PREAMBLE

Internet, social networking, and social media (SNSM) usage has the potential for security-related issues and anyone using the Internet with "administrator" privileges is potentially inviting attackers to permanently enter the computer being used and wreak havoc; thus, the Internet and SNSM technologies have become notorious targets for attackers looking for unsuspecting "administrator" users that are unaware of these risks.

All content, comments, and replies posted on any District Internet or SNSM technology are subject to the Missouri Sunshine Law and therefore information disseminated using District Internet and SNSM technologies is subject to being re-printed in newspapers, magazines or online in any other Internet or media format.

All content, comments, and replies posted on any District Internet or SNSM technology that is created or received by District employees – whether during work hours or on personal time, regardless of whether the communication device is publicly or privately owned – may meet the definition of a record as defined by Missouri Sunshine and Missouri State and Local Records Laws.

Missouri law prohibits local governments like the District from entering into agreements which are indefinite in term and uncertain in amount, indemnifying an entity from possible future claims which might arise from the use of a product (because it creates an unfunded contingent liability). The terms of service or terms of use agreements of many Internet and SNSM technologies contain both an indemnification and limitation of liability clause and therefore the District is prohibited from using vendors that employ these clauses as a condition of use of their technology. At this time only Facebook and Twitter are allowed to be used for District SNSM technology.

Missouri law prohibits the District from promoting a political agenda or campaign, e.g., a "Vote Yes" posting or comment is prohibited on a District Internet or SNSM technologies.

The terminology can be intimidating for those unfamiliar with Internet and SNSM technologies; therefore, an appendix of common Internet and SNSM terms is located at the end of this Policy.

POLICY

It is the policy of the District to use approved Internet and SNSM technology to enhance communication, outreach, collaboration, and information exchange while establishing proper use of these tools, consistent with applicable laws and regulations.

It is the policy of the District that District Internet and SNSM technologies should communicate trust and integrity while ensuring brand consistency is achieved, e.g., correct spelling of the District's name; correct logo; etc.

It is the policy of the District that District Internet and SNSM technologies should support proprietary and intellectual property rights, e.g., no copyright infringement.

It is the policy of the District to protect the privacy of the District's patrons, patients, employees, and other stakeholders.

It is the policy of the District that SNSM technology accounts on behalf of the District shall not be created, installed, or implemented without approval.

It is the policy of the District that communications made through the Internet and SNSM technologies do not constitute a legal or official notice or comment to the District or any official or employee of the District for any purpose.

PURPOSE

The purpose of this policy is to provide guidance regarding the creation and use of emerging Internet and SNSM technologies to facilitate collaboration, information sharing, social networking, and social media, e.g., blogs; bulletin boards; virtual worlds; video and photo sharing sites; social networking; podcasts; microblogging, etc.

DEFINITION

Record--document, book, paper, photograph, map, sound recording or other material, regardless of physical form or characteristics, made or received pursuant to law or in connection with the transaction of official business— whether the record was created during work hours or on personal time, and regardless of whether the communication device on which the record was create is publicly or privately owned.

POLICY: **Internet, Social Networking, and Social Media** #892
EFFECTIVE DATE: **03/23/22**
PAGE: **3 of 9**

RESPONSIBILITIES

It is the responsibility of **every District employee** to ensure personal accounts are not used for any District-related business on any Internet or SNSM.

The **Public Information Officer, District Manager,** or **Chief** is responsible for moderating or providing an editorial review of content or comments prior to the posting of information for public view on District Internet or SNSM technologies.

The **Privacy Officer** or designee shall ensure that District employees are made aware of which information to share, with whom information can be shared, and what not to share, e.g., photographs from an incident scene, PII, PHI, etc.

The **Custodian of Records** shall ensure records are retained according to the Missouri State and Local Record Law for all content, comments, and replies posted on any District Internet or SNSM technology that is created or received by District employees.

The **Information Security Officer (ISO)** is responsible for ensuring that the only Internet and SNSM technologies that are implemented are those whose terms of services do not contain indemnification and limitation of liability clauses.

The **Public Information Officer, District Manager,** or **Chief** is responsible for approving specific District Internet or SNSM technologies and executing such terms of service agreements on behalf of the District.

