Stratmoor Hills Fire Protection District
Policy

Number: **D 5**

Date Issued: November 30, 2005

Revised: December 6, 2017

Date Effective: January 17, 2018

Subject: **COMPUTER / PRINTER / COPY MACHINE & SOCIAL MEDIA USE**

Purpose: In an effort to preserve the public trust and to make the most efficient use of taxpayer funded computers, printers, copy machine and Internet / Social Media access the following guidelines will be followed by all personnel of the Stratmoor Hills Fire Protection District ("SHFPD").

Procedure:

Section 1. Unacceptable Content Viewing

1.1 At no time shall any SHFPD owned computer, or any computer connected to the internet via the SHFPD contracted Internet Service Provider (ISP), be used to view, browse, display, bookmark, or download any content generally considered to be pornographic or "adult" oriented, regardless of whether or not such content violates current laws.

1.2 Persons violating Section 1.1 above will be subject to disciplinary action, to include suspension or dismissal from the SHFPD, as deemed appropriate by the SHFPD Fire Chief ("Fire Chief") or the SHFPD Board of Directors ("Board of Directors"). Further, SHFPD personnel shall not use SHFPD computers to violate the law (including, but not limited to, the viewing of child pornography). Any personnel utilizing a SHFPD computer in violation of the law may be subject to investigation and prosecution by the appropriate law enforcement agencies.

1.3 Any SHFPD member (career and/or volunteer member/recruit) that uses any SHFPD computer to violate the law or encourage others to violate the law. Transmitting of offensive or harassing messages; offering for sale or use any substance the possession or use of which is prohibited by law; viewing, transmitting or downloading materials that encourage others to violate the law; downloading or transmitting confidential information.

1.4 Any SHFPD member (career and/or volunteer member/recruit) that uses any SHFPD computer that can/will cause harm to others or damage to their property. Engaging in defamation (harming another person's reputation by lies); uploading a worm, virus, "trojan horse," "time bomb" or other harmful form of programming or vandalism; participating in "hacking" activities or

any form of unauthorized access to other computers, networks, or information systems.

1.5 Any SHFPD member (career and/or volunteer member/recruit) that uses any SHFPD computer that can/will jeopardize the security of access of the computer network or other networks on the Internet. Disclosing or sharing the user's password with others; impersonating another user; using one's own software programs on the District's computers; altering the District's computer settings; damaging or modifying computer equipment or software.

Section 2. Installation of Software

2.1 Only the SHFPD contracted ISP shall be used to connect and access the Internet on SHFPD owned computers. The installation and use of any other ISP (i.e. AOL, AT&T, etc.) on SHFPD owned computers are prohibited.

2.2 The installation of any software on SHFPD computers not directly related to the business of the SHFPD, or for fire and/or EMS, related training or education is prohibited.

Section 3. E-Mail

3.1 It is the responsibility of all personnel having an official SHFPD e-mail address to check their e-mail on a regular basis, either from a SHFPD owned computer or from any other computer.

3.2 At no time shall official SHFPD e-mail addresses be used for the purpose of sending "SPAM", viruses, gossip, chain-letters or other transmission that are not related to SHFPD business, or for any other inappropriate uses.

3.3 The downloading of e-mail file attachments is strongly discouraged. However, if necessary, such attachments shall not be downloaded without first being screened by virus checking software. The downloading of attachments from non-official e-mail is prohibited.

Section 4. Monitoring Software

4.1 SHFPD reserves to right to install software on any and all SHFPD owned computers, without prior notification, capable of monitoring the usage of said computers. Information gathered via the use of such software may be used for any legal purposes as determined by the Fire Chief and the Board of Directors.

Section 5. Privately Owned Computers

5.1 Privately owned computers shall only be allowed in SHFPD owned buildings while being used by the person owning that computer. At no time shall a privately owned computer become a permanent or semi-permanent fixture in any SHFPD owned building.

5.2 SHFPD personnel are cautioned that although the usage of privately owned computers shall not be monitored by the SHFPD, a person discovered to be viewing inappropriate or illegal material as defined in section 1.1 and 1.2 above while in SHFPD owned building, shall be subject to disciplinary actions.

