

Geneva Police Department GENERAL ORDERS		SOCIAL MEDIA			
<input checked="" type="checkbox"/> new: <input type="checkbox"/> rescinds: Policy & Procedure <input type="checkbox"/> amends:		cross-reference			
		Accreditation/Recognition standards: C.A.L.E.A.: NYS L.E.A.P.:			
effective date: 9.22.14	issue/amend date: 9.22.14 / 12.20.17 / 11.19.19				
I. PURPOSE	The purpose of this General Order is to establish and describe policies and procedures to ensure 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	It is the policy of the Geneva Police Department to ensure 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	<ul style="list-style-type: none"> 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 - Information that a user provides about themselves on a social networking site. E. Record - Any information kept, held, filed, produced or reproduced by, with or for an agency or the state legislature, in any physical form whatsoever including, but not limited to, reports, statements, examinations, memoranda, opinions, folders, files, books, manuals, pamphlets, forms, papers, designs, drawings, maps, photos, letters, microfilms, computer tapes or discs, rules, regulations or codes (§86 (4) NYS Public Officers Law). F. 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), micro-blogging sites (Twitter, Nixle), photo and video-sharing sites (Flickr, YouTube), wikis (Wikipedia), blogs, and news sites (Digg edit). G. Social Networks - Online platforms where users can create profiles, share information, and socialize with others using a range of technologies. H. Speech - Expression or communication of thoughts or opinions in spoken words, in writing, by expressive conduct, symbolism, photographs, videotape, or related forms of communication. 				

III. DEFINITIONS (CONT.)	<p>I. <u>The second generation of the World Wide Web</u> - Focused on shareable, user-generated content, rather than static web pages. Some use this term interchangeably with social media.</p> <p>J. <u>Wiki</u> - Web page(s) that can be edited collaboratively.</p>
IV. PROCEDURE	<p>A. <u>Department Sanctioned Presence – Official Use</u></p> <ol style="list-style-type: none"> 1. <u>Determine Strategy</u> <ol style="list-style-type: none"> 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 content will be designed with the specific target audience in mind. 2. <u>Content Procedures</u> <ol style="list-style-type: none"> a. All Department social media sites or pages must be approved by the Chief of Police or his/her designee and will be administered, including regular monitoring, by the Chief of Police or his/her designee. b. Content originators are responsible for ensuring accuracy of their content. c. Where possible, social media pages shall clearly indicate that they are maintained by the Department and will have Department contact information displayed prominently. d. Social media content shall adhere to applicable laws, regulations and policies, including all information technology and records management policies. <ol style="list-style-type: none"> i. Content is subject to public records laws. 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. ii. Content may be subject to applicable Freedom of Information Law (FOIL) regulations as required by the NYS Public Officers Law §87. iii. 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. iv. Content must be managed, stored, and retrieved in compliance with open records laws, e-discovery laws and policies. e. Social media pages should state that opinions expressed by visitors to the page do not reflect the opinions of the Department. <ol style="list-style-type: none"> i. Pages will clearly indicate that posted comments will be monitored and that the Department reserves the right to remove obscenities, off-topic comments, and personal attacks. ii. Pages shall clearly indicate that any content posted or submitted for posting is subject to public disclosure. 3. <u>Posting Procedures</u> <ol style="list-style-type: none"> a. Personnel representing the Department will: <ol style="list-style-type: none"> i. Comply with all Departmental standards of conduct, conventionally accepted protocols and proper decorum. ii. Identify themselves as a member of the Department. iii. Not make comments or statements regarding their opinion of the guilt or innocence of any suspect, arrestee or defendant.

