

<b>POLICY AND PROCEDURE</b>	<b>DATE 1/19/2017</b>	<b>JCSO P&amp;P 363</b>
<b>CHAPTER TITLE: INFORMATION MANAGEMENT INFORMATION TECHNOLOGY</b>	<b>ACCREDITATION STANDARDS: N/A</b>	<b>RE-EVALUATE: AS NEEDED</b>
<b>SUBJECT: INTRANET, INTERNET AND SOCIAL MEDIA</b>	<b>APPROVED:</b>	

### 363. INTRANET, INTERNET AND SOCIAL MEDIA

The Jefferson County Sheriff's Office endorses the secure use of social media to enhance communication, collaboration, and information exchange; streamline processes; and foster productivity. This policy establishes the agency's position on the utility and management of social media and provides guidance on its management, administration, and oversight. This policy is not meant to address one particular form of social media; but rather social media in general, as advances in technology will occur and new tools will emerge.

#### DEFINITIONS

**Digital Communications Manager** - The employee responsible for the agency's social media platforms, responses, strategy and policy decisions.

**Blog** - A self-published diary or commentary on a particular topic that may allow visitors to post responses, reactions, or comments. The term is short for "Web log".

**Intranet** - The Sheriff's Office internal website; a computer network that uses Internet Protocol technology to share information, operational systems, or computing services within the Sheriff's Office.

**Internet** - The external world wide web; an electronic communications network that connects computer networks and organizational computer facilities around the world.

**Internet Posting** - Any written correspondence, photographs or other media depictions made to private or public internet domains.

**Page** - The specific portion of a social media website where content is displayed, and managed by an individual or individuals with administrator rights.

**Post** - Content an individual shares on a social media site or the act of publishing content on a site.

**Profile** - Information that a user provides about himself or herself on a social networking site.

**Social Media** - A category of Internet-based resources that integrate user-generated content and user participation. This includes, but is not limited to, social networking sites (Facebook, Instagram, Snapchat, Nextdoor, LinkedIn), microblogging sites (Twitter, Nixle), photo- and video-sharing sites (Flickr, YouTube, Snapchat), wikis (Wikipedia), blogs, and any other like site.

**Social Networks** - Online platforms where users can create profiles, share information, and socialize with others using a range of technologies.

**Speech** - Expression or communication of thoughts or opinions in spoken words, in writing, by expressive conduct, symbolism, photographs, videotape, or related forms of communication.

**Web 2.0** - The second generation of the World Wide Web focused on shareable, user-generated content, rather than static web pages. Some use this term interchangeably with social media.

**Wiki** - Web page(s) that can be edited collaboratively.

## **POLICY**

Social media provides a potentially valuable means of assisting the Sheriff's Office and its personnel in meeting community outreach, problem-solving, investigative, crime prevention, and related objectives. This policy identifies potential uses that may be explored or expanded upon as deemed reasonable by administrative and supervisory personnel. The Sheriff's Office also recognizes the role that these tools play in the personal lives of some personnel. The personal use of social media can have bearing on departmental personnel in their official capacity. As such, this policy provides information of a precautionary nature as well as prohibitions on the use of social media by agency personnel.

### Employee Internet Postings

The Sheriff's Office expects employees to use common sense when posting on any social media site.

Employees should consider the possible adverse consequences of internet postings, and are encouraged to seek the guidance of supervisors or the digital communications manager regarding any posting that may disrupt law enforcement operations or impede the performance of official duties.

As public employees, personnel are cautioned that while they do not relinquish the First Amendment rights they would otherwise enjoy as citizens to comment on matters of public interest, individuals who accept public employment must also accept certain limitations to those rights. Personnel can express themselves on social media sites to the degree that their speech does not:

- impair working relationships of the sheriff's office for which loyalty and confidentiality are important
- impede the performance of official duties or disrupt law enforcement operations; or
- impair discipline and harmony among coworkers

The Sheriff's Office encourages employees to be proud of where they work and to share appropriate postings on their personal social media sites as they relate to the Sheriff's Office as well as from their daily interactions with the community. For example, a photo of deputies at a child's lemonade stand is fine; a photo showing a crime scene is not. Any postings made to social media sites that include reference to the Sheriff's Office will be shared with the digital communications manager when possible.

