INTERNET AND SOCIAL MEDIA GENERALLY

The District provides access to the internet to assist employees in performing assigned duties and responsibilities. This policy is designed to encourage the appropriate use of the internet, while minimizing security risks. This policy also establishes guidelines for the use of social media by employees and volunteers including but not limited to, social networking sites, blogs, on-line forums, and news articles.

INTERNET USE

1. Internet access is provided to assist in the conduct of District business.

2. Pubic Wi-Fi access is available to guests utilizing District meeting rooms.

3. Violation of this policy may result in loss of privileges or discipline.

4. While accessing the internet through District resources, users should recognize that there is no right of privacy for any electronic record or communication.

5. Use of a password does not give rise to generate any right of privacy.

6. District provided internet access will be used primarily for District business. District members may use the internet for limited personal use but must comply with all other District rules regarding use of District property.

7. The display of any kind of sexually explicit image or document is not allowed. In addition, sexually explicit material may not be archived, stored, distributed, edited, or recorded using the District network or computers.

8. Any software or files downloaded via the internet become the property of the District. Licenses and copyrights applicable to the use of any such file or software will be adhered to according to the manufacturer's license agreement.

9. No member of the District may use the District provided computers to download or distribute pirated software or data.

10. No employee may jeopardize the security of the network by purposefully propagating any virus, worm, Trojan horse, or other malicious program.

11. No employee may use the internet to purposefully disable or overload the network infrastructure, or to circumvent any system intended to protect the privacy or security of another user.

12. Employees are expected to use caution when opening unsolicited email

messages and attachments from unknown sources.

MANAGEMENT OF THE INTERNET

1. The District contracts Information Technology services to a third party. Information Technology personnel utilize software which allows for the retrieval of detailed information regarding web sites accessed, as well as the date, time accessed, and length of time on the site.

2. If employees inadvertently access a restricted site, they should close the site immediately and notify their supervisor of the occurrence.

SOCIAL MEDIA

1. Social media includes a broad spectrum of internet platforms and websites including, but not limited to Facebook, You Tube, Twitter, MySpace, on-line forums, blogs, and news media website comment threads.

1. The District seeks to engage its citizens and stakeholders by using social media tools to promote its mission and share important information.

2. Only authorized District personnel may use social media to conduct District business, including District activities, events, and incidents, recruitment and hiring information and calendars.

3. The District will not release confidential or HIPAA protected information without written permission from the involved parties. If HIPAA protected information is released it will include a statement that informs viewers that consent of the patient was obtained.

4. Photos of an emergency incident shall not be posted to any internet or social media website without authorization from the District.

5. All photos and videos posted to the internet or social media website must be in compliance with HIPAA regulations regarding patient privacy (i.e. not showing patient's face, license plate, or other identifying features).

6. Any photos taken at the emergency scene will be done with appropriate discretion and regard for the potential emotional reaction of the victim, patient, or the general public.

7. The District logo will not be used on a non-District web site in a manner that implies the District endorses and/or has a relationship with an individual or business.

8. Employees or volunteers should be conscious of what they post on social media sites and avoid presenting personal opinions that imply endorsement by the District. If posted material may reasonably be connected to the District or its operations, the material should be accompanied by a disclaimer stating the opinions are the author's only and do not reflect those of the District.

9. Employees and volunteers are reminded to keep the following in mind when using a social media site:
   A. Information posted goes out immediately to thousands possibly millions of people around the world and once published it cannot be undone.
   B. All information posted on the internet is public.
   C. Users should ensure that their online profile is one they wish to share with the public.
   D. Approved friends should be reviewed; keeping in mind these individuals have access to all posted personal information.
   E. Tagged photos should be reviewed to ensure the images portrayed reflect positively on the employee/volunteer or the District.

10. Employees and volunteers who see violations of this policy must address the issue and should report violations to their supervisor.