PLANNING AND DEPLOYMENT

TRANSMITTAL OF WRITTEN DIRECTIVE

FOR SIGNATURE OF: James E. Craig, Chief of Police

TYPE OF DIRECTIVE: Manual Directive 102.8

SUBJECT: **DEPARTMENT INTERNET USAGE/WEB PAGES/SOCIAL NETWORKING**

ORIGINATED OR REQUESTED BY: Planning and Deployment

APPROVALS OR COMMENTS:
The above referenced was reviewed by Crime Intelligence. Revisions are marked in strikethroughs, bold, and italics.

The recommended changes reflected in this policy are as follows:

1. 102.8 – 3 - Definitions – Several definitions were added in reference to the addition of social media accounts used in law enforcement.
2. 102.8 – 10 – Social Media use and Law Enforcement Investigations – This section was added as an update to social media use.

APPROVED
FEB 26 2019
ASSISTANT CHIEF
OFFICE OF THE CHIEF

RECEIVED
MAR 07 2019
BOARD OF POLICE COMMISSIONERS

APPROVED
FEB 19 2019
ASSISTANT CHIEF
ADMINISTRATIVE OPERATIONS

APPROVED
JAN 10 2018
SECOND DEPUTY CHIEF
POLICE LEGAL ADVISOR

Approved
1/14/19

AFTER THE DIRECTIVE IS APPROVED AND SIGNED, PLEASE RETURN TO PLANNING AND DEPLOYMENT.
1301 Third Avenue, 7th Floor, Detroit MI 48226

4345

Series	Effective Date	Review Date	Directive Number
100 Administration		Three Years	102.8
Chapter 102 – Standard of Conduct			
Reviewing Office *Crime Intelligence*			☐ New Directive ☒ Revised Revisions in *italics*
References *Michigan State Police Social Media Policy*			

DEPARTMENT INTERNET USAGE/WEB PAGES/SOCIAL NETWORKING

102.8 - 1 PURPOSE

This directive establishes written guidelines to ensure that, when utilizing personal web pages and Internet and social network sites, members use appropriate discretion when referencing the Detroit Police Department as not to discredit or disrespect the Department. In addition, these guidelines will ensure that the release, either directly or indirectly, of information concerning crimes, accidents, or violations of ordinances/statutes to persons outside the Department is not disseminated, and that all members treat the official business of the Department as confidential. Further, this directive addresses the appropriateness while using social media for personal use.

102.8 - 2 POLICY

Social media provides a potentially valuable means of assisting the Department and its members in meeting community outreach, problem solving, investigative, crime prevention, and other 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 members. The personal use of social media can have bearing on Department members 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 members.

102.8 - 3 Definitions

102.8 - 3.1 *Criminal Intelligence Information*

Data which meets criminal intelligence collection criteria and which has been evaluated and determined to be relevant to the identification of criminal activity engaged in by individuals who or organizations which are reasonably suspected of involvement in criminal activity.

102.8 - 3.2 *Criminal Justice Information (CJI)*
Criminal Justice Information (CJI) is any data (electronic or hard copy) collected by criminal justice agencies that is needed for the performance of their functions as authorized or required by law.

102.8 - 3.3 *Criminal Justice Information Systems*
Criminal Justice Information Systems (CJIS) means systems provided by a governmental agency or authorized private entity that store and/or disseminate information used for the administration of criminal justice and public safety.

102.8 - 3.4 *Criminal Nexus, Criminal Predicate*
Established when behavior or circumstances are related to an individual or organization's involvement or planned involvement in criminal activity or enterprise.

102.8 - 3.5 Internet
An international computer network providing e-mail and information from computers in educational institutions, government agencies, and industry accessible to the general public via modem links.

102.8 - 3.6 *Online Alias*
An online identity encompassing identifiers, such as name and date of birth, differing the member's actual identifiers, that uses a nongovernmental Internet Protocol address. Online alias may be used to monitor activity on social media websites or to engage in authorized online undercover activity.

102.8 - 3.7 *Online Undercover Activity*
The utilization of an online alias to engage in interactions with a person via social media sites that may or may not be in the public domain (i.e. "friending a person on Facebook").

102.8 - 3.8 *Public Domain*
Any Internet resource that is open and available to anyone.

