

# Orchard Farm Fire Protection District Standard Operating Procedure

Division: 100 Administration  
Section: 104 Rules and Regulations  
Subject: 104.01 Computer Usage



Supersedes: N/A

Approved By: 

Date: 01/29/2013

Date Last Reviewed: N/A

Page: 1 of 3

---

## PURPOSE:

To provide guidelines and regulations to prohibit unauthorized use of District computers and network, and prevent socially unacceptable material and communications

## RESPONSIBILITY:

All District Personnel

## PROCEDURES:

Use of the department computers and/or electronic information system (network) shall be consistent with the mission of the Fire District. Access of inappropriate sites is strictly forbidden.

Any use of any part of the District's computer network or peripherals implies understanding of, and compliance with, this policy.

Any use of the system must be in conformity to state and federal law, network provider policies and licenses, and District policy. Users are responsible for the appropriateness and content of material they access, transmit or publish on the system. Use of the system shall only occur under the following general guidelines:

1. No person shall have access to the system without having received appropriate training in the use of the system.
2. Non-department personnel shall be prohibited from system use unless expressly authorized by the IT Officer.
3. No software or program may be installed or downloaded onto a computer or the network without prior approval of the IT Officer.
4. Use of the system to access, store or distribute obscene or pornographic material is strictly prohibited.
5. Malicious use of the system to develop programs to harass other users or gain unauthorized access to any computer or computing system and/or damage the components of a computer or computing system is prohibited.
6. Logging onto or utilizing the network under someone else's name is prohibited.

## **Subject 104.01      Computer Usage**

Date: 01-29-2013

Page: 2 of 3

---

7. District Internet access shall not be used to make infringing uses of copyrighted or otherwise proprietary materials. District Internet users shall regard and respect copyright, trademark and license notices in all materials and information accessed. This policy does not preclude the copying of on-line materials for research or educational purposes.
8. Subscriptions to bulletin boards, chat groups and commercial on-line services and other information services must be pre-approved by the IT Officer.
9. Hate mail, harassment, discriminatory remarks or jokes, or other antisocial behaviors are expressly prohibited.

### Security:

Off-site access to the department computer system and/or files is limited to only those department members who have been approved by the IT Officer. Written requests for system access shall be directed to the IT Officer and shall clearly state the specific purpose of the access. Users may not share their password with another person or leave an open file or session unattended. User files and email files are to be used only by the authorized user. Users shall not seek information on, obtain copies of, or modify files, other data, or passwords belonging to other users, or misrepresent other users on the system, or attempt to gain unauthorized access to the system.

Confidential information should not be left open on the screen when the computer is unattended. Confidential information should never be transmitted or forwarded to outside individuals or companies not authorized to receive that information and should not be sent or forwarded to other employees inside the department who do not need to know the information.

Antivirus software is installed and should always be running on District computers. Never disable this software. Never insert any disks or download any files from any outside source without first checking them for viruses.

### E-mail

Please note that e-mail is forever and can never be totally deleted. As such, all email messages are permanent records and can be accessed months or years later by IT professionals. Accordingly, please create and send only messages that are courteous, professional and businesslike.

Due to potentially confidential District information and limited storage capabilities, the District strongly discourages the storage of large numbers of email messages. Accordingly, employees should promptly delete any e-mail messages they send or receive that no longer require action or are not necessary to

## Subject 104.01 Computer Usage

Date: 01-29-2013

Page: 3 of 3

---

an ongoing project. Employees should audit their e-mail messages regularly to identify messages that are no longer needed and that should be deleted.

### District Access

The District has the capability to access, review, copy, modify and delete any information transmitted through or stored in the system, including e-mail messages. The District reserves the right to access, review, copy, modify or delete all such information for any purpose and to disclose it to any party (inside or outside the District) it deems appropriate. Employees should treat the computer system like a shared file system, with the expectation that files sent, received or stored anywhere in the system will be available for review by an authorized representative of the District for any purpose.

### Violation:

Any violation of this policy should immediately be brought to the attention of the Fire Chief or Network Administrator.

Violations could result in loss of network privileges, written reprimand, suspension or termination.

Misuse of any part of the District Network, for any reason, will result in disciplinary action in accordance with the Orchard Farm Fire Protection District's Disciplinary Policy, and may be crimes that could lead to individual criminal prosecution and, upon conviction, to fines and imprisonment.

## DEFINITIONS:

### Inappropriate Sites:

Inappropriate sites include, but are not limited to, sites that contain sexually explicit materials, promote hate or violence, or encourage any type of offensive behavior.

### District Network:

The District network includes the District web site, all individual computers (PCs and laptops) and peripherals, email and file servers, and all other components and software of the District's computer network. **All personally owned computers (PCs and laptops), and peripherals, are considered part of the District's computer network when connected to a District computer, or are accessing the internet through the District's network, and fall under the scope of this policy.**