East Lake Tarpon Special Fire Control District

SOP 134 Computer, Electronic Communications, and Internet Usage

Implementation Date: 04/26/2016	**Revision Date(s): 04/26/2016**
	Reviewed Date(s):
Forms or Attachments: None	

PURPOSE: This policy provides the guidelines for the use of District computers, and the use of the District computer system by District personnel. It governs the use of District computers, as well as the use of the District computer system for emails, files, data, software, images, voice mails, text messages, electronic communications, and stored electronic communications. This policy also clarifies employee expectation of privacy as it relates to the workplace use of computers, emails, files, data, software, images, voice mails, text messages, electronic communications, and stored electronic communications. To the extent that District issued cellular telephones, personally owned cellular telephones, personally owned computers, and other department issued or personally owned electronic devices utilize the District computer system for access to the intranet and/or Internet, this policy shall be fully applicable.

POLICY: It is the policy of the District to provide personnel with the tools they need to safely and efficiently do their jobs by leveraging technology to the maximum extent possible, while at the same time protecting the District's professional image and reputation. It is further the department's policy to educate and inform employees about the proper purposes for which the computer system may be used, and to set forth the criteria and grounds for which employees may be disciplined for improper use of the computer system.

DEFINITIONS:

Electronic Device – a computer, cellular telephone, personal data assistant (PDA), pager, two-way paging device, iPad, iPod, nook, Kindle, or similar device capable of sending and receiving an electronic communication.

Electronic Communication: Any transfer of signs, signals, writings, images, sounds, data or intelligence that is created, sent, forwarded, replied to, distributed, broadcast, stored, held, copied, downloaded, displayed, viewed, read, printed, or otherwise transmitted in whole or in part by a wire, radio, electromagnetic, photo electronic or photo optical system. This term expressly includes, but is not limited to, emails, attachments to emails, text messages, recorded voicemail messages, web sites visited, computer files, and data files sent over the intranet or Internet, or sent by wired or wireless communication.

Stored Electronic Communication: Any temporary or intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; any storage of an electronic communication for purposes of backup protection of such communication; and any other storage, retention, backup, or archiving of an electronic communication, whether accident, incidental or purposeful, utilizing an electronic storage medium.

Internet: The world-wide system of interconnected computer networks that consists of millions of private, public, academic, business, and government networks linked by a broad array of electronic and optical networking technologies.

Intranet: The District's internal computer system and network.

PROCEDURE

I. General:

1. The District computer system, including all District computers and hardware, the intranet, and access to the Internet provided by the District, are owned by the District. The use of such systems, equipment and access is conditioned upon employee consent to the terms of this policy.
2. The District computer system, District computers and hardware, the intranet, and access to the Internet provided by the District, may not be used by employees for personal gain, including personal businesses, but rather is available to enhance the service that the District provides to the public.
3. The District reserves the right to examine, monitor, intercept, review, copy, store, save, and forward to third parties any and all electronic communications sent or received over the fire department computer system, as well as any stored electronic communication or other files stored on a District computer, hard drive, memory device, or storage medium. The failure of the District to exercise its rights under this section shall not constitute a waiver of these rights.
4. Employees are advised that they have no expectation of privacy in any electronic communication, stored electronic communication, file, image, sound, message, web site visited, or other action or activity while working on a District computer, or while using any other computer, cellular telephone, or electronic device that is accessing the District computer system, including while accessing the Internet through the District computer system.
5. Employees are advised that they have no expectation of privacy in any electronic communication, stored electronic communication, file, image, sound, or message contained on a portable memory device such as a hard disk, flash drive, memory card, CD Rom, DVD, or other media that is attached to/accessible by a District computer, or is attached to/accessible by an electronic device that is accessing the District computer system.
6. Employees are further advised that no employee, including the Fire Chief, has the authority to verbally alter the terms and conditions of this policy under any circumstance.
7. Employees are responsible for any information that they view, access, generate or distribute through the District computer system.

