#### OFFICE OF THE CHIEF OF POLICE

<u>NOTICE</u> 14.5 March 12, 2015

TO:

All Department Personnel

FROM:

Chief of Police

**SUBJECT:** 

SOCIAL MEDIA USER GUIDE

This Notice introduces the Social Media User Guide (Guide). The Department recognizes the importance of social media and the right of employees to engage in the use of social media as private citizens. The Guide provides direction on Department-sanctioned uses of social media as an integral part of the Department's community relations mission, situational awareness, and as an investigative tool.

Specialized units with existing policies and procedures for the use of online communications, including, but not limited to, Anti-Terrorism Intelligence Section and Internet Crimes Against Children Unit are not affected by these guidelines. These units should continue to follow their respective approved guidelines regarding Online Undercover Activity.

Major Crimes Division is responsible for updating the Guide. The "Organization and Functions of the Los Angeles Police Department" link on the Department's Local Area Network will be updated accordingly.

Any questions regarding this Notice should be directed to Major Crimes Division, at (213) 486-7220.

CHARLIE BECK Chief of Police

Attachment

DISTRIBUTION "B"

# LOS ANGELES POLICE DEPARTMENT Major Crimes Division



# SOCIAL MEDIA USER GUIDE

2015

# Contents

INTRODUCTION	
SOCIAL MEDIA DEFINED	3
SOCIAL MEDIA BENEFITS	4
FIRST AMENDMENT CONCERNS	4
FOURTH AMENDMENT CONCERNS	4
DEPARTMENT-SANCTIONED USES OF SOCIAL MEDIA	5
1. SITUATIONAL AWARENESS	5
2. INVESTIGATIONS	5
INVESTIGATOR RESPONSIBILITIES	6
INVESTIGATIVE EXAMPLES	6
3. COMMUNITY RELATIONS/ENGAGEMENT	6
COMMUNITY RELATIONS/ENGAGEMENT EXAMPLES	7
USE OF PERSONAL EQUIPMENT	
PROHIBITED USES	7
HOW TO START USING SOCIAL MEDIA: DOs AND DON'Ts	8
DOs:	8
DON'Ts:	9
SOCIAL MEDIA-RELATED POLICIES	9

#### INTRODUCTION

The Social Media User Guide (Guide) provides direction on Department-sanctioned uses of social media: as an integral part of the community relations mission, for situational awareness, and as an investigative tool. The Department recognizes the importance of social media and the right of employees to engage in the use of social media as private citizens.

This Guide constitutes a set of guiding principles. All existing Department policies and directives governing general on-duty and off-duty conduct also apply to activity on the Internet including internet usage guidelines found in Department Manual Section 3/788.40. Due to the diverse needs of specialized units, rules for social media use within the scope of investigations may at times deviate from this Guide, subject to approval from the unit's commanding officer.

Specialized units with existing policies and procedures for the use of online communications, including, but not limited to, Anti-Terrorism Intelligence Section and Internet Crimes Against Children Unit are not affected by these guidelines. These units should continue to follow their respective approved guidelines regarding Online Undercover Activity.

#### SOCIAL MEDIA DEFINED

Social media is a category of Web-based services that incorporate user-generated content and user participation. These services allow users to create public or semi-public profiles within a finite system, articulate a list of other users with whom they share a connection, and view and navigate this list and lists made by others within the system. Within the broad category of social media are social network sites such as Facebook, microblogging sites like Twitter, photograph sharing and video sharing sites, wikis, blogs, and news sites such as Reddit. On these sites, users create online communities to share information, ideas, personal messages and other content.

The following are terms related to social media:

- Blog: A diary or commentary on a particular topic that may allow visitors to post responses.
- Chat Room: Any form of online conferencing technology ranging from real-time online chat and online interaction with other participants over instant messaging and online forums to fully immersive graphical social environments whether or not the access is restricted.
- Fictitious Online Persona: A fictitious identity created on the Internet.

<sup>&</sup>lt;sup>1</sup> "International Association of Chiefs of Police (IACP), Social Media Model Policy," (III. Definitions, August 2010).

<sup>&</sup>lt;sup>2</sup> Boyd, D.M, Ellison, N.B "Social Network Sites: Definition, History, and Scholarship," *Journal of Computer-Mediated Communication*, *13*(1), Article 11 (2007). http://jcmc.indiana.edu/vol13/issue1/boyd.ellison.html.