102.8 - 3.9 *Social Media*
A category of Internet-based resources that integrate user-generated content and user participation. This includes, but is not limited to, social media networking sites (Facebook), micro blogging sites (Twitter) photo- and video-sharing sites (Flickr, YouTube), wikis (Wikipedia), blogs, and new sites (Digg, Reddit).

102.8 - 3.10 *Social Media Monitoring*
Online viewing of information posted or otherwise made available on a social media or information website wherein the Department member DOES NOT interact with any individuals and merely reads or copies content for analysis or data/information collection.

102.8 - 3.11 *Social Media Monitoring Tool*
A tool used to capture data and monitor social media sites by utilizing automated tools such as web crawlers and word search functions to make predictive analysis, develop trends, or collect information. Examples include Netbase, Twitterfall, Trackur, Tweetdeck, Socialmention, Socialpointer, and Plancast.

102.8 - 3.12 *Social Media Websites*
Sites which focus on building online communities of people who share interests and activities and/or exploring the interests and activities of others. Social media websites are further categorized by Internet-based resources that integrate user-generated content and user anticipation. This includes, but is not limited to, social networking sites (Facebook), micro blogging sites (Twitter, Nixle), photo- and video-sharing sites (Flickr, YouTube), wikis (Wikipedia), blogs, and news sites (Digg, Reddit). The absence of an explicit reference to a specific social media website does not limit the application of this policy.

102.8 - 3.13 Social Network
Online platforms where users can create profiles, share information, and socialize with others using a range of technologies.

102.8 - 3.14 *Valid Law Enforcement Purpose*
A purpose for information/intelligence gathering development, or collection, use, retention, or sharing that furthers the authorized functions and activities of a law enforcement agency, which may include the prevention of a crime, ensuring the safety of the public, furthering officer safety, and homeland and national security, while adhering to law and agency policy designed to protect the privacy, civil rights, and civil liberties of Americans.

102.8 - 3.15 Web Page
The specific portion of a social media website where content is displayed and managed by an individual or individuals with administrator rights.

102.8 - 4 Introduction

Professionalism, ethics, and integrity are of paramount importance in the law enforcement community. To achieve and maintain the public's highest level of respect, the Department must place reasonable restrictions on the conduct and appearance of all Department members and hold to these standards of conduct whether on or off duty. A member's actions must never bring the Department into disrepute, nor should conduct be detrimental to its efficient operation.

102.8 - 4.1 Potential Use
Social media is a valuable investigative tool when seeking evidence or information about missing persons, wanted persons, gang participation, etc. It can be used for community outreach, time-sensitive notifications, and employment positions, serving as a valuable recruitment mechanism.

102.8 - 5 Guidelines for Department-Sanctioned Use

1. Members representing the Detroit Police Department by social media outlets shall adhere to the following guidelines:

    a. Conduct themselves at all times as representatives of the Department and adhere to all Departmental standards of conduct and observe conventionally accepted protocols;
    b. Identify themselves as members of the Department;
    c. 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 expressed written permission of the Chief of Police;
    d. Not conduct political activity or private business; and
    e. Observe and abide by all copyright, trademark, and service mark restrictions in posting materials to electronic media.

2. The use of Department computers by Department members to access social media is prohibited without authorization by supervision. Member's use of personally owned devices to manage the Department's social media activities is prohibited without prior approval from a supervisor.

102.8 - 6 Guidelines for Personal Use

1. Department members shall abide by the following guidelines when using social media:

    a. Members are free to express themselves as private citizens on social media sites to the extent that their speech *is not detrimental to the Department's efficient operations;* 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; discredit or disrespect the Department or any Department member; or negatively affect the public perception of the Department;
    b. As public employees, Department members are cautioned that while on or off duty, speech made pursuant to their official duties is not protected under the First Amendment and may form the basis for discipline if deemed detrimental to the Department;
    c. Members shall not post, transmit, or otherwise disseminate any information obtained as a result of their employment with the *Detroit* Police Department without written permission from the Chief of Police, or their designee; and
    d. For safety and security reasons, members are cautioned not to disclose their employment with this Department and shall not post information pertaining to the employment of any other member without prior consent by that member. As such,

members are advised to use good judgement when conducting any of the following actions:

- Placing or allowing photographs or depictions of themselves dressed in the Detroit Police Department uniform and/or displaying official identification, patches, or badges, or in any other way, either directly or indirectly, identifying themselves as a member of the Department for any reason; and/or
- Posting photographs or other depictions of Department uniforms, badges, patches, or marked/unmarked vehicles on Internet sites.

