Township Of Jackson, Fire District 3, Station 55

Standard Operating Guidelines

COMPUTERS

Guideline # 130.28 Date: 1/10 N

PURPOSE

The purpose of this directive is to establish policy and procedures for the use of the District's in house and assigned computers.

POLICY

This District may assign to its employees District owned computers for business purposes. This computer equipment and the data stored within are and remain the property of Jackson fire District 3.

It is the policy of this District that all members abide by the guidelines set forth in this directive when using this agencies in house computer system or any of its components, exchange networks, e-mail, and internal or external databases.

Failure to abide by this policy may result in discipline procedures up to and including termination.

GENERAL

For purposes of this policy, the collective system referred to as the in house computer system includes:

All hardware associated with the server, desktops, and laptops
All applications associated with the server
Windows applications, Word, Excel, Access, Power point, etc.
E-mail applications, Microsoft Outlook
Web Browser applications, Internet explorer, Netscape.etc.
All other software applications licensed to the District.

No employee shall have any expectation of privacy with regards to any information on the in house computer system.

PROCEDURE

Any use of the system must be in conformity to state and federal law, network provider policies and licenses, and District 3 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. Non-department personnel shall be prohibited from system use unless expressly authorized by the Chief or his designee.
2. No software or program may be installed or downloaded onto a computer or the network without prior approval of the Fire Chief.
3. Computer usage shall be limited to Fire Department business, unless authorized by the Fire Chief or his designee.
4. Use of the system to access, store or distribute obscene, inappropriate or pornographic material is strictly prohibited.
5. Participation in or logging into peer-to-peer networks such as MySpace, Face book etc. is prohibited, with the exception of work related sites such as Firehouse.com, Fire Engineering etc.
6. 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.
7. Logging onto or utilizing the network under someone else’s name is prohibited.
8. Internet access shall not be used to make infringing uses of copyrighted or otherwise proprietary materials. Internet users shall regard and respect copyright, trademark and license notices in all materials and information accessed.
9. This policy does not preclude the copying of on-line materials for research or educational purposes.
10. Subscriptions to bulletin boards, chat groups and commercial on-line services and other information services must be pre-approved by the Fire Chief.
11. 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 Fire Chief.

Users shall not share their password with another person or leave an open file or session unattended.

User files and e-mail 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 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 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 virus.

E-MAIL

Please note that e-mail is forever and can never be totally deleted. As such all e-mail 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 number of e-mail messages. Accordingly, employees should promptly delete any e-mail messages they send or receive that no longer require action or are not necessary to an ongoing project. Members should audit their e-mail messages regularly to identify messages that are no longer needed and that should be deleted.

Members are to log on and check for electronic communications daily while on duty to ensure they are informed of any departmental information that may be sent and respond in a timely manner.

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.

Members 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.

Approved:

Date: Date:

Chief: Chief