

| | | |
|---|--|------------------|
|  | SAN MARCOS POLICE DEPARTMENT | |
| | Policy 2.8 Use of Social Media | |
| | Effective Date: June 28, 2019 | Replaces: |
| | Approved: _____ <div style="text-align: center;">  Chief of Police </div> | |
| | Reference: | |

I. POLICY

Social media platforms provide a valuable means of assisting the department and its employees in meeting community outreach, problem solving, investigations, crime prevention, and other related objectives. The department supports and utilizes the secure and appropriate use of social media to enhance communication, collaboration, and information exchange.

The department also recognizes the role that these tools play in the personal lives of employees. Because the improper use of social media platforms by employees may impact department operations, the department provides information of a precautionary nature as well as prohibitions on the use of social media by employees.

These policies and procedures apply to all employees including sworn and non-sworn employees, and any volunteers working with the department.

II. PURPOSE

The purpose of this policy is to establish guidance for the management, administration, and oversight of social media. This policy is not meant to address one particular form of social media but social media in general, as advances in technology will occur and new tools will emerge.

III. DEFINITIONS

- A. 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.”
- B. Page: The specific portion of a social media website where content is displayed, and managed by an individual or individuals with administrator rights.
- C. Post: Content an individual shares on a social media site or the act of publishing content on a site.
- D. Profile: Personal information that a user provides on a social networking site.
- E. 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 (Flicker, YouTube), wikis (Wikipedia), blogs, and news sites (Digg, Reddit).
- F. Social Networks: Online platforms where users can create profiles, share information, and socialize with others using a range of technologies.

- G. Speech: Expression or communication of thoughts or opinions in spoken words, in writing, by expressive conduct, symbolism, photographs, videotape, or related forms of communication.
- H. 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.
- I. Wiki: Web page(s) that can be edited collaboratively.

IV. DEPARTMENT SPONSORED SOCIAL MEDIA

- A. Requirements for Department Sponsored Public Social Media Sites
 1. The department's community services division is responsible for the management, posting, and monitoring of the department's public social media network sites. Other members of the department may post and monitor specific social media sites as approved by the chief of police.
 2. The chief of police, with input from departmental members and the city public information officer will determine the extent of the department's official use of social media platforms. No social media platform will be utilized by the department without the express approval of the chief of police.
 3. Each social media page shall include an introductory statement that clearly specifies the purpose and scope of the agency's presence on the website.
 4. Where possible, the page(s) should link to the department's official website.
 5. Social media pages shall clearly indicate that they are maintained by the department and shall have department contact information prominently displayed.
 6. Social media content shall adhere to applicable laws, regulations, and policies, including all information technology and records management policies.
 7. Content is subject to open government laws. Relevant records retention schedules apply to social media content. Content must be managed, stored, and retrieved to comply with open government laws, records retention laws, and e-discovery laws and policies.
 8. Social media pages should state that the opinions expressed by visitors to the page(s) do not reflect the opinions of the department.
 9. Pages shall clearly indicate that posted comments will be monitored and that the department reserves the right to remove any posting.
 10. Pages shall clearly indicate that any content posted or submitted for posting is subject to public disclosure.
- B. Operation of Department Sponsored Public Social Media Sites
Employees approved by the department to post to 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.
 5. Employees 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.
 6. Employees shall observe and abide by all copyright, trademark, and service mark restrictions in posting materials to electronic media.
- C. Uses of Departmental Sponsored Social Media Sites
1. 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.
 2. Social media is a valuable investigative tool and may be used to seek evidence or information about the following:
 - a. Missing persons,
 - b. Wanted persons,
 - c. Gang participation,
 - d. Crimes perpetrated online,
 - e. Photos or videos of a crime posted by a participant or observer.
 3. Social media can be used for community outreach and engagement for the following purposes:
 - a. Providing crime prevention tips,
 - b. Offering online-reporting opportunities,
 - c. Sharing crime maps and data
 - d. Soliciting tips about unsolved crimes (e.g., Crime Stoppers, text-a-tip).
 - e. Social media can be a valuable recruitment mechanism, since many people seeking employment and volunteer positions use the internet to search for opportunities.
- D. Background Investigations
1. This department has an obligation to include internet-based content when conducting background investigations of job candidates.
 2. Search methods shall not involve techniques that are a violation of existing law.
 3. Vetting techniques shall be applied uniformly to all candidates.
 4. Every effort must be made to validate internet-based information that is considered during the hiring process.