The **Public Information Officer, District Manager,** or **Chief** is responsible for designating District employees who are authorized to create user accounts for Internet or SNSM technologies.

PRACTICES

1. District-owned computers that have access to the Internet shall have a very limited number of "administrator" users as determined by the District ISO.

POLICY: **Internet, Social Networking, and Social Media** #892
EFFECTIVE DATE: **03/23/22**
PAGE: **4 of 9**

2. All District Internet and SNSM technology account profiles and other presences shall prominently display District contact information including, at a minimum:

   a. The legal name of the District, which is the Western Cass Fire Protection District, i.e., the District is not a "department";

   b. The mailing address of Post Office Box 8, Cleveland, Missouri 64734;

   c. The main telephone number of 816-618-3998; and

   d. The general information e-mail address of hello@westerncassfire.org.

3. Only authorized District employees will post moderated content on behalf of the District via the official District Internet and SNSM technologies.

4. Written permission to use or bookmark copyrighted videos, photos, graphics, or other materials must be obtained from the original source prior to use on District Internet and SNSM technologies.

5. District employees should have no expectation of privacy when using the District's Internet and SNSM technologies. The District may request or be provided reports of the District's Internet and SNSM usage by District employees as needed to monitor use.

6. District employees are prohibited from making disparaging comments about the District, its employees, patrons, patients or stakeholders and from engaging in political activity "in uniform" or on any Internet or SNSM forum, which could be considered using their District title to influence a decision or attempt to relay their personal view as that of the District's.

7. Any employee found to have violated this Policy may be subject to disciplinary action, up to and including termination of employment.

<u>USER ACCOUNT PRACTICES</u>

1. A District employee that is authorized to create a user account on behalf of the District for a specific Internet or SNSM technology must immediately provide all pertinent user account information to the Information Security Officer or designee. This includes (but is not limited to) account username and password to manage the specific Internet or SNSM technology.

2. If a District employee is authorized to create a user account on behalf of the District for a specific Internet or SNSM technology makes any changes to a user account, the changed user account information must be immediately provided to the Information Security Officer or designee.

3. The District account profile for District Internet and SNSM technologies should be specific but shall not include any personally identifying information (PII), i.e., "webmaster" instead of "Webmaster John Doe".

4. When the District employee authorized to maintain a specific Internet or SNSM technology on behalf of the District is voluntarily or involuntarily terminated, the District employee's access to the technology shall be immediately removed by the Information Security Officer or designee.

5. The user account names and channel names for District Internet and SNSM technologies shall be as specific and consistent as possible across technologies, and reflect the District's name while conveying the official status—leveraging brand attributes of authenticity and trust, e.g., "westerncass-ems" not "Paramedic1969".

CONTENT POSTING PRACTICES

1. Content postings will reflect the District's stated policy goals for using the technology and should enhance the District's communication efforts.

2. Information posted should be relevant and timely and should not be designed to raise partisan questions, issues, or promote a political agenda or campaign.

3. Content posted should be clear, concise, and relatively informal without being unprofessional. Individual content posts should be stand alone in nature, allowing for the posting to be topic or category oriented and tagged appropriately for search engines and site navigation.

4. Any content that violates commenting practices may be edited, revised, or removed, if necessary.

<u>COMMENTING PRACTICES</u>

1. When commenting functionality is used on District Internet or SNSM technologies, all comments must be moderated by an authorized District employee.

2. Only the Public Information Officer or designee is authorized to speak to traditional media on behalf of the District; meaning only the Public Information Officer or designee is authorized to "speak" in an official capacity for any District Internet or SNSM comment.

<u>POSTING STANDARDS</u>

1. Only content and comments that comply with the District's posting standards should be approved for posting by approved District moderators.

2. Content or a comment found on the District's Internet or SNSM technologies that does not comply with the District's posting standards should be edited, revised or removed.

