

# Model Policy

<i>Effective Date</i> August 2010		<i>Number</i>
<i>Subject</i> Social Media		
<i>Reference</i>		<i>Special Instructions</i>
<i>Distribution</i>	<i>Reevaluation Date</i> August 2011	<i>No. Pages</i> 4

## I. PURPOSE

The department endorses the secure use of social media to enhance communication, collaboration, and information exchange; streamline processes; and foster productivity. This policy establishes this department'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, rather social media in general, as advances in technology will occur and new tools will emerge.

## II. POLICY

Social media provides a new and potentially valuable means of assisting the department 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 department also recognizes the role that these tools play in the personal lives of some department 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 department personnel.

## III. DEFINITIONS

*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."

*Page:* The specific portion of a social media website where content is displayed, and managed by an indi-

vidual 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, MySpace), microblogging sites (Twitter, Nixle), photo- and video-sharing sites (Flickr, YouTube), wikis (Wikipedia), blogs, and news sites (Digg, Reddit).

*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.

## IV. ON-THE-JOB USE

### A. Department-Sanctioned Presence

1. Determine strategy
  - a. Where possible, each social media page shall include an introductory statement that clearly specifies the purpose and scope of the agency's presence on the website.
  - b. Where possible, the page(s) should link to the department's official website.
  - c. Social media page(s) shall be designed for

- the target audience(s) such as youth or potential police recruits.
2. Procedures
    - a. All department social media sites or pages shall be approved by the chief executive or his or her designee and shall be administered by the departmental information services section or as otherwise determined.
    - b. Where possible, social media pages shall clearly indicate they are maintained by the department and shall have department contact information prominently displayed.
    - c. Social media content shall adhere to applicable laws, regulations, and policies, including all information technology and records management policies.
      - (1) Content is subject to public records laws. Relevant records retention schedules apply to social media content.
      - (2) Content must be managed, stored, and retrieved to comply with open records laws and e-discovery laws and policies.
    - d. Where possible, social media pages should state that the opinions expressed by visitors to the page(s) do not reflect the opinions of the department.
      - (1) Pages shall clearly indicate that posted comments will be monitored and that the department reserves the right to remove obscenities, off-topic comments, and personal attacks.
      - (2) Pages shall clearly indicate that any content posted or submitted for posting is subject to public disclosure.
  3. Department-Sanctioned Use
    - a. Department personnel representing the department via social media outlets shall do the following:
      - (1) Conduct themselves at all times as representatives of the department and, accordingly, shall adhere to all department standards of conduct and observe conventionally accepted protocols and proper decorum.
      - (2) Identify themselves as a member of the department.
      - (3) Not make statements about the guilt or innocence of any suspect or arrestee, or comments concerning pending prosecutions, nor post, transmit, or otherwise disseminate confidential information, including photographs or videos, related to department training, activities, or work-related assignments without express written permission.
      - (4) Not conduct political activities or private business.
        - b. The use of department computers by department personnel to access social media is prohibited without authorization.
        - c. Department personnel use of personally owned devices to manage the department's social media activities or in the course of official duties is prohibited without express written permission.
        - d. Employees shall observe and abide by all copyright, trademark, and service mark restrictions in posting materials to electronic media.
  - B. Potential Uses
    1. Social media is a valuable investigative tool when seeking evidence or information about
      - a. missing persons;
      - b. wanted persons;
      - c. gang participation;
      - d. crimes perpetrated online (i.e., cyberbullying, cyberstalking); and
      - e. photos or videos of a crime posted by a participant or observer.
    2. Social media can be used for community outreach and engagement by
      - a. providing crime prevention tips;
      - b. offering online-reporting opportunities;
      - c. sharing crime maps and data; and
      - d. soliciting tips about unsolved crimes (i.e., Crimestoppers, text-a-tip).
    3. Social media can be used to make time-sensitive notifications related to
      - a. road closures,
      - b. special events,
      - c. weather emergencies, and
      - d. missing or endangered persons.
    4. Persons seeking employment and volunteer positions use the Internet to search for opportunities, and social media can be a valuable recruitment mechanism.
    5. This department has an obligation to include Internet-based content when conducting background investigations of job candidates.
    6. Searches should be conducted by a nondecision maker. Information pertaining to protected classes shall be filtered out prior to sharing any information found online with decision makers.
    7. Persons authorized to search Internet-based content should be deemed as holding a sensitive position.
    8. Search methods shall not involve techniques that are a violation of existing law.
    9. Vetting techniques shall be applied uniformly to all candidates.
    10. Every effort must be made to validate Internet-based information considered during the hiring process.

