

**SUBJECT:** COMPUTER USE**SECTION:** 102.09**REVISED:** MARCH 1, 2008**PAGE(S):** 5

---

## **PURPOSE**

The Reading Fire Department network, hardware and software, are provided conducting fire department business and that while incidental personal use is permitted in accordance with the terms of this policy, the user has no personal privacy interests in the use which is subject to inspection and review by the Fire Chief or his/her designees without notice to or consultation with the user.

The Department is also committed to protecting staff members, the patients we serve, and the Department from illegal or damaging actions by individuals and the improper release of protected health information and other confidential or proprietary information.

The Reading Fire Department will take all steps necessary to secure the privacy of all protected health information in accordance with all applicable laws.

---

## **RESTRCTIONS AND PROHIBITIONS**

### **A. Computer Hardware**

1. No person is permitted to access to any computer hardware or software under the control of the Fire Chief unless that person is providing service support pursuant to contract or is a member of the department, who is familiarized with these rules and has signed an user agreement.
2. No computer housing, chassis, monitor, keyboard or accessory will be opened or otherwise accessed without direction or supervision of the Systems Manager(s) or Fire Chief.
3. No member will knowingly cause physical harm, to any component of any computer equipment under the control of the Fire Chief.
4. No member will connect any external or peripheral computer hardware to any computer equipment under the control of the Fire Chief without the consent of the Systems Manager(s).
5. The computer hardware and software are to be used only for the purpose of conducting official fire department business. This prohibition extends to any games or to any programs that are accessible to the user but which have not been installed by the Systems Manager(s), with approval by the Fire Chief.

## **B. Laptop Computers**

1. Portable or “laptop” computers/MDCs/notebooks are to be used solely for the purpose of providing flexible, portable support to personnel in the conduct of official business.
2. Unless required by the circumstances of official business, laptop computers are to be retained in the assigned apparatus.
3. Laptop computers may be used to transfer data in relation to the system network but only under the supervision of the System Manager(s) or Fire Chief.
4. The use of laptop computers fall under the same restrictions for use and understanding of privacy as stated for other system computers.
5. Devices containing confidential or patient information must not be left unintended.
6. If confidential or patient information is stored on device, access controls must be employed to protect improper access. This includes, where possible, the use of passwords and other security mechanisms.
7. Any loss of Laptop or remote devices must be reported immediately to the Fire Chief (Privacy Officer).

## **C. Software**

1. No member will trade or transfer any item of computer hardware or software on any premise controlled by the Fire Chief.
2. No member, with exception of persons under the supervision of the Fire Chief, will use any department owned computer except to gain access to his/her own assigned files, permitted programs or directories through his/her own login password.
3. Unless expressly permitted by the Fire Chief, only the System Manager(s) are authorized to gain access to any computer resource (drives, servers, modems) that was not made available at machine setup.
4. No member is permitted to copy any licensed software which has been procured by the department. The System Manager(s) will copy any copies that are permitted and required.
5. No member shall allow any software licensed to the fire department, or any copy of such software, to be used in conjunction with any computer that is not under the control of the Fire Chief.
6. Each member of the department will protect access to his/her files, programs and directories by creating a password to be used at the time of logging on to the system and no member of the staff will reveal his/her password to anyone. Care shall be taken to “log-off” of the system when your work is completed.
7. No member shall obtain, provide information about, or lists of Reading Fire Department members or patients to parties outside the Reading Fire Department.

#### **D. E-Mail**

1. The Reading Fire Department respects the individual privacy of its employees. However, employee privacy does not extend to the employee's work-related conduct or to the use of fire department equipment and supplies.
2. E-mail systems are available to facilitate business communications among participating users.
3. While each employee has an individual mailbox and password on the system, the system in its entirety will belong to the City of Reading. Therefore, the contents of all e-mail messages will be considered City property.
4. The City of Reading reserves the right to review contents of employee's e-mail communications at any time, for any reason, without prior notification. Members should also be aware that e-mail messages may be considered public record and thus subject to disclosure to the general public. For these reasons, members cannot assume that e-mail messages are confidential.
5. Members should note that if the member deletes an e-mail message, this does not ensure that the message has been deleted throughout the system.
6. E-mail systems are designed to assist in the performance of your assigned work, for official business only, similar to the telephone. Incidental and occasional personal use of e-mail is permitted. However, keep in mind that **all** messages are subject to management review. You should not use e-mail to transmit any message you would not want read by a third party.
7. Content of e-mail messages should be written in a business-like manner. You may not use the e-mail system in any way that may be seen as insulting, disruptive or offensive by other persons, or harmful to morale. Forbidden e-mail transmissions include, but are not limited to:
  - a. Profane or vulgar language;
  - b. Discriminatory, insulting or defamatory remarks or any messages that can be construed to be harassment;
  - c. Sexually-explicit messages, cartoons or jokes;
  - d. Personal propositions, letters or chain letters;
  - e. Solicitation of funds, commercial interests, personal or religious causes, political opinions, campaigns or endorsements;
  - f. Any message that encourages violation of employer policies, procedures, rules/regulations or any message that expresses knowledge or allegations of such violation.
8. Members may not intentionally intercept, eavesdrop, record, read, alter or receive another person's e-mail messages without proper authorization. Members are prohibited from the unauthorized use of passwords of other members.
9. Any suspected violations of this policy should be reported to your supervisor.

## **E. Internet Access**

The Internet provides a powerful medium for sharing a wide range of information globally. Through group communications, sharing of ideas and information can be accomplished with many other users. Fire department business can be research, communications, data and information requests to other users of the Internet.

1. Occasional and incidental personal use may be permitted, subject to the limitations of this policy and subject to the operational needs of the department, as determined by the supervisor.
2. During the course of any communication, members are strongly cautioned not to express any viewpoint, which may be perceived to be an official departmental position or opinion.
3. Restraint should be exercised regarding the time of day and the amount of time spent accessing the Internet.
4. Accessing or downloading materials which are considered adult or sexually oriented, or in any way obscene, salacious or pornographic, is strictly prohibited.
5. The downloading of any programs, including but not limited to, screen savers, is prohibited unless authorization prior by the System Manager(s) or Fire Chief.
6. Internet use is subject to monitoring under the supervision of the Fire Chief. The purpose of this monitoring will be to determine compliance with department policy. Although policy will be that information collected through monitoring is to be used for supervisory purposes and not disseminated generally, users are cautioned that such information is not deemed confidential or private, and that there should be no expectation of privacy in use of the Internet.
7. Accessing a web site or location on the Internet where a fee is charged is prohibited.
8. Participating in chat rooms is prohibited.
9. Interfering with or disrupting network users, services and/or equipment is prohibited.
10. Internet access may be limited or eliminated at the discretion of the Fire Chief.

## **RESPONSIBILITY**

---

- A. It shall be the responsibility of each member to keep confidential information protected at all times, regardless of the medium of which it is stored. Examples of confidential information include, but not limited to, individually identifiable health information concerning patients, patient lists and reports, and research data. Staff members should take all necessary steps to prevent unauthorized access to this information. All inquiries shall be referred to the Fire Chief (Privacy Officer).
- B. It shall be the responsibility of each member to comply with the provisions of this standard and the executed computer user agreement.

- C. It shall be the Officers' responsibilities for enforcing the provisions of this standard and reporting any violations to the Fire Chief immediately.