

Model Policy for a Law Enforcement Agency's use of Social Networking

Disclaimer: This is a model policy was designed to provide a guide to writing a policy related to social networking use. This model policy should be reviewed and revised based on your local legal requirements. Implementation of any of this model policy should be done so only after legal review by your agency attorney. Additionally, your policy prior to implementation will need to conform to any national or local laws, labor agreements and existing policy within the agency.

I. POLICY

That all <Agency Name> police department personnel use computers, computer applications, computer programs, Internet resources and network/Internet communications in a responsible, professional, ethical, and lawful manner. This policy is intended to guide Employees who will use Social Media and Social Media venues to engage with customers on behalf of the agency when it relates to their employment or representations of employment through the numerous social networking venues.

The following rules apply to any online post by an agency staff member that (a) occurs during working hours; (b) is posted using agency equipment; or (c) identifies the agency, links to information about agency or identifies the staff member's position with agency. In the case of (c), these rules also apply to any subsequent posts by the agency member on the same forum (e.g., the same Facebook page, blog, etc.). In addition to being subject to the rules below, all such online activity (a, b and c) is subject to the same rules and guidelines that apply to agency staff members' activities in general, including but not limited to the agency's Email and Internet Acceptable Use Policy and other policies.

The Agency strives to provide the public accurate and timely information, communicated in a professional manner, and in accordance with the laws regarding public information and data practices. This policy provides guidelines for all external communications from the Agency using various social networking mediums.

II. POLICY REVIEW

This policy will be reviewed by the <Appropriate administrative level Supervisor> or any person so designated by the <Chief of Police, Sheriff or lead Law Enforcement Administrator> on an annual basis to ensure that it is legally sound and reasonably enforceable.

III. POLICY TRAINING

All full-time officers, administrative staff, support personnel, student interns and volunteer staff will become familiar with and adhere to the provisions of this policy and receive training and notification pertaining to this policy by in-service training, internal mail, email, and/or occasional network log-on reminders

IV. DEFINITION OF "SOCIAL NETWORKING"

Is defined as social network sites that use Internet services to allow individuals to construct a public or semi-public profile within that system, define a list of other users with whom they

share some connection, and view and access their list of connections and those made by others within that system. The type of network and its design vary from site to site. Examples of the types of Internet based social networking sites include: blogs, networking sites, photo sharing, video sharing, microblogging, podcasts, as well as comments posted on the sites. *The absence of, or lack of explicit reference to a specific site does not limit the extent of the application of this policy.*

Social media includes text, images, audio, and video. Some examples of social media are:

- ▶ Blogs, and micro-blogs such as WordPress and Twitter
- ▶ Social networks, such as Facebook and MySpace
- ▶ Professional networks, such as LinkedIn
- ▶ Video sharing, such as YouTube and vlogs (video weblogs)
- ▶ Audio sharing, such as podcasts
- ▶ Photo sharing, such as Flickr and Photobucket
- ▶ Social bookmarking, such as Digg and Delicious

IV. POLICY GUIDELINES

Guidelines for Authorizing The Use Of Social Media By Agency Employees

When an agency employee identifies a business need for using social media, the employee must present the business case to the agency administrator. If the agency administrator decides to move forward with the use of social media, the agency administrator (or designee) must work with the communications staff to define the goals of the social media use and ensure compliance with this policy.

The communications staff will review any required Terms of Service (TOS) agreement (which may also require legal review by the agency legal advisor) and develop a project plan that identifies:

- ▶ The resources needed to support and sustain the social media tool.
- ▶ Risks and mitigation strategies.

- ▶ How the social media tool integrates with the existing agency website, other social media outlets in use and the general agency communications strategy.
- ▶ Whether or not a unique “use policy” is necessary.

A draft project plan will be presented to the agency administrator, who will then finalize the project plan and make a recommendation for approval. Once the approval has been given, the Communications Director may then authorize the posting of information or prepared materials such as text, documents, video files or streams to a social networking site by agency employees on behalf of the agency. Before the logo or trademark of a private social networking site is featured on an agency web site, the Communications Director should ensure that the use of the logo or trademarks in question is consistent with the agency's purpose.

General Guidelines for All Official Social Networking Communications

All agency employees have the responsibility to help communicate accurate and timely information to the public and in a professional manner. Any employee who identifies a mistake in reporting should bring the error to the agency Communications Director or other appropriate staff member. Communications by employees in an official agency role must comply with all laws related to trademark, copyright and software use. Employees must also follow all Agency policies that may apply.

Communicating on behalf of the Agency

The agency administrator, department directors, and communications staff are authorized to communicate on behalf of the agency in interviews, publications, news releases, on social media sites, and related communications. Other employees may represent the agency if approved by one of these individuals to communicate on a specific topic. When speaking on behalf of the agency:

- Employees must identify themselves as representing the agency. Account names on social media sites must clearly be connected to the agency and approved by [communications coordinator or agency administrator].
- All information must be respectful, professional and truthful. Corrections must be issued when needed.
- Personal opinions generally don't belong in official agency statements. One exception is communication related to promoting an agency service. For example, if an employee posted on the agency's Facebook page, “My family visited the central city park this weekend and really enjoyed the new band shelter”. Employees who have been approved to use social media sites on behalf of the agency should seek assistance from the [communications coordinator or agency administrator] on this topic.

