contain offensive

<h1 style="text-align: center;">POLICY MANUAL</h1>	Date Adopted:        May 23, 2001
Classification: GENERAL ADMINISTRATION	Date Last Amended:
Subject:            Electronics Communications Policy	Approved By:

material, nor can the District prevent transmission and/or receipt of offensive e-mail messages. The District reserves the right to monitor the Internet sites visited by employees and to track the content, destination and point of origin of e-mail messages. Employees using on-line services and/or Internet access must understand that they may receive unsolicited e-mail or information that may be considered offensive.

**IV. Technology Users:**

All employees of the Fresno Metropolitan Flood Control District who use District technology resources shall be defined as "Technology Users." The Technology Users Agreement shall be signed prior to the employee utilizing District technology resources. Current users of technology resources will be required to sign this agreement within 10 days following adoption of this policy or risk the loss of access privileges.

<h1 style="text-align: center;">POLICY MANUAL</h1>	Date Adopted:        May 23, 2001
Classification: GENERAL ADMINISTRATION	Date Last Amended:
Subject:            Electronics Communications Policy	Approved By:

V.    **Security:**

The District's technology systems require that each user have a unique identity, referred to as a "User-ID", protected by a "password" to gain access to the system. The User-ID represents a user in various system activities, provides access to certain software and data based on his/her department-established authorization, and associates his/her own software and data with his/her identity. As such, this User-ID is another instrument of identity and its misuse constitutes forgery or misrepresentation.

An employees' password and User-ID are unique, identifying him/her as the user accessing a particular workstation or PC. The employee is responsible for any modifications or access to system information made using his/her User-ID. Every change to technology information is logged with the identification of the person who signed on. Therefore, it is imperative that users do not share passwords, and that no PC, terminal, or workstation is left unattended while logged on (i.e.; users should either log off or lock their workstation through their screen saver or other method). Users should be aware that merely turning a PC off does not always log off the user

<h1 style="text-align: center;">POLICY MANUAL</h1>	Date Adopted:        May 23, 2001
Classification:    GENERAL ADMINISTRATION	Date Last Amended:
Subject:            Electronics Communications Policy	Approved By:

from the system. Users needing assistance with logging off procedures or locking their workstation should contact Information Systems Department.

Each employee may perform specific functions, as authorized by his/her Department Head, which are identified through use of the User-ID. Employees may have access to large volumes of information, much of which may be confidential to the Department or the District. It is important that the employee be knowledgeable of, and understands what information may be shared with others in the work unit, in the department, with personnel in other departments, and with the general public. Employees who are uncertain as to the confidentiality of data should request clarification from their supervisor immediately.

**VI. The Use of E-Mail Services (e.g.; Exchange or Internet Mail) provided by the Fresno Metropolitan Flood Control District:**

All electronic mail messages are considered District records. The District reserves the right to access and use for business purposes the contents of all messages sent over its electronic mail systems, including electronic mail sent over the Internet.

<h1 style="text-align: center;">POLICY MANUAL</h1>	Date Adopted:        May 23, 2001
Classification: GENERAL ADMINISTRATION	Date Last Amended:
Subject:            Electronics Communications Policy	Approved By:

Employees should not expect or assume any privacy regarding the content of electronic mail communications. Users of District provided e-mail systems shall use these systems in a professional manner.

In order to use system resources efficiently, general interest work-related announcements should be posted to the "District Information" bulletin board (when created), not sent to individual mailing lists. Personal use of electronic mail is not permitted.

All District employees are instructed to not delete any electronic e-mails pertaining to District business. All District messages will be backed-up on a daily basis and archived monthly.

**VII. Technology Users Agreement for the Fresno Metropolitan Flood Control**

**District Electronic Communications:**

USERS OF TECHNOLOGY SERVICES PROVIDED BY THE DISTRICT SHALL

ABIDE BY THE FOLLOWING:

<h1 style="text-align: center;">POLICY MANUAL</h1>	Date Adopted:        May 23, 2001
Classification: GENERAL ADMINISTRATION	Date Last Amended:
Subject:            Electronics Communications Policy	Approved By:

- A.    Make a reasonable effort to inform themselves of these access guidelines and acceptable and unacceptable uses of District internal technology systems, the Internet, and other on-line services in general. The burden of responsibility is on the user to inquire as to acceptable and unacceptable uses prior to accessing the system. Compliance with applicable use restrictions is mandatory.
  
