MIDDLETON POLICE DEPARTMENT	DATE **April 5, 2011**	POLICY **1.2.07**
SUBJECT: **Social Media Policy**	REVIEWED November 22, 2017	

Refer to: City Policy – Electronic Communication & Information Systems
History: 2011, Updated 11/15; 11/2017
WILEAG (5th Ed.) Standards: None

Contents

Purpose 1
Policy 1
Definitions 1
On-The-Job Use 2
Personal Use 4

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

Social media provides a potentially valuable means of assisting the Department and its personnel in meeting community outreach, problem-solving, investigative, crime prevention and related objectives. 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

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. ***Covert or Undercover***: Investigative activity involving the use of an assumed name or cover identity.

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

D. ***Post***: Content an individual shares on a social media site or the act of publishing content on a site.

E. ***Profile:*** Information that a user provides about himself or herself on a social networking site.

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), microblogging sites (Twitter, Nixle), photo and video sharing sites (Flickr, YouTube), wikis (Wikipedia), blogs and news sites (Digg, Reddit).

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.

I. ***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.

J. ***Wiki***: Web page(s) that can be edited collaboratively.

On-The-Job Use

A. Department Sanctioned Presence
    1. Determine strategy
        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 page(s) shall be designed for the target audience(s) such as youth or potential police recruits.
    2. Procedures
        a. All Department social media sites or pages shall be approved by the chief executive or his or her designee and shall be administered by Administration Services or as otherwise determined.
        b. Where possible, social media pages shall clearly indicate they are maintained by the Department and shall have Department contact information prominently displayed.
        c. Social media content shall adhere to applicable laws, regulations and policies, including all information technology and records management policies.

1) Content is subject to public records laws.
2) Content must be managed, stored and retrieved to comply with open records laws.

d. 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.
    1) Pages shall clearly indicate that posted comments will be monitored and that the Department reserves the right to remove obscenities, off-topic comments, personal attacks and political and private business promotions.
    2) Pages shall clearly indicate that any content posted or submitted for posting is subject to public disclosure.

3. Department Sanctioned Use
    a. Department personnel representing the Department via 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 permission.
        4) Not conduct political activities or private business.
    b. Accessing social media by use of Department equipment, or during work hours, is restricted consistent with the Personal Use section of the City's Electronic Communication & Information Systems Policy.
    c. 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 permission.
    d. Employees shall observe and abide by all copyright, trademark and service mark restrictions in posting materials to electronic media.

B. Covert Investigations

The Department may engage in covert Internet and social networking investigations that are appropriate to carry out its law enforcement responsibilities, including the conduct of preliminary inquiries, general crime investigations, and intelligence investigations. The investigation should be well planned, deliberate and performed in compliance with all applicable policies. The actions of undercover officers on the Internet should always be appropriate, under the circumstances, and easily justified to prosecutors, judges and juries. Officers and supervisors conducting covert Internet and social networking investigations will conduct such investigations under the following guidelines:

1. Officers will obtain the approval of the Investigative Services Commander prior to the initiation of an undercover investigation involving social networking sites.
2. Social Networking investigations have no different requirements when it comes to documenting the investigations. The techniques applied on the Internet still require the information be properly collected, properly preserved and properly presented in a report.
3. When possible, officers will utilize investigative computer systems and software intended to record data from the Internet and audio and/or video recording in an evidentiary manner when contacting suspects.
4. Officers will not knowingly transfer or make available for download any files that contain any malicious code or other type of file that would disrupt, delay, or destroy another person's computer system.
5. The officer, or his/her supervisor, should notify the appropriate law enforcement agencies within the area of operation, if identified through the investigation, to ensure appropriate de-confliction has been conducted.
6. Entrapment must be scrupulously avoided. Entrapment occurs when the Government implants in the mind of a person who is not otherwise disposed to commit the offense the disposition to commit the offense and then induces the commission of that offense in order to prosecute.
7. Except as authorized, no undercover employee on the Internet shall engage in any activity that would constitute a violation of Federal, state, or local law if engaged in by a private person acting without authorization.
8. The Investigative Services Commander will only approve investigations that have a legitimate purpose and are reasonable to undertake; assure the investigator is properly prepared for the assignment; determine operational procedures, guidelines and plans; authorize undercover identities; supervise the operation; and review and approve all investigative reports and material, which are prepared and submitted by the investigating officer.

Personal Use

A. Precautions and Prohibitions

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 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 should 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 permission from the chief executive 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.
    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.
5. 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:
    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 Department personnel reflecting behavior that would reasonable 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, appearance, and endorsements; or publish materials that could reasonably be considered to represent the views or positions of this Department without express authorization.
8. Department personnel should 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 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.
10. 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.
11. 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.