- Employees need to notify [Information Technology or agency administrator] if they will be using their personal technology (cell phones, home computer, cameras, etc) for agency business. Employees should be aware that the data transmitted or stored may be subject to the state statutes governing data retention.

Specific Restrictions when using social media

Social media must not be used to transmit information or knowingly connect to sites for an unlawful or prohibited purpose, including, but not limited to, the following examples:

- ▶ Discrimination on the basis of sex, race, creed, color, gender, religion, age, marital status, national origin, sensory, mental, or physical disability, sexual orientation or veteran status.
- ▶ Sexual harassment or sites containing sexual content.
- ▶ Transmission of obscene materials.
- ▶ Transmission of protected or private information.
- ▶ Infringement on any copyright.
- ▶ Expression of any campaign, political or religious beliefs.
- ▶ Conduct of a personal, outside business, or other financial benefit or gain.

Agency management has the authority to monitor authorized employee use of the Internet to ensure appropriate use.

Guidance for General Social Media Postings

1. Online activity during working hours or using agency equipment must be primarily business related. Incidental personal use is permitted; however, personal use must not impede the staff member's or other staff members' work or adversely impact access to or the use of AGENCY's electronic resources for business purposes.
2. Respect your audience.
3. Don't use religious, racial or ethnic slurs, personal insults, or obscenity. Don't engage in sexual harassment or in any conduct that would not be acceptable offline in a work situation.
4. Show proper consideration for others' privacy and for topics that may be considered objectionable or inflammatory—such as politics, religion and personal life.
5. Do not participate in any political activity or political communication during work hours

- and/or with AGENCY resources (such as computers, blackberries and recording devices).
6. AGENCY staff members are personally responsible for the digital content they publish. Be mindful that what you publish will be public for a long time.
 7. Protect your privacy. Before posting any content, determine what personal information you are comfortable sharing. Remember content can be removed but it can also be forwarded, digitally and manually. Though not directly business-related, background information you choose to share about yourself, such as information about your family or personal interests, may be useful in helping establish a relationship between you and your readers, but it is entirely your choice whether to share this information.
 8. Identify yourself. Anonymous postings are rarely beneficial to anyone. When discussing AGENCY or AGENCY related issues be sure your role at the AGENCY is clear and state whether you are speaking for AGENCY or yourself.
 - a. If you are speaking for yourself, use a disclaimer such as this: "The views in this post are my own and don't necessarily represent my employer's positions, strategies or opinions."
 - b. If you identify yourself as a AGENCY staff member, ensure your profile and related content is consistent with how you wish to present yourself with colleagues and partners. Only those officially designated by AGENCY have the authorization to speak on behalf of the agency.
 - c. The lines between public and private, personal and professional are blurred in online and mobile interactions. By virtue of identifying yourself as an AGENCY staff member, you are now connected to your colleagues and the AGENCY members. Ensure that content associated with you is consistent with your work at AGENCY and AGENCY's mission.
 9. Respect copyright, fair use and public records laws.
 - a. For the AGENCY's protection as well as your own, it is critical that you show proper respect for the laws governing copyright and fair use of copyrighted material owned by others, including AGENCY's own brand. You should never quote more than short excerpts of someone else's work. Always give credit where credit is due, and it is good general practice to link to others' work.
 - b. Where applicable, staff members must follow the state's public records and must not delete content and items without properly retaining these public records according to statute.
 10. Protect confidential and proprietary information. Social media blurs many of the traditional boundaries between internal and external communications. For example, ask permission (and obtain a signed waiver if required) before posting someone's picture or publishing a conversation that was meant to be private.
 11. Prior to any AGENCY events, acquire:
 - a. Written agreements from speakers that all event materials be available to the public.
 - b. Written agreements from participants to use content created and photos/video taken during the event for use on social media.

12. Don't pick fights. Be the first to correct your own mistakes. Don't alter previous posts without indicating that you have done so. When responding to a negative post, state facts and provide supporting documentation. Avoid ongoing conversations that do not progress toward greater understanding.
13. Consider the purpose of the social media use. Online communications must not negatively impact achievement of your assigned tasks and goals or AGENCY's mission.

Handling General Requests

All agency employees are responsible for communicating basic and routine information to the public in relation to their specific job duties including those identified by the agency administration as responsible for social media outlets. Requests for private data or information outside of the scope of an individual's job duties should be routed to the appropriate department or to the data practices authority.

Handling Media Requests:

With the exception of routine events and basic information that is readily available to the public, all requests for interviews or information from the media shall be routed through the agency Communications Director. Media requests include anything intended to be published or viewable to others in some form on a social media outlet (i.e. Facebook, Twitter, or blog). When responding to media requests, employees should follow these steps:

1. If the request is for routine or public information (such as a meeting time or agenda) provide the information and notify agency Communications Director of the request.
2. If the request is regarding information about agency personnel, potential litigation, controversial issues, an opinion on a agency matter, or if you are unsure if it is a "routine" question, forward the request to the agency Communications Director. An appropriate response would be, "I'm sorry, I don't have the full information regarding that issue. Let me take some basic information and submit your request to the appropriate person who will get back to you as soon as he/she can."
 - Ask the media representative's name, questions, deadline, and contact information (email, blog site or twitter name).

Failure to comply with the social media policy

Failure to abide by policies established for use of social media or participation in any activity deemed inappropriate may result in the loss of access privileges. As with any policy, violation may also result in disciplinary action up to and including termination.