

# EAST COUNTY FIRE & RESCUE

## Policies, Procedures, and Guidelines

---

**SUBJECT: Internet and Computer Use Policy**

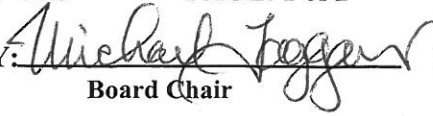
---

**PPG NUMBER: 00.3**

**PAGE: 1 of 2**

**DATE OF ISSUE: 07-17-07**

**APPROVED BY:**

  
Board Chair

**REVIEWED: 09-05-2017**

**BY: Board**

---

### **POLICY:**

The purpose of this policy is to delineate policies and procedures related to electronic communication acquisition and use by District officials, employees and volunteers.

District computer systems shall include but not be limited to, portable lap tops, personal workstations, server stations, phone lines, data lines, hardware, and all software purchased and owned by the District.

### **Computer Usage:**

As a District official, employee or volunteer, you are likely to use computers extensively in duties and tasks related to the agency. In order to protect the agencies computer systems from viruses and ensure that the software used is compatible with the agencies computers only software acquired or approved by a department head may be installed on District computers. Before installing any software not acquired by the department, you must gain approval from the Chief or his designee, or the Information Technology manager.

### **Electronic Mail:**

All electronic media should be professional and business-like. All E-Mail should be viewed as public communications and this media should only be used in a manner that would not be considered inappropriate in the workplace. Some examples of inappropriate communications would be ones that are sexual in nature, racial comments, religious or political solicitations, insubordinate comments or comments which violate confidentiality.

### **Internet Access:**

The Internet provides a valuable tool for research, interaction, communication, and delivery of services.

Except as permitted herein for personal use, all approved internet usage within the department shall be relevant to the job which the user is expected to perform for the agency and to enhance the value, knowledge, or productivity of that job.

Acceptable business use of the Internet will vary depending upon the nature of the employee's job. The following is a list of steps the department may take to limit or monitor employees' access to the Internet;

1. The agency reserves the right to monitor and block access to all inappropriate Internet sites.
2. The agency reserves the right to inspect any and all files stored in public or private areas of the agencies computers and networks to assure compliance with this policy.
3. No software or file downloads via the Internet into the agencies computers without prior approval. The downloads will then become property of the district.

**Personal Use:**

Personal use of the Internet is acceptable. Employees may use their Internet facilities for non-business research or browsing during mealtime or other breaks, or outside of work hours, provided that all other usage policies are adhered to.

**Expectation of No Privacy:**

Employees should have no expectation of privacy, both internally and externally. Remember, all activities are traceable; E-mail or any Internet usage can be compared to sending a postcard through postal mail. Send only information you would not expect others to find objectionable.

The agency administration has the absolute right to examine all the electronic transactions at anytime similar to its rights to examine other aspects of an employee's job. While this does not imply management will look at Internet access files or information, the right to do so is reserved.

The agency will comply with reasonable requests from law enforcement agencies for logs, diaries and archives on individuals' Internet activities.

**File Downloads:**

No files will be downloaded with out prior approval. Files that are downloaded from the Internet may have viruses that may cause damage to the agencies computers. Users are advised to use caution when downloading files. This includes ensuring files originate from professional sites and downloading files needed in your course of work. All agency computers should be installed with virus protection software and all downloaded files should be scanned to prevent infection by harmful viruses. Also any executable files should not be downloaded with out Chief or his designee approval

**Offensive Material:**

The Internet has representations on it of all types of interests, business, education and discussions that occur in a worldwide society. It is possible to accidentally venture into material which you or others may find personally offensive or which violates laws. If that occurs you are expected to immediately back out of such a site and return to acceptable uses of the Internet per this policy.