Model Policy
for Law Enforcement
Off-Duty Employee 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. That conduct of its employees off off-duty has a reflection on the department. This policy is intended to guide employees conduct when it relates to their employment or representations of employment though the numerous social networking venues.

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*.

IV. POLICY GUIDELINES

a) Self-Identification

Employees may identify themselves as representatives of the agency. However, if they do their actions are reflective of the agency and will conform to the agencies general internet use policy. Self-identification can include the acknowledgment in the user profile for work experience, job

title, etc. by identifying oneself as an employee of agency. Posting on their or another's social networking sites the identification of their employment. If the employee identifies their employment with the agency they take on the responsibility for representing the agency in a professional manner from that period forward while still employed by the agency. If the employee does self-identify themselves as a member of the agency, the employee will at a minimum post on their social networking sites a disclaimers that make it clear that the opinions expressed are solely those of the employee and do not represent the views of the agency. An example of a disclosure to use in these circumstances is:

> "The posts on this site, including but not limited to images, links, and comments by left by readers, are my own and don't necessarily represent my employers positions, strategies or opinions."

b) Confidential and Law Enforcement Sensitive Information

You must take proper care not to purposefully or inadvertently disclose any information that is confidential or law enforcement sensitive. Consult the agency's other policies for guidance about what constitutes "confidential" or "law enforcement sensitive" information. Employees will also honor the privacy rights of our current employees by seeking their permission before writing about or displaying internal agency happenings that might be considered to be a breach of their privacy and confidentiality. Any employee who violates this policies regarding confidentiality can be subject to disciplinary action.

c) Terms of Service

Social networking sites require that users, when they sign up, agree to abide by a terms of service (TOS) document. Agency employees are responsible for reading, knowing, and complying with the TOS of the sites they use. For example, most TOS agreements prohibit users from giving false names or other false information.

d) Copyright

Employees at all times comply with the law in regard to copyright/plagiarism. Posting of someone else's work without permission is not allowed (other than short quotes that comply with the "fair use" exceptions). Other relevant laws that need to be complied with include those related to libel and defamation of character. Employees may not the agency's logos or other identifying items related to their employment without first obtaining written permission from the agency.

e) Productivity

Agency employees need to comply with the general agency Internet use policy and recognize that all time and effort spent on their personal site should be done on their personal time and should not interfere with their job duties.

f) Disciplinary Action

Employees should use common sense in all communications, particularly on a website or social networking site accessible to anyone. What you say or post on your site or what is said or posted on your site by others could potentially be grounds for discipline. If you would not be comfortable with your supervisor, co-workers, or the management team reading your words, do not write them. Recognize that you are legally liable for anything you write or present online. Employees can be disciplined by the company for commentary, content, or images that are defamatory, pornographic, proprietary, harassing, libelous, or that can create a hostile work environment. You can also be sued by agency employees or any individual that views your commentary, content, or images as defamatory, pornographic, proprietary, harassing, libelous or creating a hostile work environment.

g) Investigative Activities

No employees should conduct any activity related ongoing investigations through their personally owned social networking accounts. Employees should refer to their agency policy on conducting online investigations and the investigative use of social networking.