CARVER FIRE DEPARTMENT

Standard Operating Guidelines

Section 1.20 –Internet/E-mail/Intranet/ Computer **June 15, 2013**

1.0 PURPOSE

The purpose of this guideline is to establish guidelines for the use of fire department electronic systems and/or networks owned and/or operated by the Town of Carver or the Carver Fire Department.

1.1 SCOPE

All Fire Department members

1.2 POLICY

01. The Carver Fire Department respects the individual privacy of its employees. However, employee privacy does NOT extend to the use of the Department's internet, intranet, e-mail or computer networks. The primary purpose of these tools is to aid employees in the course of their duties. Occasional personal use is permitted, except in prohibitive ways as outlined below. Employees should never consider their files private and all files remain the property of the Carver Fire Department.

02. The contents of all files, e-mail folders, hard drives and other storage devices are subject to review by management at any time and such inspections may be announced or unannounced.

03. No employee may send any e-mail, image, audio or video file that contains any of the following: pornography, ethnic or racial slurs, offensive language, obscene material, personal attacks, harassment or disparagement of others, unwelcome propositions or love letters, or any other derogatory e-mail based on sex, race, sexual orientation, age, ethnicity or religion. E-mail shall not be used to question the orders of superior officers or to undermine official policy of the Department.

04. The Internet may not be used to conduct private business or for the purpose of any political campaign or organization

05. Resources of any kind, for which there is a fee, must not be accessed or downloaded without prior approval from a supervisor.

06. Personal use of the Internet should be governed by the same tests of reasonableness as personal phone calls and internal e-mail. These include:

* there is no cost associated with the use.
* use is moderate in time.
* use does not interfere with an employee's or coworkers' work.

07. Employees may not use the Internet to visit inappropriate sites, such as those that feature pornography, promote violence or sponsor hate speech, except in the course of their investigative duties. In such cases, the employee‘s supervisor should be notified in advance, of the employee‘s need to visit these sites as part of an investigation.

08. The Carver Fire Department reserves the right to track an employee‘s use of the Internet, including information available in cookie files.

09. It is the responsibility of employees to NEVER give out their passwords to anyone. Employees should change their passwords frequently. Employees may not use unauthorized codes, passwords or other means to gain access to e-mail belonging to others. If an employee finds that another employee has not logged out of a computer, the employee who discovers this should immediately report this to either the system administrator or the shift commander. No employee may access the e-mail of another employee or send e-mail in the name of another employee by taking advantage of the fact that they are still logged into the system. Employees should always log out when finished using the system.

10. Employees are reminded that management retains the right to access e-mail accounts and employees should not consider their accounts private. E-mail has been deemed a public record and should be treated as such.

11. No employee may install or remove any software or device on any computer without receiving prior permission from the Chief or Deputy. Employees may not knowingly introduce a virus into the system.

12. These policies apply to all present and future computer systems, including mobile data terminals in fire apparatus and laptop terminals.