The Sheriff's Office is dedicated to ensuring the efficient, harmonious, and non-partisan provision of quality law enforcement to the residents of and visitors to Jefferson County. Additionally, the Sheriff's Office is committed to assuring that law enforcement protection will be available to the public free from political overtones or the appearance of politicized justice and employees of the Sheriff's Office will deal impartially with any individual they encounter. In order to foster this environment, employees of the Sheriff's Office will not display partisan political statements nor political badges, buttons, or similar partisan emblems or images on their social media pages or profiles while in uniform or wearing the agency logo. As an elected official, the Sheriff is exempt from these restrictions.

Employees will consider the impact on officer safety when posting information to social media sites. Deputies/investigators who are, or who may reasonably be expected to work in undercover operations, will not

post any form of visual or personal identification.

Sheriff's Office logos, uniforms, or similar identifying items will not be posted on personal web pages for personal gain.

When using social media, employees should be mindful that their speech becomes part of the worldwide electronic domain. Therefore, adherence to the Sheriff's Office's code of conduct is required in the personal use of social media. Engaging in prohibited speech may provide grounds for undermining or impeaching an employee's testimony in criminal proceedings, may disrupt or hinder law enforcement operations or impede the performance of official duties. Employees are therefore prohibited from the following:

- Speech containing obscene or sexually explicit language, images, or acts and statements or other forms of speech that ridicule, malign, disparage, or otherwise express bias against any race, any religion, or any protected class of individuals;
- Speech involving themselves or other personnel reflecting behavior that would reasonably be considered reckless or irresponsible; and
- Employees may not divulge information gained by reason of their authority; make any statements, speeches, appearances, and endorsements; or publish materials that could reasonably be considered to represent the views or positions of this department.

Employees should be aware that they may be subject to civil litigation for:

- Publishing or posting false information that harms the reputation of another person, group, or organization (defamation);
- Publishing or posting private facts and personal information about someone without their permission that has not been previously revealed to the public, is not of legitimate public concern, and would be offensive to a reasonable person;
- Using someone else's name, likeness, or other personal attributes without that person's permission for an exploitative purpose; or
- Publishing the creative work of another, trademarks, or certain confidential business information without the permission of the owner.

## **PROCEDURES**

### Security and Access

Employees should be aware that privacy settings and social media sites are constantly in flux, and they should never assume that personal information posted on such sites is protected.

Employees should expect that any information created, transmitted, downloaded, exchanged, or discussed in a public online forum may be accessed by the Sheriff's Office at any time without prior notice.

### Intranet and Internet Access and Usage

Access to the sheriff's office intranet system is available to all PCs connected to the JSLEN. Employees are encouraged to use the intranet services and information.

The Sheriff's Office reserves the right to monitor, record and review internet usage at any time. The internet is a public medium and information that is considered to be law enforcement sensitive, confidential, or otherwise restricted for release will not be revealed or posted.

Access to the internet is available to all computers connected to the JSLEN. Internet access may be restricted on computers in sensitive or restricted areas.

Employees may use the internet for non-business browsing and research during breaks, or outside of normal work hours providing that all Sheriff's Office usage policies are observed.

Sheriff's Office computer systems and internet facilities may not knowingly be used to violate the laws or regulations of the United States, the State of Colorado, or any subdivision thereof.

Use of Sheriff's Office computer systems and internet facilities for the purpose of viewing pornographic materials, online gambling, and other gaming other than in the official course of duty is prohibited at all times.

