TOWN OF SENECA FALLS POLICE DEPARTMENT

GENERAL ORDER

GENERAL ORDER #: 197	**RESCINDS:** 07/01/13, 09/15/14, 03/13/19
SUBJECT: Social Media	**NYS ACCREDITATION:** 28.4, 29.1
EFFECTIVE DATE: 06/26/2019 **BY ORDER OF:** Stuart W. Peenstra, Chief of Police	

I. PURPOSE

To establish the Seneca Falls Police Department's position on the utility and management of social media and provide guidance on its management, administration, and oversight by Department personnel both on-duty in the course of their official duties and off-duty when identified as members of the organization, or otherwise pursuant to their official duties in the public arena.

II. POLICY

It is Seneca Falls Police Department policy that all personnel use computers, computer applications, computer programs, Internet resources, and network/Internet communications in a responsible, professional, ethical, and lawful manner. Department employees are prohibited from posting, transmitting, and/or disseminating any photographs, video or audio recordings, likenesses or images of department logos, emblems, uniforms, badges, patches, marked or unmarked vehicles, equipment, or other material that specifically identifies the Department, on any personal or social networking website or web page, without express written permission of the Chief of Police.

All existing laws, rules, regulations, and directives that govern on- and off-duty conduct are applicable to conduct associated with social media and networking. When engaging in social networking, employees will strictly adhere to any and all existing federal, state, and local laws, policies of the Seneca Falls Police Department, and laws regarding public information on arrests, investigations, and personnel data.

III. DEFINITIONS

Blog: A self-published diary or commentary on a particular topic that may allow visitors to post responses, reactions, or comments.

Blogosphere: Denotes the world of blogs and refers to all the blogs and blog interactions on the internet.

Chat: An interaction on a website, with a number of people adding text items one after another into the same space at nearly the same time – differs from a forum because conversations happen in "real time."

Comments: Responses to a blog post, news article, social media entry, or other social networking post.

Feed: A list of user's recent tweets which can be posted on other sites such as Facebook or an agency's website.

Forums: Discussion areas on websites where people can post messages or comment on existing messages at any time.

Page: The specific portion of a social media website where content is displayed, and managed by an individual or individuals with administrator rights.

Post (noun): Content that an individual shares on a social media or similar site or the act of publishing content on such a site.

Post (verb): The act of creating, uploading, editing, or adding to any social media outlet. This includes text, photographs, audio, video, or any other multimedia file.

Profile: Information that a user provides about himself or herself on a social networking or similar 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, blogs and microblogging sites, photo and video sharing sites, wikis, and news sites that permit user contributed content.

Social Networks: Online platforms where users can create profiles, share information, and socialize with others using a range of technologies, such as Facebook, Twitter, LinkedIn, Usenet Group message or on-line bulletins boards, blogs, wikis, news sites, or other similarly developed formats.

Speech: Expression or communication of thoughts or opinions in spoken words, in writing, by expressive conduct, symbolism, photographs, videotape, or related forms of communication.

Tweet: A post or status update on Twitter of 280 characters or less.

Wall: The users own profile page and the updates it contains. People can write updates on your wall that are viewable by all your friends.

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.

YouTube: An online video community that allows users to upload video content, share that content, and view the videos uploaded by others. Viewers are able to rate videos and leave comments.

IV. PROCEDURE

Where the Seneca Falls Police Department uses social media to advance the purposes and goals of the organization, the following procedures shall apply to these officially-sanctioned uses:

A. General Operating Procedures for Department-Sanctioned Use of Social Media

1. 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.

2. When appropriate, the page(s) should link to the Department's official website.

3. Social media page(s) should be designed for the target audience(s) such as youth or potential police recruits.

4. All Department social media sites or pages shall be approved by the Chief of Police or his or her designee and shall be administered by the Chief of Police.

5. Where possible, social media pages shall clearly indicate 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 may be subject to public records laws. Relevant records retention schedules can apply to social media content.

   The MU-1 Records Retention and Disposition Schedule indicates the minimum length of time that public officials must retain their records before they may be disposed of legally. Relevant sections apply to social media content.

   Content may be subject to applicable Freedom of Information Law (F.O.I.L.) regulations as required by the NYS Public Officers Law 87.

   Content that is specific to a criminal Investigation should be retained in the appropriate case file and is likely discoverable and, as such, should be brought to the prosecutor's attention.

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

8. Content must be managed, stored, and retrieved to comply with public records laws.

9. 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.

10. 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.

11. Pages shall clearly indicate that any content posted or submitted for posting is subject to public disclosure.

B. Conduct during Department-Sanctioned Use of Social Media

When representing the Department via social media outlets:

1. Employees shall 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. Employees shall identify themselves as a member of the Department unless law-enforcement purposes dictate otherwise.

3. Employees shall 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. Employees shall not conduct political activities or private business.

5. The use of Department computers by Department personnel to access social media is prohibited without authorization.

6. 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.

7. Employees shall observe and abide by all copyright, trademark, and service mark restrictions in posting materials to electronic media.