E. Use of Covert Social Media Sites for Investigative Operations

1. Covert or undercover social media sites are exempt from the requirements of sections 1, 2, and 3 above.
2. The chief of police, or designee, may approve the use of any covert or undercover social media site or postings to other social media sites for undercover investigative operations. A supervisor will be assigned to monitor the operation of the investigation.

V. **PERSONAL USE OF SOCIAL MEDIA**

A. Precautions and Prohibitions

Barring state law or binding employment contracts to the contrary, employees shall abide by the following rules when using social media:

1. Employees may not access social networking or social media sites through the use of departmentally provided information systems unless authorized to do so on behalf of the department or during the course of an investigation.
2. While on duty, employees may use personal communications devices to access social networking sites, provided such usage does not in any way interfere with the performance of job duties or violate policy.
3. Due to concerns for officer safety and to preserve tactical advantage, the posting of information related to any police response by any officer or an assisting agency is absolutely prohibited without the approval of the chief of police.
4. All matters of, by, within, and about department details regarding calls for service and the customers we interact with are generally considered confidential information that may not be released, blogged about, posted, or otherwise shared outside the department without prior authorization that has been obtained through an official open-records request, or without the information already being in the public realm [already otherwise released officially].
5. Employees 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.
6. As public employees, department personnel are cautioned that speech, whether on or off-duty, made pursuant to their official duties—that is, speech which owes its existence to the employee’s professional duties and responsibilities—may not be protected speech under the First Amendment and may form the basis for discipline if deemed detrimental to the department.
7. Employees should assume that their speech and related activity on social media sites will reflect upon their office and this department. Display of departmental logos, uniforms, uniform patches, or departmental badges on personal social media sites can increase the likelihood of the employee’s free speech being limited.

8. Employees shall not post, transmit, or otherwise disseminate any information to which they have access as a result of their employment without permission from the chief of police.
 - a. For safety and security reasons, employees are cautioned not to disclose their employment with this department nor shall they post information pertaining to any other member of the department without that member's permission. In relation to this, employees are cautioned not to 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 working, or who may reasonably be expected to work, in undercover operations shall not post any form of visual or personal identification.
 - b. Employees are reminded that some individuals that we contact in our profession become angry and on occasion seek revenge for official actions taken. Employees are encouraged not to post any information that could be used to identify any employee's residence, vehicle, or the identity of employees or family members.
9. When using social media, employees should be mindful that their speech becomes part of the worldwide electronic domain. Employees are required to be credible witnesses in criminal prosecutions and that credibility can be attacked using inappropriate posts on social media sites. Therefore, adherence to the department's code of conduct is required in the personal use of social media. In particular, employees 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 employees reflecting behavior that would reasonably be considered reckless or irresponsible.
 - c. Engaging in prohibited speech noted herein may provide grounds for undermining or impeaching an officer's testimony in criminal proceedings. Employees thus sanctioned are subject to discipline up to and including termination of office.
 - d. Employees 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.
 - e. Employees should be aware that they may be subject to civil litigation for the following:
 - i. Publishing or posting false information that harms the reputation of another person, group, or organization (defamation);

- ii. Publishing or posting private facts and personal information about someone without that person's permission that has not been previously revealed to the public, is not of legitimate public concern, and would be offensive to a reasonable person;
 - iii. Using someone else's name, likeness, or other personal attributes without that person's permission for an exploitative purpose;
 - iv. Publishing the creative work of another, trademarks, or certain confidential business information without the permission of the owner.
 - 10. Employees 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. Employees should be aware that privacy settings and social media sites are constantly in flux, and never assume that personal information posed on such sites is protected.
 - 12. Employees are reminded that the department policies and code of conduct apply to on-line activities.
 - 13. There should be no expectation of privacy for items or activities conducted on-line.
- B. Monitoring of Social Media
- 1. Supervisors within the department may make random investigations into the postings of employees for purposes of protecting the integrity and reputation of the department, protecting the integrity of investigations, and ensuring privacy and security of departmental records and information.
 - 2. 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 their supervisor immediately for follow-up action.