- B.    Use District provided technology, Internet and other on-line servers for the District related activities only.
  
- C.    Respect the rights of others. Conduct, which involves the use of District computing resources to violate another users rights, includes:
  - 1.    Copying, or altering another users software or data, which has been obtained by unauthorized or illegal means.
  - 2.    Abusing or harassing another user through electronic means.
  
- D.    Respect the legal protection provided to programs and data by copyrights and licenses. Users may not copy District owned or licensed software data to another technology system for personal or external use. Personally owned

<h1>POLICY MANUAL</h1>	Date Adopted:        May 23, 2001
Classification: GENERAL ADMINISTRATION	Date Last Amended:
Subject:                Electronics Communications Policy	Approved By:

software, or software not obtained through the District may not be installed or copied to District owned hardware.

- E. Non-District owned hardware may not be installed or used with current District owned hardware.
- F. District owned hardware may not be taken home for personal use.
- G. Respect the integrity of computing systems connected to the District network, the Internet and other on-line services. Please be advised that when using the District technology resources you are acting as an agent of the District.
- H. Know and follow the generally accepted etiquette of e-mail, the Internet and other on-line services. For example, use civil forms of communication.
- I. Avoid uses that reflect poorly on the District.
- J. Under no circumstances shall an employee install free on-line services, e-mail software, Internet access, etc., from a District technology system without prior approval of the Information Systems Coordinator.
- K. Use of “chat services” such as ICQ, AOL-Instant Messenger, Yahoo-Pager, etc., is not to be installed or used on District owned technology resources.
- L. Internal and external e-mail and on-line Internet use.

<h1 style="text-align: center;">POLICY MANUAL</h1>	Date Adopted:        May 23, 2001
Classification: GENERAL ADMINISTRATION	Date Last Amended:
Subject:            Electronics Communications Policy	Approved By:

Acceptable Internal and External E-Mail and On-Line Internet Uses:

1.     Communication and information exchange directly related to the District or Department mission, or to the users work tasks.
2.     Communication and exchange for professional development, to obtain training or education, or to discuss issues related to the users governmental activities.
3.     Use in applying for or administering grants or contracts for District programs.
4.     Governmental tasks or duties.
5.     Announcement and/or tracking of new laws, procedures, policies, rules, services, programs, information or activities.
6.     Any other governmental administrative communications not requiring a high level of security.
7.     Communications incidental to otherwise acceptable use, except for illegal or specifically unacceptable uses.

Unacceptable Internal and External E-Mail and On-Line Internet Uses:

<h1 style="text-align: center;">POLICY MANUAL</h1>	Date Adopted:        May 23, 2001
Classification: GENERAL ADMINISTRATION	Date Last Amended:
Subject:            Electronics Communications Policy	Approved By:

1.     Use of District technology systems, the Internet or any other on-line service for any purposes that violate the law.
2.     Use for any profit activities.
3.     Use for purposes not directly related to the mission or work tasks of the users department.
4.     Use for private business, including commercial advertising and sending or replying to “chain letters”. Use of District computing resources for external consulting is prohibited.
5.     Sending or soliciting sexually oriented messages or images.
6.     Libelous, offensive, or harassing statements, including disparagement of others based on their race, sex, age, disability, religious or political beliefs.
7.     Use for access to and distribution of technology systems, the Internet or other on-line services so as to interfere with or disrupt network users, services, or equipment.

<h1 style="text-align: center;">POLICY MANUAL</h1>	Date Adopted:        May 23, 2001
Classification: GENERAL ADMINISTRATION	Date Last Amended:
Subject:                Electronics Communications Policy	Approved By:

M. Users of Technology services provided by the District shall refrain from:

1. Intentionally seeking out information on, obtain in copies of, modifying, or divulging files, reports, and other data, which is private, confidential, or not open to public inspection or release unless specifically authorized to do so once the legal conditions for release are satisfied.
2. Intentionally copying or printing any software, electronic file, program or data-using District provided technology systems, Internet or other, on-line services without a prior, good faith determination that such copying or printing is, in fact, permissible. Any efforts to obtain permission should be adequately documented.
3. Intentionally seeking information on, obtaining copies of, or modifying files or data without proper authorization. Seeking passwords of others or the exchanging of passwords is prohibited.
4. Intentionally representing themselves electronically as others, either on the District network or on the Internet or other on-line services. Users shall not circumvent established policies defining eligibility for access