8. Employees are required to prevent the unauthorized use of the District computer system, and for that reason shall use password–protected screen savers or other appropriate techniques while away from their computer. Any use that occurs on an employee's workstation under that employee's login is presumed to be performed by that employee. Employees must log off the computer when not using it, and before leaving the computer unattended.

II. Email

1. Only District personnel are allowed access to the department e-mail system.
2. Employees should not use their District e-mail account as their primary personal e-mail address.
3. Incidental or occasional use of e-mail for personal reasons is permitted.
4. The following e-mail activity is prohibited:
    a. Accessing, or trying to access, another user's e-mail account
    b. Obtaining, or distributing, another user's e-mail account
    c. Using e-mail to harass, discriminate, or make defamatory comments
    d. Jokes, junk mail, chain letters and other non-work-related items should not be sent or forwarded.
    e. Transmitting department records within, or outside, the department without authorization
    f. Advertising political activities which benefit one political candidate or party
    g. Advertising purely commercial activities or events
    h. Any activities which are inconsistent with the mission of the District
    i. Any illegal activities
5. Employees are reminded that email messages may be subject to public disclosure under the Freedom of Information act and may be discoverable during litigation. Assume any email sent over the District system will be viewed by the public.
6. Employees are required to report inappropriate use of e-mail.

III. Confidentiality

District personnel routinely handle information that is considered to be confidential under Federal and state law. This includes information relative to incidents, investigations, patients, and employees, and may include confidential personal information, financial information, and medical information. The following conduct is prohibited when dealing with confidential information:

1. Forwarding or sending confidential information to someone not authorized by law to receive it;
2. Printing confidential information to a printer in an unsecured area where documents may be read by others;
3. Leaving a computer unattended with confidential files logged on, accessible, or visible;
4. Leaving computer disks or memory media with confidential data unattended, in easy to access places.

IV. Prohibited Activities

The following uses of the District computer system are prohibited:

1. Personal use of the District computer system that interrupts District business and that keeps an employee from performing his/her work.
2. Extensive personal use of the internet for any non-work-related purposes during working hours which decreases employee productivity or results in decreased performance of the department e-mail system.
3. Unauthorized downloading and/or distributing of copyrighted materials (e.g. music, videos, photos, games, software, or other proprietary information).
4. Downloading or copying music, videos, photos, or games, including legally obtained music, videos, photos or games, for non-business purposes onto department computers or servers.
5. Unauthorized reading, deleting, copying, modifying, or printing of electronic communication of another user.
6. Using the District's computer system for private gain or profit, including but not limited to, online gambling, personal business, on-line auctions (e-Bay), stock trading, etc.
7. Instant messaging through public service providers. (e.g. AOL, Yahoo, MSN, etc.).
8. Personal software, which allows peer to peer communications between two or more workstations. (e.g. online chat, KaZaA file sharing, etc.).
9. Soliciting for political, religious or other non-departmental reasons.
10. Non- District related streaming media (e.g. listening to internet radio stations, stock tickers, etc.).
11. Using District computers for political purposes.
12. Sending or forwarding junk email, chain letters, or mass mailings.
13. Using, viewing, accessing, or transmitting pornographic or sexually explicit materials, or materials that are offensive, threatening, or constitute hate mail/messaging pertaining to race, national origin, gender or religion.
14. Engaging in any form of harassment, whether sexual or otherwise, or sending any unwelcome personal communication after being asked or instructed to cease communications. It is the perception of the recipient that prevails, not the intention of the sender.

15. Breach or attempt to breach any security mechanisms, hack-into, defeat, disable, or otherwise manipulate the intranet or fire department computer system in order to circumvent a technological measure to gain access to information in ways not permitted or authorized, or to cause the system to react or respond in ways other than as intended by the District administration.
16. Engaging in any illegal activity.