MINNEAPOLIS POLICE DEPARTMENT

SPECIAL ORDER

BY ORDER OF THE CHIEF OF POLICE

DATE ISSUED:	DATE EFFECTIVE:	NUMBER:	PAGE:
xx xx, xx	xx xx, xx	SOxx-0xx	1 of 10
TO: Distribution "A"			RETENTION DATE: Until Rescinded
SUBJECT: **Manual Revision – 10-217 Social Media Use in Investigations** **5-108 Social Media Sites**			APPROVED BY:

MP-8806

Introduction:

Effective with the issuance of this Special Order, Section 10-217 of the MPD Policy and Procedure Manual shall be amended as follows:

10-217 Social Media Use in Investigations ~~Covert use of social media sites~~

(xx/xx/xx)

Revisions to prior policies: (12/15/09) (05/24/13) (09/20/21) (09/26/22)

I. Purpose

A. The ~~MPD~~ Minneapolis Police Department (MPD) recognizes that ~~the use of covert~~ social media ~~profiles~~ can be a useful tool in the investigation of criminal activity, when used in a lawful, non-discriminatory manner. This may include social media actions such as "following" and "engaging with" other accounts to establish a credible covert social media profile, as detailed and authorized in this policy.

[Moved from 5-108]

B. The purpose of this policy is to provide members with guidance on the use, management, administration, and oversight of social media for investigative and intelligence-gathering purposes. Personal social media accounts are covered by P&P 5-108.

II. Policy

A. Use For Law Enforcement or Public Safety Purposes

1. Social media accounts under this policy shall only be used when they could reasonably aid a legitimate criminal investigation of a person, group or organization, or for

intelligence collection efforts related to public safety or potential criminal activity. Personal social media accounts shall not be used for the purposes detailed in this policy.

2. Members shall not use social media accounts to collect and maintain criminal intelligence information about a person unless there is reasonable articulable suspicion (RAS) that the person is involved in criminal conduct or activity and the information is relevant to that criminal conduct or activity.

B. Use Department-Approved Equipment

Members shall only use access or use social media accounts under this policy through Department-approved electronic equipment.

C. Approval Requirements for Covert Social Media Accounts

1. Any member seeking to create or use a covert social media account shall obtain prior written approval from the member's Deputy Chief, through the chain of command (supervisor, Lieutenant, etc.) for the account and the proposed profile details. If a member needs to create a covert social media account due to an imminent threat or potentially life-threatening situation (such as a hostage situation), they may create the account with Deputy Chief or Watch Commander approval. After the situation is resolved, the member shall notify their chain of command.

2. These requirements apply to all covert social media accounts, including those used to collect open-source social media information.

D. ~~3.~~ No Promotion of Violence or Criminal Activity

MPD ~~employees~~ members shall not post any information through a ~~covert~~ social media ~~profile~~ account that promotes violence or criminal activity.
[Moved from 5-108]

E. Subject to MPD and City Policies

1. Social media use in investigations is subject to the requirements of P&P 5-108 Social Media Sites, the City's Electronic Communications Policy and Social Media Policy, and all other applicable MPD and City policies.

2. Members using social media accounts for investigation shall not post, display, or transmit content on their personal social media accounts or through City technology that is disparaging or evidences knowing and intentional discrimination toward a person or group based on protected class status, and that would lead an objectively reasonable person to doubt the member's ability to perform the duties of a peace officer in a fair and impartial manner (P&P 5-104).

3. When using covert social media techniques, conducting investigations, or otherwise establishing RAS or probable cause (PC), members shall not consider a person's protected class status, or substitutes for, or stereotypes of race or national origin, to any

extent or degree, when taking, or refraining from taking, any law enforcement action, except as provided below:

Members may consider a person's protected class status only if the demographic descriptors are part of a specific and detailed suspect description tied to a time and place that refers to a person with a particular demographic category and that includes other appropriate non-demographic identifying factors. This consideration must be based on credible and recent information that links specific unlawful or suspicious activity to the person or group, as part of an ongoing criminal investigation. (P&P 5-104)

4. Documentation collected under this policy, including registries and logs, shall be maintained in accordance with the City of Minneapolis' Records Retention Schedules.

