USE OF SOCIAL NETWORKING WEBSITES

Directive 3 - 108

Date Issued: April 2016 Amends/Cancels: 3-108 July 2013

I. PURPOSE

The purpose of this Directive is to provide guidance to employees of the Department of General Services Maryland Capitol Police (MCP) on their use of social networking websites. As such, this Directive provides information of a precautionary nature as well as prohibitions on the use of social networking websites.

II. POLICY

MCP allows employees to use social media while off-duty while ensuring that employees maintain a level of professionalism and do not engage in conduct that contradicts or impedes the MCP mission.

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. CONFIDENTIAL INFORMATION: Digital photographs, video, audio, or other digital media depicting the Department or its employees, content from criminal or administrative investigations, security procedures, internal videos, daily work activity, or any other information that could be considered sensitive to law enforcement or information that could potentially expose the Department to liability.

C. PERSONAL INFORMATION: Any type of identifying information including but not limited to ; social security numbers, dates of birth, addresses, phone numbers, e-mail addresses, driver's license or state identification numbers**.**

D. POST OR POSTING: Placing text or digital information publicly on the internet**.**

E. SOCIAL MEDIA: Internet-based resources that integrate user-generated content and user participation, including social networking sites (Facebook, MySpace), microblogging sites (Twitter, Nixle), photo- and video-sharing sites (Flickr, YouTube), wikis (Wikipedia), blogs and news sites, etc.

F. SOCIAL NETWORKING WEBSITES: For the purpose of this policy, social networking websites means computer network sites which focus on building online communities of people who share interests and activities and/or exploring the interest and activities of others. Examples of social networking websites include: Facebook, MySpace, Friendster, Linked In, Twitter, and sites that allow

users to post personal blogs. The absence of, or lack of explicit reference to, a specific site does not limit the extent of the application of this Policy as advances in technology will occur and new tools will emerge.

III. BACKGROUND

A. MCP employees have the right to use social media when off-duty; however MCP employees are public servants who are held to higher ethical standard than the general public.

B. The MCP has a duty to protect the reputation of the organization and its employees and guard against potential legal liability.

C. MCP reserves the right to monitor all social media.

D. The content of social media can be subpoenaed and used in criminal and civil trials to impeach the employee's testimony or to undermine the employee's character or reputation.

E. Any reference to employment with the MCP while using social media could compromise the safety of the employee or their family.

F. All electronic communications created, received or stored on the MCP computer system or network are the sole property of the MCP and/or State of Maryland and not the author, recipient or user.

IV. PROCEDURES

A. ON-DUTY USE

1. Employees are prohibited from accessing social networking websites while on-duty, unless the employee is conducting a criminal or administrative investigation that has been approved by a supervisor.

2. Employees representing the MCP via social media outlets will:

    a. identify themselves as a member of the MCP;

    b. conduct themselves at all times as representatives of the MCP and will adhere to all standards of conduct and observe accepted protocols and proper decorum; and

    c. observe and abide by all copyright, trademark and service mark restrictions when posting materials.

3. Social media content will adhere to applicable laws, regulations and policies, including all DoIT and records management policies.

    a. Content is subject to public records laws and applicable records retention schedules apply to social media content.

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

4. Employees may not conduct political activities or private business via social media while on-duty.

B. SOCIAL MEDIA USE IN GENERAL

1. While engaging in social media activities, employees may not:
   a. make statements, including personal opinions, about the guilt or innocence of any suspect or arrestee, or comment on open investigations or pending prosecutions;
   b. post photographs, images, video or any other documents or information created or received by the MCP or any other law enforcement agency related to any investigation or any other law enforcement business.
   c. post any photograph that could be used to identify anyone as being a covert law enforcement officer of any agency;
   d. post, transmit or otherwise disseminate confidential information, including photographs or videos, related to MCP training, activities or assignments without written permission from the Chief of Police;

2. Employees are prohibited from posting messages that criticize or ridicule DGS, MCP, or any other State agency.

3. Employees shall not represent that they are speaking or acting on behalf of the Department, or that they are representing or presenting the interests of the Department without the express permission of the Chief of Police.

4. Employees are prohibited from posting, transmitting, or disseminating likeness or images of Department logos, emblems, uniforms and other material that specifically identifies the Department or oneself as an employee of the department on any personal electronic communication, social networking websites, web pages and other electronically transmitted material in a manner that would be derogatory, disparaging, defaming or in any way bring the Department into an unfavorable light.

5. Employees are prohibited from posting, or disseminating any sexual, violent, racial or ethnically derogatory material, comments, pictures, artwork, video or other references on their websites or through any other means of communication on the Internet in such a way as to bring the Department into an unfavorable light.

6. Employees should be aware that they may be subject to civil litigation or criminal penalties 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 the 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.

7. Employees should exercise good judgment when networking online. This includes but is not limited to refraining from:

   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; and

   b. refraining from posting content involving themselves or other Department personnel reflecting behavior that would reasonably be considered reckless or irresponsible.

8. Employees should be aware that they may be subject to civil litigation or criminal penalties 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 the 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. Any employee becoming aware of or having knowledge of a posting or of any website, web page or e-mail in violation of the provision of this Policy shall notify his or her supervisor immediately.