<sup>&</sup>lt;sup>3</sup> Merriam-Webster Online, s.v. "social media," accessed February 14, 2013. http://www.merriam-webster.com/dictionary/social%20media.

- **Listening:** The continuous conduct of searches of content on the Internet for any discussions, posts, videos, blogs, and online conversations about the Department or other topics of interest to the Department. The purpose of listening is to discover what is being said online, raise awareness about the community, and put oneself in a position to correct false information or rumors.<sup>4</sup>
- Online Investigative Activity: The use of a Fictitious Online Persona to engage in investigative activity. Fictitious Online Personas created for the purposes of identifying and examining trends and tactics, developing profiles, or conducting research does not constitute online undercover activity.
- Online Undercover Activity: The use of a Fictitious Online Persona to engage in ongoing interactive communication existing over the Internet with an identified person or group and is related to an ongoing investigation.
- Wiki: Web page(s) that can be edited collaboratively. Wikipedia is an example.

### **SOCIAL MEDIA BENEFITS**

Reviewing social media for items of importance is referred to as listening.<sup>6</sup> Social media can enhance community outreach, problem solving, investigations, crime prevention, and related objectives. There are many benefits to listening on social media channels, including awareness of what is happening in and around the community, and what is being said about the City, the Department, officers, or events. Listening during a large event can help guide resource allocation, service efforts, and assist with mitigating criminal activity.

#### FIRST AMENDMENT CONCERNS

Social media sites are a platform for people to express themselves, including political and religious beliefs, or views on government.<sup>7</sup> The Department expressly recognizes the right of public expression. Employees should not interfere with the public's right to free speech, with the exception of those categories of speech that are not constitutionally protected (i.e., bomb threats). In addition, Department personnel shall never act as agent provocateur (an individual employed, directed, encouraged or allowed to associate with target members or groups in order to incite them to illegal action).

#### FOURTH AMENDMENT CONCERNS

The public has the right to be free from unreasonable searches and seizures. Employees should comply with the Fourth Amendment protections as they might apply to password protected or otherwise private social media sites or forums. Case law is still developing in this area. Many social media posts are public, but employees must be mindful of what is legally accessible and consistent with community standards and expectations. Nothing in this Guide shall relieve employees from existing "Search and Seizure" laws and policies related to social media. In the absence of clearly defined standing legal direction, official guidance should be sought from the prosecuting authority (i.e., City or District Attorney).

<sup>&</sup>lt;sup>4</sup> International Association of Chiefs of Police, "Listening Strategy Fact Sheet" (July 2011).

<sup>&</sup>lt;sup>5</sup> "Intelligence Guidelines for Major Crimes Division Anti-Terrorism Intelligence Section."

<sup>&</sup>lt;sup>6</sup> "Listening Strategy Fact Sheet," IACP, (June 2011).

<sup>&</sup>lt;sup>7</sup> "Developing a Policy on the Use of Social Media in Intelligence and Investigative Activities: Guidance and Recommendations." IACP National Law Enforcement Policy Center [Executive Summary, (February 2013)].

#### DEPARTMENT-SANCTIONED USES OF SOCIAL MEDIA

The Department recognizes three primary law enforcement uses of social media:

- Situational Awareness
- Investigations
- Community Relations/Engagement

# 1. Situational Awareness

Social media situational awareness is gained by the passive and active searching for information impacting operations, including information found in discussion forums, posts, videos, and blogs. Some of the many tools available to assist with listening to social media to gain situational awareness include:

- Google Alerts are e-mail updates on user-defined search terms.
- Search.Twitter.com users can conduct and save searches of terms on Twitter.
- YouTube, Vimeo, Daily Motion, etc. are video sharing sites.
- Craigslist and Backpage.com can be searched for upcoming community events.
- RSS Feeds allow new content to be sent directly to the user.
- Local Blogs provide information on specific neighborhoods, areas, and lifestyles.
- Subscriptions to social media sites allow users to review current happenings.

The following are examples of the use of social media for situational awareness:

- Policing a Nationally Televised Sports Event. Using social media, officers can identify crimes and deploy proper resources.
- **Protecting Community Gatherings**. Social media can be used for active and passive online searches that assist in protecting large community events.

Prior to using social media for Department-sanctioned purposes, employees should read, understand and adhere to all Department network security procedures.