III. Procedures/Regulations

A. Collecting Information from Social Media

Members may collect information available in the public domain for any legitimate law enforcement or public safety purpose and such activity does not require prior supervisory authorization or activity logging (except the requirements detailed in section [III-E] regarding investigations). This can include the following actions:

- Observing social media accounts and content.
- Searching for social media accounts and content.

B. Covert Social Media Profile Creation

If creation of a covert social media account has been approved ([II-C]), the member may create or use the social media account, profile, avatar, or a similar form of online identification.

1. Members shall complete the required training prior to using the account.

2. All profile details shall be fictitious and designed solely to support the authorized investigative objective, including usernames, biographical information, and photos, subject to the following:

   a. Members shall not use the name or other identifying information of any real person without that person's prior consent.

   b. Profile images or avatars shall be created using publicly available stock images or AI-generated images that do not depict real people.

C. ~~2. Employee~~ Member Responsibility for Account

[Moved from 5-108]

1. ~~a.~~ The ~~MPD employee~~ member registered as the ~~maintainer~~ account owner of a ~~covert~~ social media ~~profile~~ account is responsible for all content posted online under that profile.

2. ~~b.~~ The ~~employee~~ member shall maintain their ~~own~~ registered ~~covert~~ social media ~~profile~~account, and shall not share the access information with other ~~employees~~members, except that:

a. ~~i.~~ The ~~employee~~ member shall provide the password to their registered ~~profile~~ account upon request from the Commander of the Intelligence Division or their designee, or for auditing purposes.

D. Content Log Requirements

1. Log requirements are limited to original content

a. These logging requirements apply to original content, including but not limited to: original posts, comments made by the member, and direct messages sent.

b. These logging requirements do not apply to social media actions that do not generate original content such as reposts of other user's content, reactions (such as likes), and requests (such as requests to follow).

2. Process for logging content

Members using a covert social media account shall maintain a log of all content made through that profile.

a. The log shall include the date and time of the content, the page or profile the content was made on, and the subject of the content.

b. The member shall take screenshots of the content and store them with the log.

c. All content shall be documented in this manner and maintained even if the online content is later deleted.

E. Document Evidence and Demographics of Investigation Subject

Members using a social media account to conduct an investigation shall document in the case file all evidence collected, case numbers or incident numbers related to the investigation, and the following known or perceived demographic categories of every person who is a subject of the investigation:

- Race and ethnicity.
- Age.
- Gender.

F. Oversight

1. ~~1. Profile~~ Account registration

[Moved from 5-108]

The Commander of the Intelligence Division shall provide oversight by maintaining a centralized registry of all active covert social media accounts.

a. ~~a.~~ After accounts are approved per section [II-C], members shall register a~~A~~ll covert social media ~~profiles~~ accounts ~~shall be registered~~ with the Intelligence Division Commander ~~who oversees the Strategic Information Center (SIC)~~, and shall include the following information~~.~~

~~The information provided shall include:~~

- The name ~~&~~ and web address of the social media site or platform.
- The date the account was created.
- The username and screen name of the ~~covert~~ social media ~~profile~~account.~~, and~~
- The password for the account.
- The employe ID of the ~~MPD employee~~member responsible for maintaining the ~~covert~~ social media ~~profile~~account.

i. Members shall notify the Intelligence Division Commander if the information changes (including updating the password).

b. ~~c.~~ The Intelligence Division Commander or their designee shall conduct yearly audits to ~~ensure~~ confirm ~~that~~ whether ~~the~~ covert ~~profiles~~ social media accounts are still active.

c. ~~c.~~ When a covert ~~social media profile~~ account is no longer needed it shall be deactivated or deleted from the social media site~~,~~ to the extent permitted by the social media site, and the member shall notify the Intelligence Division Commander ~~shall be notified~~.

d. In addition to reviewing the data to confirm the active status of accounts, the Intelligence Division Commander or their designee may review accounts to ensure they are being used in compliance with MPD and City policy, and to ensure the supervisory review documentation complies with MPD policy.