#### Web Content Filtering

The Sheriff's Office will block websites that are categorized as providing content that is prohibited by existing policy, that host exploitative code, that contain potentially damaging content, or are otherwise classified as a security risk. Based upon changing business requirements, the Sheriff's Office may modify the categories of websites and content that will be filtered.

Recognizing the need for unrestricted internet access by some components of the Sheriff's Office, the Information Technology Unit will strategically deploy computers with unlimited internet access for use in investigating criminal activity, internal investigations and background investigations. The internet use on each of these computers will be monitored, but will not be restricted. Unrestricted access computers will have direct access to the internet but will not have any access to internal network resources. No personal use will be permitted on these computers, nor should any files be stored on these machines. In the event of a virus infection to one of the unrestricted access computers, the machine will be re-imaged and any stored data will not be retained.

In the event that an employee finds an internet site that has been blocked but which is deemed necessary for official business, the employee may request an exemption for the identified website. An official request citing the reason and justification for exemption must be submitted through the employee's chain of command for review and action by executive staff. The noted website will be evaluated for security risk by the IT Unit to assist executive staff in their decision.

#### Social Media Site Management

The digital communications manager will maintain and monitor the agency's social networking accounts.

No Web 2.0 application will be initiated or run in the name of the agency without the written consent of the Sheriff. No employee will post material on behalf of the agency without the expressed written consent of the Sheriff. (For example, no one shall create a social media page titled the JeffCo Sheriff K9 Facebook page or a Twitter account posing as the JeffCo Sheriff.)

Requests by divisions/sections/units to utilize "social media" as a formal communications tool must be submitted in writing to the digital communications manager who will then review and make a recommendation to the sheriff or designee.

Requests to develop projects or program-specific uses for any social media tools should be directed to the digital communications manager for consultation and development. Consideration will be given to the appropriate venue and application of tools.

#### **Sheriff's Office Social Media Posting**

##### Department-Sanctioned Presence

Where possible, each Sheriff's Office social media page will include an introductory statement that clearly specifies the purpose and scope of the agency's presence on the website. Efforts should be made to link the pages to the Sheriff's Office's official website. Where possible social media pages should state that the opinions expressed by visitors do not reflect the opinions of the agency.

### Site Creation and Approval

All official Sheriff's Office social media sites or pages must be created and approved by the digital communications manager or as otherwise determined by the Sheriff or designee.

### Commenting and Comment Monitoring

The agency's social networking pages are available for any comment on topics relevant to the business of the agency or in response to a posting. The comments may be positive or negative, praise or criticism. There are several advantages to social media networking to include community outreach and communication and establishing a forum for interested people to share comments and criticisms with the agency so that members may learn about real or perceived shortcomings and respond appropriately either by disseminating correct information, offering an explanation or changing its actions and reporting the change.

Pages will clearly indicate that posted comments will be monitored and that the department reserves the right to remove obscenities, off-topic comments, and personal attacks. Such comments include, but are not limited to, name-calling, profanity, obscenity, defamation or remarks disparaging people on the basis of race, gender, sexual orientation, disability or national origin.

The digital communications manager will remove inappropriate comments from the webpage as soon as they are discovered. If feasible, the digital communications manager will document by screen capture, remove the comment and log the date, time, fan and comment for future reference.

### Site Shut-Down and Archive

The digital communications manager will have the username and passwords to all Sheriff's Office official accounts with the ability to shut down the sites if needed. All social media sites will be archived through Archive Social and employees with official Sheriff's Office social media sites will connect them to Archive Social for that purpose.

### Adherence to Applicable Laws, Regulations and Policies

Social media content will adhere to all applicable laws, regulations and policies including all information technology and records management policies.

Social media content is subject to public records laws. Relevant records retention schedules apply to social media. Content must be managed, stored and retrieved to comply with open records laws and e-discovery laws and policies.

Agency personnel representing the agency via social media outlets will identify themselves as a member of the agency and will adhere to all agency policies.