2. When using social media, members should be mindful that their speech becomes part of the worldwide electronic domain. Therefore, adherence to the Detroit Police Manual, Directive 102.3, Code of Conduct, is required in the personal use of social media.

102.8 - 7 Required Approval by the Chief of Police

Department members must receive prior approval from the Chief of Police before conducting any of the following actions:

a. Posting photographs or other depictions of Department issued equipment, uniforms, badges, and patches, or marked/unmarked vehicles that may conflict with the Department's Mission Statement or Code of Conduct;
b. Posting photographs of the inside and/or outside of police buildings/facilities;
c. Posting crime or accident scene photos; and/or
d. Posting, transmitting, and/or disseminating any pictures, videos, or personal comments of official Department training, operations, activities, investigations, or other work-related assignments.

102.8 - 8 Approval Process

1. A member seeking approval to use references to the Detroit Police Department on a Departmental/personal social network, Internet posting, or other public forum shall submit a request for approval on an Interoffice Memorandum (DPD568), through channels, to the Chief of Police. The request shall describe the proposed reference and purpose, a list of the reference(s) and any media to be used, and a printed layout of the entire web page, posting, or site.
2. Any changes to a previously approved posting must be resubmitted for re-approval.

102.8 - 9 Limitations on Posting Information

1. No sexual, violent, racial, religious, national origin, age, physical or mental disability, veteran status, ethnically derogatory material, comments, photographs, artwork, video or other reference(s) may be posted along with any Department approved reference.

2. Members should consider the possible adverse consequences of Internet postings such as future employment, cross-examination in criminal cases, and public and/or private embarrassment.
3. Members are reminded to exercise good judgement and demonstrate personal accountability when choosing to participate on social networking sites; and
4. Members shall not post any pictures/videos of any detainee, deceased person(s), complainants, or any persons that are the subject of a police matter or investigation.

102.8 - 10 *Social Media use and Law Enforcement Investigations*

102.8 - 10.1 *General*

1. *Social media accessed on the Internet can be a powerful tool to aid investigation and analysis in public safety interest areas. In the use of the Internet and in particular social media sites, Department members must be careful to use all information appropriately and take care to avoid violating constitutionally protected rights, or using information in a way that violates the requirements of 28 CFR Part 23. Department members may use social media as an information source for the following valid reasons:*

   a. *Situation assessments;*
   b. *Crime analysis;*
   c. *Criminal intelligence development; and*
   d. *Criminal investigations.*

2. *Use of social media by Department members for these valid purposes will be consistent with all applicable laws, regulations, and Department policies.*

102.8 - 10.2 *Restrictions*

1. *Department members will use social media, access social media, use an alias, use social media monitoring tools ONLY for a valid investigative, analytical, or law enforcement purpose.*
2. *Department members will only utilize social media to seek or retain information that:*

   a. *Is based upon a criminal predicate, a threat to public safety, or to assess an event that has the potential to threaten public safety;*
   b. *Is based on a reasonable suspicion that an identifiable individual has committed an identifiable criminal offense or is involved in or is planning criminal conduct or activity that presents a threat to any individual, the community, or the nation, and the information is relevant to the criminal conduct or activity;*
   c. *Is relevant to the following:*

      - *The investigation and prosecution of suspected criminal incidents;*

- *The resulting justice system response;*
- *The enforcement of sanctions, orders, or sentences; and*
- *The prevention of crime.*

d. *Is useful in crime analysis or situational assessment reports for administration of criminal justice and public safety.*

3. *Department members will not utilize social media to seek or retain information about:*

a. *Individuals or organizations based solely on their religious, social, or political opinions or activities;*
b. *An individual's religion, race, ethnicity, citizenship, place of origin, disability, gender, or sexual orientation unless such information is relevant to the individual's criminal conduct or activity, or if required to identify the individual; or*
c. *An individual's age other than to determine if the person is a minor, or to assist in correctly identifying an individual.*

