Department Use of Social Media

385.1 PURPOSE AND SCOPE

Best Practice | MODIFIED

This policy provides guidelines to ensure that any use of social media on behalf of the Department is consistent with the Department's mission, vision and values. 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 emerge.

This policy does not address all aspects of social media use. Specifically, it does not address:

- Personal use of social media by department members (see the Employee Speech, Expression and Social Networking Policy number 1060).

- Use of social media in personnel processes (see the Recruitment and Selection Policy number 1000).

- Use of social media as part of a criminal investigation, other than disseminating information to the public on behalf of this department (see the Investigation and Prosecution Policy number 600).

385.1.1 <STRONG>DEFINITIONS</STRONG>

Best Practice | MODIFIED

Definitions related to this policy include:

Social media - Any of a wide array of Internet-based tools and platforms that allow for the sharing of information, such as the department website or social networking services.

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 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), micro-blogging sites (Twitter, Nixle), photo- and video sharing sites (Flickr, YouTube, Snapchat), 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.

385.2 POLICY

Best Practice | MODIFIED

The Indio Police Department may use social media as a method of effectively informing the public about department services, issues, investigations and other relevant events.

Department members shall ensure that the use or access of social media is done in a manner that protects the constitutional rights of all.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.

385.3 AUTHORIZED USERS

Best Practice | MODIFIED

Only members authorized by the Chief of Police or the authorized designee may utilize social media on behalf of the Department. Authorized members shall use only department-approved equipment during the normal course of duties to post and monitor department-related social media, unless they are specifically authorized to do otherwise by their supervisors.

The Chief of Police may develop specific guidelines identifying the type of content that may be posted. Any content that does not strictly conform to the guidelines should be approved by a supervisor prior to posting.

Requests to post information over department social media by members who are not authorized to post should be made through their social media team representative who shall follow the established protocol.

385.4 AUTHORIZED CONTENT

Best Practice | MODIFIED

Only content that is appropriate for public release, that supports the department mission and conforms to all department policies regarding the release of information may be posted.

Examples of appropriate content include:

    (a)   Announcements and event advertisements.

    (b)   Tips and information related to crime prevention.

    (c)   Investigative requests for information.

    (d)   Requests that ask the community to engage in projects that are relevant to the department mission.

    (e)   Real-time safety information that is related to in-progress crimes, geographical warnings or disaster information.

    (f)   Traffic information.

    (g)   Press releases.

    (h)   Recruitment of personnel.

    (i)   Community outreach.

385.4.1   <STRONG>INCIDENT-SPECIFIC USE</STRONG>

`Best Practice` `MODIFIED`

In instances of active incidents where speed, accuracy and frequent updates are paramount (e.g., crime alerts, public safety information, traffic issues), theSocial Media Officer or the authorized designee will be responsible for the compilation of information to be released, subject to the approval of the Incident Commander.

385.5   PROHIBITED CONTENT

`Best Practice` `MODIFIED`

Content that is prohibited from posting includes, but is not limited to:

    (a)   Content that is abusive, discriminatory, inflammatory or sexually explicit.

    (b)   Any information that violates individual rights, including confidentiality and/or privacy rights and those provided under state, federal or local laws.

    (c)   Any information that could compromise an ongoing investigation.

    (d)   Any information that could tend to compromise or damage the mission, function, reputation or professionalism of the Indio Police Department or its members.

    (e)   Any information that could compromise the safety and security of department operations, members of the Department, victims, suspects or the public.

    (f)   Any content posted for personal use.

    (g)   Any content that has not been properly authorized by this policy or a supervisor.

Any member who becomes aware of content on this department's social media site that he/she believes is unauthorized or inappropriate shall promptly report such content to a supervisor. The supervisor will ensure its removal from public view and investigate the cause of the entry.

385.5.1   <STRONG>PUBLIC POSTINGS</STRONG>

`Best Practice` `MODIFIED`

Department social media public postings shall be monitored by the assigned Social Media Officer and the assigned social media team members in order to monitor potential threats against the community or public service employees and to discourage inflammatory language.

DRAFT   Department Use of Social Media - 3

385.5.1(a) ON THE JOB USE OF SOCIAL MEDIA

In addition, Social media content shall adhere to applicable laws, regulations, and policies, including all information technology and records management policies:

- Content is subject to public records laws. Relevant records retention schedules apply to social media content.

- Content must be managed, stored, and retrieved to comply with open records laws and e-discovery laws and policies.

- 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.

- Where possible 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.

- Where possible pages shall clearly indicate that any content posted or submitted for posting is subject to public disclosure.

385.5.2(b) DEPARTMENT-SANCTIONED USE

Department personnel representing the department via social media outlets shall do the following:

- 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.

- Identify themselves as a member of the department.

- 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.

- Not conduct political activities or private business.

385.5.3(c) POTENTIAL USES

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.

- Social media can be used for community outreach and engagement.

- Can provide crime prevention tips.

- Offer online-reporting opportunities.

- Share crime maps and data.

- Solicit tips about unsolved crimes (i.e., Crimestoppers, text-a-tip).

385.5.4(d) SOCIAL MEDIA NOTIFICATIONS & INVESTIGATIONS Social Media Notifications & Investigations

Social media can be used to conduct investigations and make notifications regarding but not limited to;

- Road closures.

- Special events.

- Weather emergencies.

- Missing or endangered persons.

- Recruitment mechanism for volunteers and potential employees.

- This department has an obligation to include Internet-based content when conducting background investigations of job candidates.

- Searches should be conducted by a non-decision maker.

- Information pertaining to protected classes shall be filtered out prior to sharing any information found online with decision makers.

- Persons authorized to search Internet-based content should be deemed as holding a sensitive position.

- Search methods shall not involve techniques that are in violation of existing laws.

- Vetting techniques shall be applied uniformly to all candidates.

- Every effort must be made to validate Internet based information considered during a hiring process

385.6 MONITORING CONTENT

Best Practice   MODIFIED

The Chief of Police will appoint a supervisor to review, at least annually, the use of department social media and report back on, at a minimum, the resources being used, the effectiveness of the content, any unauthorized or inappropriate content and the resolution of any issues.

385.7 RETENTION OF RECORDS

Best Practice   MODIFIED

The Support Services Division Chief should work with the Custodian of Records to establish a method of ensuring that public records generated in the process of social media use are retained in accordance with established records retention schedules. Electronic and paper records are categorized, filed and retained based upon the content of the record. Records where either the content relates in a substantive way to the conduct of the public's business, or are made or retained for the purpose of preserving the informational content for future reference are saved by placing them in an electronic or paper file folder and retained for the applicable retention period. If the item is not mentioned in this policy consult with the City Attorney to determine if a record is considered transitory or preliminary draft. Refer to records retention schedule (city-wide standards record series number CW-026. Content not substantive, or not made or retained for the purpose of preserving the informational content for future reference is described as;

    (a)   Calendars, checklist

    (b)   E-mail

    (c)   Social media postings that does not have a material impact on the conduct of business

    (d)   Invitations

    (e)   Instant messaging

    (f)   Logs

    (g)   Mailing lists

    (h)   Meeting room registrations

    (i)   Supply inventories

    (j)   Telephone messages

    (k)   Transmittal letters

    (l)   Thank yous

    (m)   Request from other cities

    (n)   Undeliverable envelopes

    (o)   Visitors logs

    (p)   Voice mails

    (q)   Webpages

385.8   TRAINING

Best Practice

Authorized members should receive training that, at a minimum, addresses legal issues concerning the appropriate use of social media sites, as well as privacy, civil rights, dissemination and retention of information posted on department sites.