<h1 style="text-align: center;">POLICY MANUAL</h1>	Date Adopted:        May 23, 2001
Classification: GENERAL ADMINISTRATION	Date Last Amended:
Subject:            Electronics Communications Policy	Approved By:

to information systems. Conduct, which involves misuse of technology identities, includes:

- a. Allowing an unauthorized individual to use the employees identity.
  - b. Using another person's User-ID without that person's express permission even if that person has neglected to safeguard his/her User-ID.
5. Intentionally developing programs designed to harass other users or infiltrate a technology or computing system and/or damage or alter the software components.
  6. Using District technology resources for fund raising, partisan politics or public relations activities not specifically related to District activities.
  7. Attempting to modify District owned or licensed software or data file without prior written approval by the District's Information Services Coordinator or the staff responsible for maintaining the application.

<h1 style="text-align: center;">POLICY MANUAL</h1>	Date Adopted:        May 23, 2001
Classification: GENERAL ADMINISTRATION	Date Last Amended:
Subject:            Electronics Communications Policy	Approved By:

8.     Attempting to damage or disrupt operation of computing equipment or telecommunication equipment lines. If a user is not familiar with the ramifications of the changes he/she is attempting to make on his/her technology, call the Information Services Coordinator before making any changes.
  
9.     Using District computer resources for purposes other than those intended by the department authorizing access including allowing access by unauthorized persons, even if they are members of the community or District staff.

N.     Additional Guidelines:

1.     Any software obtained from a source other than the District Information Services Division must be virus checked prior to use.
  
2.     When setting up an account at a different information system that will be accessed using the Internet or other on-line service, choose a password that is different than the ones used on District information systems. Do not use the same password for both local and remote systems accessed via the Internet or another on-line service. If the

<h1 style="text-align: center;">POLICY MANUAL</h1>	Date Adopted:        May 23, 2001
Classification: GENERAL ADMINISTRATION	Date Last Amended:
Subject:            Electronics Communications Policy	Approved By:

password used at the remote site were compromised, the different password used locally would still be secure. Passwords should not be so obvious so that others could easily guess them.

3. Log Off. Always make a reasonable attempt to log off or other termination procedure when finished using any technology system or program, especially the Internet and other external technology systems. This will help prevent potential breach of security.
4. E-Mail Security. Unencrypted electronic mail sent or received on the District's e-mail system, the Internet or another on-line service cannot be expected to be secure. Users should always be aware that the sender has no control over what the recipient does with the message, and that the message may be sent to the wrong address or intercepted by hackers.
5. Disclaimers. The public may perceive a users postings and e-mail as official District policy. Users must avoid being drawn into discussions where disclaimers like "this represents my personal opinion and not that of my department or the Fresno Metropolitan Flood Control

<h1 style="text-align: center;">POLICY MANUAL</h1>	Date Adopted:        May 23, 2001
Classification: GENERAL ADMINISTRATION	Date Last Amended:
Subject:            Electronics Communications Policy	Approved By:

District” need to be used. When using e-mail, the Internet and other on-line services provided by the Fresno Metropolitan Flood Control District, users should remember they represent the District. Do not make statements of personal opinion that may be misinterpreted as official District policy.

Users should remember that existing and evolving rules; regulations and personnel guidelines on ethical behavior of District employees and the appropriate use of District resources apply to the use of electronic computing and communications systems supplied by the District.

<h1 style="text-align: center;">POLICY MANUAL</h1>	Date Adopted:      May 23, 2001
Classification: GENERAL ADMINISTRATION	Date Last Amended:
Subject:            Electronics Communications Policy	Approved By:

Failure to comply with the rules and guidelines set forth in the Technology Users Agreement may result in disciplinary actions up to, and including termination.

I, the undersigned, have read and agree to abide by the policies and guidelines expressed in this Technology Users Agreement.

\_\_\_\_\_  
Employee

Date\_\_\_\_\_

\_\_\_\_\_  
Department Head

Date\_\_\_\_\_