**Note:** The Cyber Support Unit of each Area is still a good resource for officers and detectives to use for their everyday Cyber support and questions (refer to Operations Order No. 2, Cyber Support Unit – Revised, dated February 28, 2014).

# 2. Investigations

Social media, like any other lawful investigative method, may be used to collect evidence for a criminal case. In this capacity, social media use can be covert and/or clandestine and target a specific suspect or crime. When social media evidence deemed material to an investigation is collected, it should be:

- Printed out on paper (if feasible) and stored in the investigation case package; and,
- Preserved digitally in a format that can be shared during discovery.

<sup>&</sup>lt;sup>8</sup> Department Internet Usage Guidelines, Special Order No. 13, dated May 6, 1999.

Online Undercover Activity is defined as the use of a Fictitious Online Persona to engage in ongoing interactive communication over the Internet with an identified person or group and is related to an ongoing investigation. Fictitious Online Personas created for examining trends, tactics, developing profiles, or conducting research do not constitute Online Undercover Activity. Unique requirements of specialized units using social media in either a covert or clandestine capacity may result in deviations from this Guide, subject to approval from the unit's commanding officer.

Investigator Responsibilities: Investigators using a Fictitious Online Persona or conducting Online Undercover Activity must follow the below guidelines. Any deviations must be approved in writing by their Commanding Officer.

- a) Obtain approval from his/her commanding officer prior to using a Fictitious Online Persona during an investigation or conducting Online Undercover Activity. If prior approval was not obtained, the employee should notify his/her supervisor as soon as practicable. Approval may be granted telephonically, and the supervisor must initial the approval document (i.e., Follow-Up Investigation, Form 03.14.00, or the Chronological Record, Form 03.11.06) as soon as practicable;
- b) Document the approval, which should be maintained by the investigator;
- Supervisors approving Online Undercover Activity must notify the commanding officer of the respective investigative unit and document it on the investigator's Follow-Up Investigation, or the Chronological Record;
- d) Ensure that communications obtained during the use of the Fictitious Online Persona or during the Online Undercover Activity that are material to the investigation are documented on a Follow-Up Investigation, or the Chronological Record;
- e) Evaluate information obtained through social media resources for source reliability and content validity; and,
- f) Employees must comply with the LA CLEAR memorandum of understanding regarding deconfliction procedures when establishing and maintaining Fictitious Online Personas.

Investigative Examples: The following are examples of the use of social media for investigative purposes:

- Criminal Investigations. An investigator accessed a missing juvenile's social media account and used it to locate her. The juvenile had posted her location and condition, allowing peers to communicate, but keeping her parents unaware. Social media is now an integral part of missing juvenile investigations.
- Online Stings. Burglary detectives identified goods consistent with frequently stolen items. Detectives negotiated with the suspect to "buy" the items.

# 3. Community Relations/Engagement

Social media is also an extension of the Department's Community-Based Policing principles, guided by the Department's Media Relations Handbook.

<sup>&</sup>lt;sup>9</sup> Intelligence Guidelines For Major Crimes Division Anti-Terrorism Intelligence Section. Los Angeles Police Department Board Of Police Commissioners, dated September 25, 2012.

Community Relations Officers should incorporate social media as part of their regular duties. Senior Lead Officers should develop and maintain appropriate social media platforms including:

- Using Skype or Facebook for virtual neighborhood meetings.
- Using Facebook for a specific crime issue or area safety hazard.
- Developing a blog to keep in contact with community members.
- Starting a youth page to encourage constructive activities.
- Using Yelp to reach out to citizens who have checked in at a police station.

# Community Relations/Engagement Examples: The following are examples for using social media for community relations:

- Officer-Involved Shooting: After an officer-involved shooting, the watch commander used social media to identify and dispel rumors. He/She clarified the facts by disseminating information from the press release, resulting in an increase of public support for the police department.
- Community Service/Freeway Closure: The Department proactively disseminated information to assist drivers and citizens with a weekend closure of a major freeway. Continually updated posts reflected construction status and predicted an earlier than expected opening of the public road.

# **USE OF PERSONAL EQUIPMENT**

Department personnel may use personal equipment to access information via social media sites when performing an authorized law enforcement mission with prior approval from the employee's commanding officer. Approval should be documented in the Employee's Report, Form 15.07.00, as per Department Manual Section 3/788.30. If prior approval cannot be obtained due to exigent circumstances, the employee should notify his/her supervisor and complete an Employee's Report, as soon as practicable. All work involving the use of personal equipment should remain in accordance with the Fair Labor Standards Act (FLSA). Personnel assigned to social media-related duties outside of their regular work shift shall obtain written permission from their commanding officer.