3. Content or comments found on any District Internet or SNSM technologies website containing any of the following shall not be allowed:

    a. Comments not topically related to the particular content being commented upon;

    b. Profane language or content;

    c. Use of harassing language or tone;

    d. Content that promotes, fosters, or perpetuates discrimination on the basis of genetic information, race, creed, color, age, religion, gender, marital status, status with regard to public assistance, national origin, physical or mental disability or sexual orientation;

    e. Obscene sexual content or links to obscene sexual content;

    f. Solicitations of commerce;

    g. Conduct or encouragement of illegal activity;

h. Information that may tend to compromise the safety or security of the public or public systems;

i. Content that violates a legal ownership interest of any other party;

j. Promotion or opposition of any person campaigning for election to a political office or promoting or opposing any ballot proposition; and

k. Disclosure of information which the District and its employees are required to keep confidential by law or regulation.

RELATED POLICIES

Disciplinary Process 621
Information Security 858
Sunshine Law 872
External Communications 894

STATUTOR REFERENCES

RSMo §67.145
RSMo §109.180
Missouri State and Local Records Law (RSMo §§109.200-109.310)
RSMo §115.646
Missouri Sunshine Law (RSMo 610)
Health Insurance Portability and Affordability ACT (HIPAA)
Health Information Technology for Economic and Clinical Health (HITECH) Act

REVISION HISTORY

Revision Date	Author	Revision Details
March 23, 2022	Monte Olsen	Initial version

APPENDIX OF COMMON INTERNET AND SNSM TERMS

Avatar – A computer user's representation of him or herself or alter ego, whether in the form of a 3-dimensional model used in computer games or a 2-dimensional icon (picture) used on Internet forums and other Internet or SNSM communities.

Blog (Web log) – A website where a blog author can post information on a specific topic targeted to a specific audience. A blog, if commenting is enabled, allows registered members of the public (called blog commenters) to post comments about posts by the blog author.

Bulletin Board – An online messaging system that may also be referred to as a discussion group or board, a message board, or an online forum. On a forum, a registered user can post a message and receive responses to the message on the bulletin board from other registered users.

Channel Name – An alias name the public sees on SNSM technology.

Microblogging – A form of blogging that allows registered users to post short updates, usually 140 characters or less, about themselves and their activities, e.g., Twitter.

Personal Identifiable Information (PII)—Information that can be used to uniquely identify, contact, or locate a single person or can be used with other sources to uniquely identify a single individual.

Photo-Sharing Website – A website that gives registered users a method and location to store their digital photos on the Internet and share them with others.

Podcasts – An audio broadcast that has been converted to an audio file format for playback in a digital music player or computer. The "pod" in podcast was coined from "iPod," Apple's popular portable, digital music player.

Post – A comment made to a SNSM technology, e.g., Facebook users can post to another user's "wall."

Protected health information (PHI)—Information about health status, provision of health care, or payment for health care that can be linked to a specific individual, including any part of a patient's medical record.

Social Bookmarking – A method of taking the bookmarks to pre-existing web pages and posting them to popular news sharing websites. The more a particular article has been bookmarked, the higher on the list it appears at the news sharing websites.

Social Media (SM) - Websites or technologies that focus on creating and fostering online social communities for a specific purpose and connect users from varying locations and interest areas. Social media websites can offer many ways for users to share information including video, audio, images, website links, and other content, e.g., Facebook.

Social Networking (SN) – A tool used to connect people who share common interests or backgrounds using web-based services. Typically, these sites use multiple methods to connect to registered users such as status updates (microblogging), instant messaging, blogs, polls, photo sharing, video sharing, etc., Facebook or LinkedIn.

Tags – Keywords that help people find content on Internet, social media, or social networking sites.

URL (Uniform Resource Locator) – Internet address typed into Internet browser software programs to access an Internet location, e.g., 'http://www.tightwadfpd.org' is a URL.

Video-Sharing Website – A website that gives registered users a method and location to store their digital videos on the Internet and share them with others, e.g., Flickr.

Virtual World/Reality – A computer-simulated environment that attempts to mimic the real world. Through a website and/or software that allows registered users to create a presence in a simulated community using a graphical identification tool known as an avatar which can be used to interact with others in the online world.

Wiki – A web-based tool that allows for collaborative development of documents, such as policies or presentations by allowing visitors to add, remove, edit and change content, with or without the need for registration depending on the settings, e.g., Wikipedia. A wiki also allows for posting links to other Web pages to connect the information.