5.3 At no time shall SHFPD personnel conduct and retain department files or department related business on their privately owned personal computers

on a permanent basis. ALL department business shall be conducted on department approved computers and available for use by all personnel. Exception: personal information such as social security numbers will not be stored on shared drive

Section 6. On-Line Gambling

6.1 The use of SHFPD owned computers for on-line gambling is prohibited.

Section 7. Printing

7.1 The use of SHFPD owned or leased printers are for Fire, EMS and Dispatch related printing only. At no time shall any personnel of SHFPD use any SHFPD owned printer to print any personal information that is not directly tied to SHFPD business.

7.2 Any personnel of SHFPD found to have used a SHFPD printer to print personnel information or papers not related to SHFPD business shall be subject to disciplinary action as set forth herein.

Section 8. Copy Machine

8.1 The use of SHFPD owned or leased copy machines are for Fire, EMS and Dispatch related copying only. At no time shall any personnel of SHFPD use a SHFPD copier to copy any personal information that is not directly related to SHFPD business.

8.2 Any personnel of SHFPD found to have used the SHFPD copy machine to copy any information not related to SHFPD business shall be subject to disciplinary action as set forth herein.

Section 9. Social Media Usage / SHFPD Transmission of Business related Information

9.1 SHFPD acknowledges that the use of technology by emergency service organizations provides several useful benefits including training and the acquisition of useful information for the betterment of the organization and its members. It also allows for the dissemination of information to the public for recruitment, safety education and public relations purposes. As such, the SHFPD embraces the usage of instant technology.

9.2 This policy is not intended to limit SHFPD personnel's freedom of speech or expression; but as SHFPD is a public entity, it has been put in place to protect the rights of SHFPD and its personnel and the public we are sworn to protect. All SHFPD personnel are advised that their speech directly or by means of instant technology either on or off duty or in the course of their official duties that has a connection to their professional duties and responsibilities may not be protected speech under the First Amendment. Speech or other conduct that impairs or impedes the performance of the SHFPD mission undermines the discipline and harmony among co-workers or negatively affects the public perception of SHFPD.

9.3 This policy establishes the SHFPD's social media and instant technology use procedures and protocols which are intended to mitigate associated risks from the use of this technology where possible. This policy applies to all SHFPD personnel (including, but not limited to members of the Board of

Directors, employees, and volunteer members), as well as consultants and contractors of SHFPD performing business on behalf of SHFPD.

9.4 All SHFPD social media pages shall be approved by the Fire Chief or the Board of Directors. All social media content shall adhere to all applicable laws, regulations and policies including the records management and retention requirements set by law and regulation.

9.5 SHFPD understands the value of such technology but also understands the concerns and issues raised when information is released that violates privacy concerns or portrays SHFPD to the public in an illegal or negative manner (intentional or unintentional). Absolutely no SHFPD information, videos or pictures gathered or created while on SHFPD business (including, but not limited to, emergency calls, meetings, drills, details, trainings or anything obtained on organization property or at organization functions) may be transmitted, shared or posted in any format without the approval and written consent of the Fire Chief or Board of Directors

9.6 SHFPD personnel are prohibited from disseminating or transmitting in any manner photographs or images of individuals receiving emergency medical assistance from SHFPD. Any such transmission may violate Colorado Sates Laws and/or the HIPPA privacy rights of such individuals and may result in a criminal and/or civil proceeding being commenced against the personnel violating this provision of the policy.

9.7 All SHFPD personnel must follow the following guidelines when discussing SHFPD on Social Media Websites:

(a) Do not make any disparaging or false statements or use profane language.

(b) Do not make any statements or other forms of speech that ridicule, malign, disparage or otherwise express bias against any race, religion or protected class of individual.

(c) Make clear that you are expressing your personal opinion and not that of SHFPD.

(d) Do not share confidential or personal information.

(e) Do not display Department logos, uniforms or similar identifying items without prior written permission.

(f) Do not post personal photographs or provide similar means of personal recognition that may cause you to be identified as a firefighter, officer or employee of the Department without prior written permission of the Fire Chief or the Board of Directors.

(g) Do not publish any materials that could reasonably be considered to represent the views or positions of SHFPD without written authorization from the Fire Chief or the Board of Directors.

9.8 Disciplinary action against personnel violating this policy may include reprimand, suspension, and termination of employment or termination of volunteer status.

Section 10. Personal Information stored on SHFPD Computers

10.1 At no time shall any SHFPD career employee or volunteer personnel store personal pictures, information, job applications or other personal information on SHFPD computers.