IV. PROCEDURE (CONT.)	<ul style="list-style-type: none"> iv. Not post, transmit, or otherwise disseminate confidential information, including photographs or videos of Departmental training activities, other Departmental activities, or work related assignments without express permission from Chief of Police. v. Not conduct political activities or private business. <ul style="list-style-type: none"> a) The use of Department computers by Department personnel to access social media is prohibited without authorization. b) The use of personally owned devices to manage the Department's social media is prohibited without express permission from the Chief of Police. c) Personnel shall observe and abide by all copyright, trademark and service mark restrictions when posting materials to social media. <p>4. <u>Undercover Profiles</u></p> <ul style="list-style-type: none"> a. 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 and LT/DB. In all such cases members will generate a CR# in PD Manager and complete an <i>Authorization Form</i> (<i>Attachment A</i>) containing all relevant information on the identity used and members responsible for such investigation. b. Undercover profiles should not be accessed from personal computers, laptops, or other devices. <p>5. <u>Potential Official Uses</u></p> <ul style="list-style-type: none"> a. Investigative tool: <ul style="list-style-type: none"> i. Missing persons ii. Wanted persons iii. Gang participation iv. Online crime (cyber-bullying, cyber-stalking, etc.) v. Source of photo or video evidence posted by observer or participant vi. Criminal intelligence gathering vii. Creation or corroboration of an undercover or fictitious identity for official use and when expressly authorized by the Department. b. Community Outreach and Engagement: <ul style="list-style-type: none"> i. Crime prevention tips ii. Online reporting opportunities iii. Data sharing (crime maps, statistics, etc.) iv. Soliciting crime information and tips v. Customer satisfaction surveys vi. Employee recognition vii. Monitoring and responding to community concerns with the Department viii. Time sensitive notifications: <ul style="list-style-type: none"> a) Road closures b) Special events c) Weather emergencies d) Missing or endangered persons c. Agency Employee Recruitment: <ul style="list-style-type: none"> i. Employment opportunities ii. Hiring process preparation aids
---------------------------------	--

IV. PROCEDURE (CONT.)	<p>d. Applicant background investigation:</p> <ul style="list-style-type: none"> i. Pre-employment investigations may include internet-based content related to the potential employee. ii. Searches should be conducted by personnel who do not otherwise influence hiring decisions. Any reference to a candidate's protected class status should be filtered from the search results prior to their submission to personnel making hiring decisions. iii. Those authorized to conduct online background searches should be deemed to hold a sensitive position. iv. Searches will be conducted in accordance with applicable laws. v. Uniform vetting techniques will be applied to all candidates, making every effort to validate internet based information considered during the hiring process. <p>B. Personal Use</p> <p>1. <u>Precautions and Prohibitions</u> - Absent State Law or binding labor agreements to the contrary, Department personnel shall abide by the following when using social media:</p> <ul style="list-style-type: none"> a. Department personnel are free to express themselves as private citizens on social media sites to the degree that their speech does not impair the working relationships of this Department for which trust and confidentiality are important, impede the performance of duties, impair discipline and harmony among coworkers, or negatively affect the public perception of the Department. b. Leader and Subordinate Relationships: Because of the nature of social media, formal leaders may interact and function in the same social media spaces as their subordinates. It is suggested that the online relationship function in the same manner as the professional relationship. c. 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 would reflect upon their office and this Department. Speech and conduct should be representative of Departmental values. d. Department personnel are prohibited from creating a fictitious identity under the auspices of conducting duty related activities without express authorization from the Chief of Police. Such activities would be governed by the official Department use provisions of this policy. e. Department personnel shall not post, transmit, or otherwise disseminate any information or imagery, such as arrest photos, accident scene photos, crime scene photos, official or unofficial reports, or information gained in their official capacity to which they have access as a result of their employment without written permission from the Chief of Police or his/her designee.
---------------------------------	--