C. Recognized Uses for a Department-Sanctioned Social Media Presence

1. Social media is a valuable investigative tool when seeking evidence or information about:

    - Missing persons
    - Wanted persons
    - Gang participation
    - Crimes perpetrated online (i.e., cyberbullying, cyberstalking)
    - Photos or videos of a crime posted by a participant or observer

    Criminal intelligence gathering

2. Social media can be used for community outreach and engagement by:

    - Providing crime prevention tips
    - Offering online reporting opportunities
    - Sharing crime maps and data
    - Soliciting tips about unsolved crimes

    Customer satisfaction surveys

    Monitoring and responding to community concerns with the Seneca Falls Police Department.

3. Social media can be used to make time-sensitive notifications related to:

    - Road closures
    - Special events
    - Weather emergencies
    - Missing or endangered persons.

D. Use during Employment Screening

1. Persons seeking employment and volunteer positions use the Internet to search for opportunities, and social media can be a valuable recruitment mechanism. This Department has an obligation to include Internet-based content when conducting background investigations of job candidates.

2. 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.

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

4. Search methods shall not involve techniques that are a violation of existing law.

5. Vetting techniques shall be applied uniformly to all candidates.

6. Every effort must be made to validate Internet-based information considered during the hiring process.

E. Personal Use of Social Media

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 speaking on matters of public concern on social media sites to the degree that their interests in engaging in such speech is not outweighed by the Department's interests against impairing the maintenance of discipline by supervisors, impairing working relationships of this Department for which loyalty and confidentiality are important, revelation of agency-sensitive information which may damage investigations or undercover operations, impeding the performance of duties, impairing discipline and harmony among coworkers, interfering with the operation of the Department, undermining the mission of the Department, conflicting with the responsibilities of the personnel, or abusing one's authority or public accountability. The instances must be judged on a case-by-case basis.

2. As public employees, Department personnel are cautioned that speech on- or off-duty, made pursuant to their official duties is not protected speech under the First Amendment and may form the basis for discipline if deemed detrimental to the Department.

3. For safety and security reasons, Department personnel should be cautious where they disclose their employment with this Department. As such, Department personnel are prohibited from the following:

    - Displaying Department logos, uniforms, or similar identifying items on personal web pages.

    - Posting personal photographs, or providing similar means of personal recognition, that may cause them, or another officer, 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.

4. 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.

5. Department personnel may not make any statements, speeches, appearances, endorsements, or publish materials that could reasonably be considered to represent the views or positions of this Department without express authorization.

6. Department personnel should be aware that they may be subject to civil litigation for:

    - Publishing or posting false information that harms the reputation of another person, group, or organization (defamation).

    - 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.

    - Using someone else's name, likeness, or other personal attributes without that person's permission for an exploitative purpose.

    - Publishing the creative work of another, trademarks, or certain confidential business information without the permission of the owner.

7. Employees should be aware that there is no reasonable expectation of privacy when engaging in social networking online. As such, the content of social networking websites may be obtained for use in criminal trials, civil proceedings, and departmental investigations. Such content may have a detrimental impact on criminal investigations or judicial proceedings.

8. 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.

9. 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.

10. 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.

11. Except in the performance of an authorized duty, employees may not use Department computers to access social networking sites, blogs, bulletin boards, or similar media.

12. Except in the performance of an authorized duty, employees may not utilize personal computers, cell phones, or other devices to access social networking sites, blogs, bulletin boards, or similar media while on duty.

13. Employees having personal web pages or other types of internet postings which can be accessed by the public, shall not place, or allow to be placed, photographs or depictions of themselves dressed in uniform and/or displaying official identification, patches or badges, or in any way, either directly or indirectly, identify themselves as an employee of the department for any reason, without approval as indicated in this policy.

14. Employees having personal web pages shall not use their rank, title, or position in a manner that would suggest that they are representing the interests or official position of the police department.

15. Photographs of the inside of the police building as well as any crime or accident scene shall not be posted without consent of the Chief of Police.

16. When engaging in the personal use of social media, employees shall not post any photograph, audio, video, illustration, or any other multimedia file related to or depicting any of the following:

    - Brandishing any Department-owned weaponry, actual or simulated, or any contraband whether actual or simulated.

    - Brandishing any Department-owned tactical instrument, including, but not limited to: firearms, ASP, baton, OC spray, electrical control weapon, and/or mechanical restraints.

F. **Undercover Profiles**

1. Nothing in this policy will prohibit the use of a fictitious name, identity, business or organization strictly for official investigative purposes with prior authorization by the Chief of Police. In all such cases members will (secure an Incident Report Number containing all relevant information on the identity used and members responsible for such investigation.

2. Undercover profiles should not be accessed from personal computers, laptops, devices or Department PC, laptops or devices that utilize a Department or government IP address (the purpose of this section is an officer safety issue to reduce the risk of suspects identifying the actual identity of officers working in an undercover roll).

G. **Approval Process**

1. An employee seeking approval to use references to the Seneca Falls Police Department on a personal website, web page, or other public forum shall submit a request for approval to the Chief of Police via the chain of command.

2. Employees who post photos, comments, or other material pertaining to other department employees must inform and seek approval from the employee(s) before posting same.

The Seneca Falls Police Department reserves the right to access, audit and disclose, for whatever reason, all content, messages, photographs, videos, and any other information created, transmitted or received via the use of any equipment issued or maintained by the Department. This includes, but is not limited to, records of all key strokes or web-browsing history made at any department computer or over any department network.