2. Supervision

a. Supervisors shall monitor the use of covert social media accounts by their members.

i. Supervisors shall conduct a documented review of all covert social media accounts used by their direct reports on the following timelines:

- Every day a direct message is sent to or received from a minor.
- Every 30 days for accounts with active direct messaging.
- Every 120 days for accounts with no active direct messaging.

ii. In the review, supervisors shall review all content logged and shall ensure that:

aa. Members are operating accounts pursuant to this policy.

ab. Members are not operating accounts in a manner which could be interpreted as biased, unprofessional, or otherwise in violation of policy.

ac. Members are logging content as required.

b. Supervisors may contact the Commander of the Intelligence Division for information on the profiles to facilitate the review.

c. Members shall update their supervisor whenever an account is created or deactivated in accordance with this policy. If a member's unit is assigned a new supervisor or the member transfers units, the member shall provide their new supervisor with a list of their current covert social media accounts.

d. Supervisors shall provide the documentation of their reviews to the Intelligence Division Commander for storage with the registry.

5-108 Social Media Sites

(12/15/09) (05/24/13) (09/20/21) (09/26/22) (xx/xx/xx)

I. Purpose

To establish policy regarding ~~employee~~ the use of social media sites by members of the Minneapolis Police Department (MPD).

~~II. Definitions~~

[Moved to [IV]]

~~III.~~II. Policy

The MPD has a duty to protect the reputation of the organization and its ~~employees~~members, as well as guard against liability and potential legal risk. Therefore, ~~employees~~ members are advised of the following:

A. ~~Employees~~ Members should exercise caution and good judgment when engaging with social media sites. ~~Employees~~ Members should be aware that the content of these social media sites can be subpoenaed and used in criminal and civil trials to impeach the ~~employee's~~ member's testimony.

A. When engaging with social media sites, ~~employees~~ members are subject to all pertinent City of Minneapolis ("City") policies, MPD policies, and local, state, and federal laws regarding public information on arrests, investigations, and personnel data.

B. This policy supplements the City's Electronic Communications Policy and Social Media Policy.

~~IV.~~III. Procedure/Regulations

A. Requirements

Failure to comply with the following may result in discipline, up to and including discharge:

1. This MPD policy on social media sites (P&P 5-108).

2. The requirements of the City's Social Media Policy and its procedures.

3. Provisions of the City's Social Media Policy's Procedures related to personal use of social media sites.

   This includes, but is not limited to, the following clauses:

   a. Clause 2

      Employees must not use personal Social Media Sites to originate Content as an official form of communication, to speak on behalf of the City, to indicate they are representing the interests of the City, or in a way that could be perceived as official City communication. Always consider how something may be interpreted or understood before posting.

   b. Clause 4

      The City expects employees to be truthful, courteous, and respectful toward supervisors, co-workers, City residents, customers, and other persons or entities associated with or doing business with the City. When an employee can be identified as someone who does work for the City, they must not engage in name-calling or personal attacks or other such demeaning behavior if the conduct would adversely affect their duties or City workplace. This Section and its limitations apply when the action of the employee adversely affects their work, job duties or ability to function in their position or creates a hostile work environment.

   c. Clause 7:

      If an employee chooses to identify themselves as someone who does work on behalf of the City on a personal Social Media Site or on a Social Media Site that is not a City-Supported Social Media Site, and posts a personal opinion on a matter related to City business, a disclaimer that is similar to the following must be used:

      "These are my own opinions and do not represent those of the City of Minneapolis."

   d. Clause 9:

      i. There may be times when personal use of Social Media Sites that are not City-Supported Social Media Sites (even if it is off-duty or using their own equipment) may affect or impact the workplace and become the basis for coaching or discipline.

