



**MESCAL J-6
FIRE DISTRICT**

**STANDARD OPERATING
POLICY # 038**

ELECTRONIC COMMUNICATIONS

I. PURPOSE

To provide members with the use of up-to-date electronic communication technology in a way that is beneficial to the member in his job, but not disruptive to the workplace.

II. SCOPE

This policy applies to all members of the District.

III. POLICY

It is the policy of the District to place electronic communication technology devices in the station and to provide Internet access for use by members in conducting District business.

IV. GUIDELINES

- A. Computers are placed in the station so that members may complete their assigned duties and communicate with others outside of the District.
- B. All components of this policy also apply to the use of all personal devices including but not limited to computers, Blackberries, iPhones, iPads, cell phones, etc. that a member may elect to bring on to District premises, as well as to any electronic communication devices that may be the property of the District.
- C. The District utilizes the Internet for business purposes; additionally, the District provides electronic mail addresses for members, and individual access is available through the District computer or other devices. The use of these systems is intended primarily for District-related work activities, as well as for those activities which promote skill building and knowledge enhancement.
- D. It is the responsibility of each member to ensure that District information disbursed via these systems is accurate, appropriate and lawful. Unauthorized copies of copyrighted or licensed materials on the Internet may not be created, distributed, or knowingly utilized.
- E. Members shall not expect privacy in their Internet and electronic communications use; management retains the right to review all member activities on the systems.
- F. Members are to utilize only the software programs provided by the District on the District-owned computers. Downloading of software programs to District computers or other devices may only be done with the prior approval of the Fire Chief. Likewise, exporting system or other computer software is strictly prohibited without the prior approval of the Fire Chief.
- G. While on duty or on District premises, members are prohibited from accessing pornographic or otherwise inappropriate websites. Social networking sites such as Myspace, Facebook, Twitter, YouTube, etc. may be accessed for purposes of conducting District-related business. The use of such networking sites for purposes of general social communications shall be limited to down time and shall not interfere with the completion of one's duties. Additionally, any communications on such sites shall be subject to all of the guidelines set forth within this policy. Member use of such sites shall be subject to monitoring and review. In addition, member's use of such sites while off-duty may come under scrutiny and review if the member posts information on such websites that could reflect unfavorably on the District or its' members.



**MESCAL J-6
FIRE DISTRICT**

**STANDARD OPERATING
POLICY # 038**

ELECTRONIC COMMUNICATIONS

- H. In using the electronic communications, members shall not disclose any confidential information regarding the District, other members, or the public we serve.
- I. Members shall use discretion in ensuring that their electronic communications reflect professional, respectful, and appropriate language and statements. The use of offensive language, disparaging remarks about the District or its members shall not be tolerated.
- J. The posting of any District-related pictures and/or videos to any website shall be at the sole discretion of the Fire Chief; members must obtain approval prior to such action. Members who take pictures at emergency scenes must submit the photos to the Fire Chief for review prior to any use of such pictures.
- K. Confidential information should be protected at all times. Members should take all necessary steps to prevent unauthorized access to this information.
- L. Authorized users are responsible for the security of their individual passwords and accounts; passwords are not to be disclosed to others and should be changed quarterly.
- M. All computers and remote devices should be secured with a password-protected screen saver and set to deactivate after being left unattended in excess of ten minutes.
- N. All computer equipment used by departmental members shall regularly run approved virus-scanning software with a current virus database.
- O. Any introduction of malicious programs (i.e., viruses, worms) into the network or server is strictly forbidden and may result in disciplinary action up to and including termination.
- P. Sending unsolicited e-mail messages (e-mail spam) to individuals who did not specifically request such or creating or forwarding chain letters or other "pyramid" type schemes shall be forbidden.
- Q. Upon termination of volunteer employment with the District, members are prohibited from taking any computer-related programs, files, or materials for personal possession. Access to the District's computer system shall be eliminated at the point of termination.

Approved by the Mescal-J6 Fire District Governing Board on October 12th, 2015. Replaces February, 2012