#### PROHIBITED USES

Posting inappropriate material, including photographs, via Department-sanctioned social media profiles is a violation of Department policy. The use of photographs for social media profiles should not infringe upon copyright law and should adhere to relevant legal regulations and Department policy. Generally, the use of photographs without the permission of the owner is prohibited. Some examples of prohibited onduty social media use include:

- Engaging in illegal or illicit activities.
- Exploiting relationships for personal reasons.
- Converting on-duty contacts into off-duty relationships.
- Expressing or promoting political, social or religious beliefs.
- Endorsing commercial products.
- Posting racist, sexist, bigoted, or pornographic words, photos, images, or other media.
- Unapproved use of the Department's official trademarked images (i.e., badge, logos, motto).

#### HOW TO START USING SOCIAL MEDIA: DOS AND DON'TS

#### DOs:

- Use popular sites such as: YouTube, Twitter, Facebook, etc;
- Use MCG LAPD Online Unit to set up accounts;
- Adhere to the Media Guide when releasing information;
- Read local blogs, such as Eastsider LA, LAist, Patch, Times Blog, Yelp;
- Use Google Alerts and other similar services to help identify important information;
- Preface all social media presences with language, which clearly states that said site is not an open public forum, and is subject to policy; and,
- Communicate respectfully.

#### The following is an example of a well-written policy statement for Facebook:

"The purpose of this site is to present matters of community interest concerning [the entity's] programs, activities, news stories, and photos. We welcome your comments; however, please note that this is a moderated online discussion site and not a public forum.

Comments made to our page will be reviewed, and while comments will not be edited by our personnel, [the entity] reserves the right to remove comments that include:

- Comments unrelated to the programs, activities, news stories or photos of [the entity]. The page is not meant for comments that do not directly relate to the purpose or topical scope of the page;
- Obscenity;
- Child pornography;
- Incitement to imminent lawless action;
- Speech presenting a grave and imminent threat;
- Fighting words;
- True threats:
- Fraud:
- Defamation (libel/slander);
- Solicitations to commit, or speech integral to, criminal conduct;
- Promotion or advertisement of a business or commercial transaction;
- Promotion in favor of, or in opposition to, a candidate campaigning for election to a political
  office; and,
- Material posted without the copyright holder's consent.

[The entity] may take steps to have a comment removed if it falls within one of the foregoing categories.

Also, please keep in mind that this is an internet page on facebook.com. Facebook, Inc. owns and operates facebook.com. It has its own policies and standards concerning what may, and what may not, be posted and the actions that it may take with regard to unauthorized posts. See "Facebook Community Standards" at www.facebook.com/communitystandards/.

[The entity] may also take steps to remove "robospam" and/or comments by "social bots" (i.e. content posted by automatic software programs, or "hots"), if necessary, to ensure access for the general public.

[The entity] is not responsible for, and neither endorses nor opposes, comments placed on this site by visitors to this site. Commenters are personally responsible for their own comments, username, and/or any information placed on this page by the commenter."

#### DON'Ts:

- Engage in offensive behavior/inappropriate comments;
- Endorse a vendor or the use of certain products;
- Release investigative details or photos; and,
- Use Department social media for non-Departmental or personal reasons.

#### SOCIAL MEDIA-RELATED POLICIES

Department employees who choose to use social media sites for personal use or Department-related activities are reminded to adhere to Department policies and procedures, including, but not limited to:

- Department Manual Section 1/210.35, Conduct Unbecoming an Officer;
- Department Manual Section 1/270.20, Endorsement of Products and Services;
- Department Manual Section 3/405, Confidential Nature of Department Records, Reports, and Information;
- Department Manual Section 3/788.40, Internet Usage Guidelines;
- Department Manual Section 3/813.05, Employee's Responsibility;
- Department Manual Section 1/546, Conduct of Undercover Assignment Officers;
- Department Manual Section 1/547, Undercover Assignment Officers Posing as Members of the News Media;
- Department Manual Section 3/788.30, Provisions for the Use of Personal Computers;
- Use of Force Tactics Directive No. 10.1 Undercover Operations, dated March 2013; and,
- Operations Order No. 2, Cyber Support Unit Revised, dated February 28, 2014.