102.8 - 10.3 *Authorization for Accessing and Searching Social Media Websites*

1. *Overt monitoring, searching, and collecting of information in the Public Domain for any legitimate law enforcement purpose requires no supervisory authorization. This includes Social Media sites, new sites, or other widely available information sources.*
2. *Covert collecting or using an online alias to INTERACT with individuals online, to collect information will ONLY be done by swom Department members with the approval from the Deputy Chief of the Detective Bureau.*
3. *Covert monitoring or using an online alias to access information posted to social media sites on an individual's pages or other commonly available media may be done by Department members with the approval of the Deputy Chief of the Detective Bureau. Online aliases will only be used for the following reasons:*

a. *To obtain or retain information that is based on a criminal predicate or imminent threat to public safety:*
b. *Reasonable suspicion exists that an identifiable individual has committed an identifiable criminal offense or is involved in or is planning criminal conduct or activity that presents a threat to any individual, the community, or the nation and the information is relevant to the criminal conduct or activity;*
c. *Is relevant to any of the following:*

- *The investigation and prosecution of suspected criminal incidents;*
- *The resulting justice system response;*
- *The enforcement of sanctions, orders, or sentences; and*
- *The prevention of crime.*

d. *Is useful in crime analysis or situational assessment reports for administration of criminal of criminal justice and public safety.*

102.8 - 10.4 *Establishing Social Media Aliases*

1. *Department members desiring to use an online alias must submit an Inter-Office Memorandum (DPD568) to the Deputy Chief of the Detective Bureau (through channels).*
2. *The Local Agency Security Officer (LASO) will maintain a roster of personnel using aliases and the alias name along with the pertinent information associated with the alias, and the name of each social media site where the alias is employed.*
3. *Department members will report any potential compromise of an online alias by either the public, or a social media provider to the LASO.*

102.8 - 10.5 *Authorization to use Social Media Monitoring and Searching Software*

1. *Department members will use available Department approved software and computers/devices to monitor, search, or collect from social media sites when they are working within the scope of their duties and pursuing a valid law enforcement purpose.*
2. *Department members will only utilize social media monitoring and searching software to seek or retain information that:*

   a. *Is based upon a criminal predicate, a threat to public safety, or to assess an event that has the potential to threaten public safety;*
   b. *Is based on a reasonable suspicion that an identifiable individual has committed an identifiable criminal offense or is involved in or is planning criminal conduct or activity that presents a threat to an individual, the community, or the nation and the information is relevant to the criminal conduct or activity;*
   c. *Is relevant to the following:*

      - *The investigation and prosecution of suspected criminal incidents;*
      - *The resulting justice system response;*
      - *The enforcement of sanction, orders, or sentences; and*
      - *The prevention of crime.*

   d. *Is useful in crime analysis or situational assessment reports for administration of criminal justice and public safety.*

102.8 - 10.6 *Prohibitions*

1. *Department members will not associate with known or suspected criminals electronically or in person, except as a function of their assigned duties. In the event of an unexpected encounter, members are to limit exposure as much as possible with the objective being to maintain personal safety and the fidelity of aliases and investigations.*

2. *Department members will not use Department provided software, applications, or devices to perform investigations, checks, look ups, etc. on any personal business, personal interest, or on any situation where there is not a valid law enforcement purpose.*
3. *Because the Internet is an open media with infinite possibilities to input fraudulent information and create misinformation, members using information developed from social media or social media search applications must use standard investigative approaches to attempt to verify as much of the information gathered from social media as possible.*

102.8 - 10.7 *Documentation and Retention*

1. *Any information that is collected and held for evaluation or assessment purposes where no criminal predicate or threat to public safety is found will be deleted within 90 days of collection.*
2. *For assessments of public events where no criminal predicate or threat to public safety is found, a file may be maintained that will be useful in the event that the event will occur again (annual events). The only information that can be retained will be non-personally identifying information, and information like useful websites, useful search terms, etc.*
3. *Collected information that has a criminal predicate or indicates a threat to public safety will be saved and documented as is the case for any criminal investigation. Information will be passed to the sworn member(s) assigned, and if necessary, disseminated through the appropriate Detroit Police Department Crime Intelligence product.*
4. *Department members will still forward information that is found to not have a criminal predicate but qualifies as suspicious activity to the appropriate agencies.*

Related Policies:

- Manual Directive 102.3 – Code of Conduct
- Directive 307.1 – Electronic Mail and Internet Systems