Examples of situations where this might occur include, but are not limited to:

- Cyber-bullying, stalking or harassment.
- Participating in offensive, hateful conduct.
- When conduct on personal Social Media could be perceived as a conflict with the City's mission, values, or degrades public trust in the City or its department.
- Release of City data that is not public.
- Unlawful activities.
- Inappropriate use of the City's name, logo, website URL, or the position or title of an employee or of someone who performs services for the City.
- Using City-owned equipment or City-time for more than occasional personal use on Social Media Sites that are not City-Supported Social Media Sites, which interferes with one's ability to do their job.
- Violation of law, whether federal, state, or local, or violation of a City policy.

ii. Each situation will be evaluated on a case-by-case basis because the laws in this area are evolving.

B. Authorized City-supported use

Certain MPD employees may be authorized to use social media sites for MPD-approved public relations and official investigative or work-related purposes. Such use must be approved by Police Administration.

~~**C. Covert use of social media sites**~~

~~The MPD recognizes that the use of covert social media profiles can be a useful tool in the investigation of criminal activity.~~

~~1. Profile registration~~

~~a. All covert social media profiles shall be registered with the Commander who oversees the Strategic Information Center (SIC). The information provided shall include:~~

- ~~The name & web address of the social media site~~
- ~~The username and screen name of the covert social media profile, and~~
- ~~The MPD employee responsible for maintaining the covert social media profile.~~

~~b. The Commander or their designee shall conduct yearly audits to ensure that the covert profiles are still active.~~

~~c. When a covert social media profile is no longer needed it shall be deactivated or deleted from the social media site, to the extent permitted by the social media site, and the Commander shall be notified.~~

~~2. Employee responsibility~~

~~a. The MPD employee registered as the maintainer of a covert social media profile is responsible for all content posted online under that profile.~~

~~b. The employee shall maintain their own covert social media profile, and shall not share the access information with other employees, except that:~~

~~i. The employee shall provide the password to their registered profile upon request from the Commander or their designee or for auditing purposes.~~

~~3. No promotion of violence or criminal activity~~

~~MPD employees shall not post any information through a covert social media profile that promotes violence or criminal activity.~~

Definitions

Social Media Content: Any posts, writings, material, documents, photographs, graphics, videos, links, or other information that is created, posted, distributed, or transmitted via social media.

Social Media Site: An internet site or application where users create and share content and participate in online communities and conversations, in the form of a page, profile, account, group or other presence. These include, but are not limited to, blogs, forums, chat sites, Facebook, Twitter, Instagram, Nextdoor, LinkedIn, Reddit, and YouTube. This policy includes emerging new web-based platforms generally regarded as social media or having many of the same functions as those listed.

Covert Social Media ~~Profile~~Account: ~~A social media site profile created and~~Account maintained by an MPD ~~employee~~member, on behalf of MPD, but in a username not associated with the MPD ~~employee~~member, for the purpose of furthering criminal investigations, gathering evidence for criminal investigations, or intelligence collection efforts related to public safety ~~investigating criminal activity~~.

Social Media Actions:

Follow: Subscribing to a feed of an account's activity.

Message: A direct or private communication sent between specific users. This includes direct messages, chats, etc. Unlike public posts or comments, messages are only visible to the sender and the recipients.

Post: Uploading content to a page or profile, or adding an original comment to content uploaded by another user. This includes comments, replies, posts (including uploading material someone else created), images, videos, etc.

React: Using a built-in function to indicate appreciation or another emotional reaction to another account's content. This includes using a "Like" button or other preset option that does not add a text comment.

Repost: Sharing another account's content. This includes functions such as retweet, share, repin, etc.

Request to Connect: A request sent from one account to another account to establish a mutual sharing relationship, requiring the recipient to confirm or accept the request to provide access to content not available to other accounts. This includes functions such as Facebook's "Friend" requests.

Request to Follow: A request to subscribe to a feed of an account's activity that requires the account to approve the request. This includes functions such as a Follower Request in "X" (formerly Twitter).