## V. PERSONAL USE

### A. Precautions and Prohibitions

Barring state law or binding employment contracts to the contrary, department personnel shall abide by the following when using social media.

1. Department personnel are free to express themselves as private citizens on social media sites to the degree that their speech does not impair working relationships of this department for which loyalty and confidentiality are important, impede the performance of duties, impair discipline and harmony among coworkers, or negatively affect the public perception of the department.
2. As public employees, department personnel are cautioned that speech on- or off-duty, made pursuant to their official duties—that is, that owes its existence to the employee’s professional duties and responsibilities—is not protected speech under the First Amendment and may form the basis for discipline if deemed detrimental to the department. Department personnel should assume that their speech and related activity on social media sites will reflect upon their office and this department.
3. Department personnel shall not post, transmit, or otherwise disseminate any information to which they have access as a result of their employment without written permission from the chief executive or his or her designee.
4. For safety and security reasons, department personnel are cautioned not to disclose their employment with this department nor shall they post information pertaining to any other member of the department without their permission. As such, department personnel are cautioned not to do the following:
  - a. Display department logos, uniforms, or similar identifying items on personal web pages.
  - b. Post personal photographs or provide similar means of personal recognition that may cause them to be identified as a police officer of this department. Officers who are, or who may reasonably be expected to work in undercover operations, shall not post any form of visual or personal identification.
5. When using social media, department personnel should be mindful that their speech becomes part of the worldwide electronic domain. Therefore, adherence to the department’s code of conduct is required in the personal use of social media. In particular, department personnel are prohibited from the following:
  - a. 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.
  - b. Speech involving themselves or other department personnel reflecting behavior that would reasonably be considered reckless or irresponsible.
6. Engaging in prohibited speech noted herein, may provide grounds for undermining or impeaching an officer’s testimony in criminal proceedings. Department personnel thus sanctioned are subject to discipline up to and including termination of office.
7. Department personnel 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 without express authorization.
8. Department personnel should be aware that they may be subject to civil litigation for
  - a. publishing or posting false information that harms the reputation of another person, group, or organization (defamation);
  - b. 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;
  - c. using someone else’s name, likeness, or other personal attributes without that person’s permission for an exploitative purpose; or
  - d. publishing the creative work of another, trademarks, or certain confidential business information without the permission of the owner.
9. Department personnel 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.
10. Department personnel should expect that any information created, transmitted, downloaded, exchanged, or discussed in a public online forum may be accessed by the department at any time without prior notice.
11. Reporting violations—Any employee becoming aware of or having knowledge of a posting or of any website or web page in violation of the provision of this policy shall notify his or her supervisor immediately for follow-up action.

### **Acknowledgment**

This *Model Policy* was developed by the International Association of Chiefs of Police (IACP) Center for Social Media in conjunction with the IACP National Law Enforcement Policy Center. We are appreciative of the many policy agencies across the country who shared their existing policies.

Every effort has been made by the IACP National Law Enforcement Policy Center staff and advisory board to ensure that this model policy incorporates the most current information and contemporary professional judgment on this issue. However, law enforcement administrators should be cautioned that no "model" policy can meet all the needs of any given law enforcement agency. Each law enforcement agency operates in a unique environment of federal court rulings, state laws, local ordinances, regulations, judicial and administrative decisions and collective bargaining agreements that must be considered. In addition, the formulation of specific agency policies must take into account local political and community perspectives and customs, prerogatives and demands; often divergent law enforcement strategies and philosophies; and the impact of varied agency resource capabilities among other factors.

This project was supported by Grant No. 2006-DG-BX-K004 awarded by the Bureau of Justice Assistance, Office of Justice Programs, U.S. Department of Justice. The Assistant Attorney General, Office of Justice Programs, coordinates the activities of the following program offices and bureaus: the Bureau of Justice Assistance, the Bureau of Justice Statistics, National Institute of Justice, Office of Juvenile Justice and Delinquency Prevention, and the Office of Victims of Crime. Points of view or opinions in this document are those of the author and do not represent the official position or policies of the United States Department of Justice or the IACP.

© Copyright 2010. International Association of Chiefs of Police, Alexandria, Virginia U.S.A. All rights reserved under both international and Pan-American copyright conventions. No reproduction of any part of this material may be made without prior written consent of the copyright holder.