

## City of Johns Creek Police Department

<i>Subject:</i> Social Media Policy		<i>Number:</i> 01-22
<i>Reference:</i> See Also Social Media Posting/Monitoring Guidelines		<i>Amends:</i>
<i>Effective:</i> 10/11	<i>Review Date:</i> Annually	<i># of</i> 5
<i>Revision:</i> 02/15		<i>Pages:</i>

**PURPOSE:** 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.

### **POLICY: (01-22)**

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.

### **DEFINITIONS:**

**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, MySpace), microblogging sites (Twitter, Nixle), photo- and video-sharing sites (Flickr, YouTube, Pinterest), 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.

**Social Media Team:** Members of the department approved by the Chief of Police to post on approved department social media sites.

## **PROCEDURES:**

### **On-The-Job-Use (01-22-01)**

#### **A. Department-Sanctioned Presence**

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. Where possible, the page(s) shall link to the department's official website.
3. Social media page(s) shall be designed for the target audience(s) such as youth or potential police recruits.

#### **B. Procedures**

1. 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 Community Services Unit, Social Media Team or Public Information personnel or as otherwise determined.
2. Where possible, social media pages shall clearly indicate they are maintained by the department and shall have department contact information prominently displayed.
3. Social media content shall adhere to applicable laws, regulations, and policies, including all information technology and records management policies.
4. Content is subject to public records laws. Relevant records retention schedules apply to social media content.
5. Content must be managed, stored, and retrieved to comply with open records laws.
6. Where possible, social media pages shall state that the opinions expressed by visitors to the page(s) do not reflect the opinions of the department.
7. 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.

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

### **C Department-Sanctioned Use**

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

- a. Conduct themselves at all times as representatives of the department;
- b. Shall adhere to all department standards of conduct and observe conventionally accepted protocols and proper decorum;
- c. Identify themselves as a member of the department;
- d. 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 from the Chief of Police;
- e. Not conduct political activities or private business;
- f. 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 from the Chief of Police; and
- h. Employees shall observe and abide by all copyright, trademark, and service mark restrictions in posting materials to electronic media.
- g. Follow approved social media posting and monitoring guidelines.

### **D. Potential Uses**

The social media team and members of the department shall follow the approved social media posting and monitoring guidelines.

In addition the following shall be considered when using social media sites:

1. 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., cyber bullying, cyber stalking); and
  - e. posting photos or videos of a crime posted by a participant or observer.
2. Social media can be used for community outreach and engagement by
  - a. providing crime prevention tips;
  - b. offering online-reporting opportunities;
  - c. sharing crime maps and data; and
  - d. soliciting tips about unsolved crimes (i.e., Crimestoppers, text-a-tip).
4. 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.
5. Persons seeking employment and volunteer positions use the Internet to search for opportunities, and social media can be a valuable recruitment mechanism.
  6. The department has an obligation to include Internet-based content when conducting background investigations of candidates.
  7. Searches shall be conducted by a non-decision maker or hiring authority. Information pertaining to protected classes shall be filtered out prior to sharing any information found online with decision makers.
  8. Persons authorized to search Internet-based content shall be deemed as holding a sensitive position.
  9. Search methods shall not involve techniques that are a violation of existing law or policy.
  10. Vetting techniques shall be applied uniformly to all candidates.
  11. Every effort must be made to validate Internet-based information considered during the hiring process.

### **Personal use (01-22-02)**

A. Precautions and Prohibitions - department personnel shall abide by the following when using social media.

1. Department personnel 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.
2. 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 shall assume that their speech and related activity on social media sites will reflect upon their office and this department.
3. Department personnel shall not post, transmit, or otherwise disseminate any information to which they have access as a result of their employment without written permission from the Chief of Police or his or her designee.
4. 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 their permission. As such, department personnel are cautioned **not** to do the following:
  - a. Display department logos, uniforms, or similar identifying items on personal web pages, without prior approval of the Chief of Police.
  - b. Officers who are, or who may reasonably be expected to work in undercover operations, shall not post any form of visual or personal identification.

- c. Post any videos, pictures or any other media related to their job using their personal electronic devices without the prior approval of the Chief of Police, or his/her designee.
5. When using social media, department personnel shall 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:
  - 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 or department personnel.
  - b. Speech involving themselves or other department personnel reflecting behavior that would reasonably be considered reckless or irresponsible.
6. 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.
7. Department personnel 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 of the Chief of Police.
8. Department personnel shall be aware that they may be subject to civil litigation for
  - 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;
  - c. using someone else's name, likeness, or other personal attributes without that person's permission for an exploitative purpose; or
  - d. publishing the creative work of another, trademarks, or certain confidential business information without the permission of the owner.
9. Department personnel shall be aware that privacy settings and social media sites are constantly in flux, and they shall never assume that personal information posted on such sites is protected.
10. Department personnel shall 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. Reporting violations—any employee becoming aware of or having knowledge of an employee's 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.