

Standard Operating Procedures Manual
City of Poquoson Fire and Rescue



**City of Poquoson
Fire and Rescue**

830 Poquoson Ave.
Poquoson, VA 23662
757-868-3510
F757-868-3514

GENERAL ADMINISTRATION

SOP#: GA 15.00

Title: Software Copyright Violation

Effective Date: 02/01/2009

Revised Date: 02/01/2009


Fire Chief's Signature


City Manager's Signature

**SOFTWARE COPYRIGHT
VIOLATION**

I. PURPOSE

To outline software copyright violation policies within the Fire Department.

This SOP is not all-inclusive and cannot encompass all situations that may be encountered.

II. POLICY

The Fire Department has a moral and legal responsibility to abide by copyright related federal laws and standards, specifically those regarding computer software. Therefore, this SOP has been established to assist all personnel in avoiding copyright violations.

Personnel conduct while using city resources are governed by existing city policies including, but not limited to those dealing with property, privacy, misuse of city resources, sexual harassment, equal employment opportunity, data security and confidentiality.

Although connection to the internet and the availability of e-mail offers many benefits, the city and personnel can be at risk if the city's resources are used inappropriately, or in a manner that breaches security or confidentiality.

III. RESPONSIBILITIES

The Fire Chief shall be responsible for overall activities of information technology, including the assurance that no software copyright violations exist on the Department's computer systems. Company Officers shall be responsible for assisting with the compliance of this SOP.

All Fire Department personnel shall be responsible for knowledge and compliance with this SOP and become aware of federal software copyright laws.

IV. PROCEDURES

As per the City of Poquoson Personnel Policy Manual, Section 39:

- E-mail is provided by the City for employees to conduct City business. All employees are to use e-mail as they would any other official City communication.
- Before selecting e-mail as a means for communication or document transmission, users should consider the need for immediacy, formality, accountability, access, security, and permanence. E-mail is more permanent than a telephone conversation, but may be less secure than paper mail since it is so easy to duplicate and distribute.
- All employees should understand that they have no right or expectation of privacy in their use of the Internet or the City's other electronic communications resources, including e-mail. Although the City does not expect to engage in frequent

monitoring of electronic communications by employees, the City reserves the right to monitor and review any employee's access and use of the Internet or the City's other electronic communications resources at any time. All electronic messages and other files created on or transmitted through the City computer network are the property of the City.

- Employees are individually responsible for the content of all text, audio, or images that they distribute using the Internet or the City's other electronic communications resources (including e-mail).
- Sending, knowingly receiving, viewing, downloading, or displaying material that might reasonably be determined unlawful or inappropriate, including obscene or pornographic materials, is not permitted. The Internet and the City's other electronic communications resources may not be used to make or disseminate hate mail, threats, personal attacks, defamatory statements or discriminatory remarks; to engage in harassment; to violate any person's rights of privacy or publicity; or to engage in any similar behaviors. Employees should take particular caution to carefully screen any personal e-mail received from other sources before deciding to forward such messages within or outside the City. Although the City does not intend to prevent our employees from enjoying *occasional* humorous e-mails and similar messages that have become a staple of Internet communications, each employee assumes personal responsibility for the content of any message he or she chooses to send, regardless of who originally created that content. Jokes and other messages that contain content that might reasonable be viewed by another person as offensive or discriminatory may not be circulated using the City's resources. Employees should promptly disclose to an appropriate supervisor any message they receive that they believe contains inappropriate content.

- Sexually explicit material may not be displayed, archived, stored, distributed, edited or recorded using the City's resources.
- Any improper use of the Internet or the City's other computer resources to threaten or harass other, intercept e-mail, infiltrate computer or computing system (e.g., hacking), interfere, clog or damage the performance, files, data, or software components of a computer or computer system (e.g., by spamming or introducing computer virus), or to attempt any of the foregoing, is prohibited. Employees may not use the Internet to disrupt any discussion group, mailing list or newsgroup with frivolous, vulgar or repetitious postings; by posting a binary, or excessively large, unrelated test file; or posting articles that are off-topic according to the charter or other public statement of the forum.
- The bandwidth of the City network is not large enough to support internet radio, or Internet television, or other large interactive files. The City's network should not be used to distribute large e-mail attachments, unless they have a valid business purpose.
- The Internet and the City's other electronic communications resources may not be used to send unsolicited bulk e-mail, or otherwise unsolicited messages where the recipient objects to the content of the message or to the receipt of the message in general. No e-mail or other electronic communications may be sent that hides the identity of the sender or that represents the sender as anyone other than the actual sender.
- No employee may use the City's computer resources knowingly to download, distribute or use software or other information in violation of any intellectual property or other proprietary rights. Also, the introduction of additional software without consideration of the impact on an employee's workstation, or

the network as a whole, could compromise the integrity of the City's system. Therefore, employees may download only software with direct business use, and must arrange to have such software properly licensed, registered, scanned for viruses and authorized by the employee's department head prior to its being downloaded. Downloaded software must be used only in accordance with the terms of its license. Employees may not send or otherwise provide to any other person any software licensed to the City or data owned or licensed by the City unless permitted by the license agreement.

- Employees may not use the Internet to download entertainment software or games, or to play games against opponents over the Internet.
- Employees disclosing confidential information via a newsgroup, discussion list, or chat forum, even if the disclosure is inadvertent, will be subject to all penalties under City policies and procedures.
- Employees may NOT use the Internet for non-business research or browsing.
- The City uses an Internet firewall to assure the safety and security of the City's network. An employee shall not attempt to disable, defeat or circumvent any City security facility.
- Employees also may not use the encryption device or other security protection device on City resources without express written authorization from the City's Systems Administrator. Employee passwords shall be used as instructed and new passwords must be disclosed to the Systems Administrator or designated person as directed.
- Employees should understand that violations of these policies may not only subject them to disciplinary action within the City,

but may expose them to civil and/or criminal action. The City will cooperate with the inquiries of any legitimate law enforcement authority relating to employee use of the Internet or the City other computer resources.

- The City reserves the right to use appropriate software to filter or monitor the Internet access it provides to employees.
- Transitory and personal messages that do not support City business should be destroyed in a timely manner. Any messages kept in the e-mail system are subject to Freedom of Information Act (FOIA) and the Personal Privacy Protection Law (PPPL) because information created or stored in e-mail systems is considered a record for purposes of both laws. FOIL establishes a right of access to records by the public unless one or more specific exemptions apply. PPPL requires agencies to identify and protect any system or records that contain personal information. E-mail messages are also subject to discovery proceedings in legal actions.
- Retention and disposition of records apply to critical e-mail documents and have the same retention periods as other records. To meet filing requirements, e-mails can be printed and filed manually or transferred to an electronic filing system or repository.