IV. PROCEDURE (CONT.)	<p>f. 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 his/her permission.</p> <p>i. As such, Department personnel are cautioned not to:</p> <ul style="list-style-type: none"> a) Display Departmental 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. <p>ii. Members should be alert to the content and nature of their postings including online conversations and those of family and friends. When certain strings of information are compiled, persons viewing such information may be able to identify shift schedules, location of your residence, when the residence is unoccupied, family members, vacations and other private information.</p> <p>g. 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:</p> <ul style="list-style-type: none"> i. Speech containing obscene or sexually explicit language, images, acts, 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. ii. Speech involving themselves, or other Department personnel, reflecting behavior that might reasonably be considered reckless or irresponsible. <p>h. 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.</p> <p>i. Personnel may not divulge information gained by reason of their authority without express authorization from Chief of Police or his/her designee. This includes, but is not limited to:</p> <ul style="list-style-type: none"> i. Any statements, speeches, appearances or endorsements; ii. Publishing materials that could reasonably be considered to represent the views or positions of this Department. <p>2. <u>Department personnel should be aware that they may be subject to civil litigation for:</u></p> <ul style="list-style-type: none"> 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;
---------------------------------	--

IV. PROCEDURE (CONT.)	<p>c. Using someone else's name, likeness, or other personal attributes without that person's permission for an exploitative purpose; or</p> <p>d. Publishing the creative work of another, including trademarks, or certain confidential business information without the permission of the owner.</p> <p>e. Department personnel should be aware that privacy settings and social media sites are constantly changing and they should never assume that personal information posted on such sites is protected.</p> <p>f. Department personnel should expect that the Department, at any time and without prior notice, might access any information created, transmitted, downloaded, exchanged or discussed in a public online forum.</p> <p>3. Reporting Violations: Any employee becoming aware of or having knowledge of a posting or of any website or web page in violation of the provisions of this policy shall immediately notify their supervisor.</p>
V. LEGAL ISSUES	<p>A. The use of social media has presented personnel conduct challenges for law enforcement executives that have resulted in employee discipline and terminations. There are many examples of employee misconduct across the United States. These cases highlight the issues associated with such misconduct.</p> <p>1. Garcetti V. Ceballos, 126 S. Ct. 1951 (2006) A deputy district attorney filed a §1983 complaint against county and supervisors at district attorneys' office, alleging that he was subject to adverse employment actions in retaliation for engaging in protected speech, that is, for writing a disposition memorandum in which he recommended dismissal of a case on the basis of purported government misconduct. The Court held that: (a) when public employees make statements pursuant to their official duties, they are not speaking as citizens for the First Amendment purposes, and the Constitution does not insulate their communications from employer discipline; and (b) here, district attorney did not speak as a citizen when he wrote his memo and, thus, his speech was not protected by the First Amendment.</p> <p>2. City of San Diego v. Roe, 125 S. Ct. 521 (2004) Police officer (Roe) who was discharged for offering home-made, sexually explicit videos (in a police uniform) for sale on online auction site sued police department, city, and his supervisors under 1983, alleging that his off-duty, non-work-related activities could not be grounds for terminating his employment. The uniform apparently was not the specific uniform worn by the San Diego police, but it was clearly identifiable as a police uniform. Roe also sold custom videos, as well as police equipment, including official uniforms of the San Diego Police Department, and various other items such as men's underwear. Roe's eBay user profile identified him as employed in the field of law enforcement. The Court held that officer's speech did not touch on a "matter of public concern" (that is, subject of legitimate news interest or general interest, and of value and concern to public activities); and officer's activities, though outside the workplace and purportedly about subjects not related to his employment, had injurious effect on mission of his employer. Therefore were not entitled to First Amendment protection.</p>

**V. LEGAL ISSUES
(CONT.)**

3. **Brady v. Maryland, 83 S. Ct. 1194 (1963); Giglio v. United States, 92 S. Ct. 763 (1972).** Prosecutor must disclose evidence or information that would prove the innocence of the defendant or would enable the defense to more effectively impeach the credibility of government witnesses. This disclosure requirement may apply to social media communications made by police officers.

Approved By

MICHAEL J. PASSALACQUA
CHIEF OF POLICE