EXECUTIVE ORDER

METROPOLITAN POLICE

DISTRICT OF COLUMBIA

Subject
Social Media for Investigative and Intelligence-Gathering Purposes
Number
EO-21-025
Effective Date
November 8, 2021
Replaces: EO-21-024 (Social Media for Investigative and Intelligence-Gathering Purposes), Effective Date October 15, 2021 **Related to:** GO-OPS-304.01 (Operation and Management of Criminal Investigations)

I. PURPOSE

The purpose of this executive order is to provide Metropolitan Police Department (MPD) members with guidance on the use, management, administration, and oversight of social media for investigative and intelligence-gathering purposes.

II. PROCEDURES

A. Use of Social Media for Investigations and Intelligence-Gathering

1. Overt monitoring, searching, and collecting of information available in the public domain for any legitimate law enforcement purpose is permitted and requires no supervisory authorization. Overt use of social media in the public domain may include the use of fictitious accounts created to monitor social media provided the account is not used to engage in conversation.

2. In certain circumstances and pursuant to the procedures set forth in this order, members of the following elements may request approval to use non-official MPD social media accounts (i.e., undercover accounts) in the course of legitimate criminal investigations or intelligence collection efforts related to public safety or potential criminal activity.

Undercover Accounts
a. Criminal Investigations Division
b. Intelligence Division
c. Internal Affairs Division (criminal investigations only)
d. Narcotics and Special Investigations Division
e. Youth and Family Services Division

3. Members shall request written approval from the Narcotics and Special Investigations Division (NSID) commander through the chain of command **prior** to using or creating an undercover account. The NSID commander shall ensure new accounts are reviewed to ensure de-confliction with existing accounts and investigations.

4. If approved, the member may create or use an undercover social media account, profile, avatar, or a similar form of online identification.

    a. Members shall complete training prior to using an undercover account.

    b. Members shall not use a proprietary image or another person's likeness without prior consent.

    c. Members using an undercover account to engage in conversations with a subject may only do so when the member is physically located in the District of Columbia (i.e., to ensure compliance with one-party consent).

    d. Members shall not use their personal social media account or personal information to access content that is being used as part of an investigation or intelligence-gathering effort.

5. Members have no expectation of privacy when using fictitious social media accounts for overt monitoring or when using undercover social media accounts as all accounts are subject to discovery.

6. Members shall ensure that any criminal investigations involving or overlapping investigations related to First Amendment activities are conducted pursuant to DC Official Code § 5-333.01, *et seq*.

7. Members shall use only department or federal law enforcement equipment throughout the investigation.

8. Members shall not use another individual’s personal account without his or her consent and the written approval of their commanding official, the rank of commander or above.

9. Members shall not use undercover social media accounts on personal devices.

10. Members seeking to use the personal account of confidential informants or cooperating witnesses shall request specific approval from NSID through the member’s commanding official.

11. Members shall not post content that is disparaging to a person or group based on race, color, religion, national origin, sex, age, marital status, personal appearance, sexual orientation, gender identity or expression, familial status, family responsibilities, matriculation, political affiliation, genetic information, disability, source of income, status as a victim of an intrafamily offense, place of residence or business, and status as a victim or family member of a victim of domestic violence, a sexual offense, or stalking.

12. Members shall report any potential compromise of an online alias to their official immediately upon becoming aware and be guided by his or her direction.

B. Oversight and De-Confliction

1. NSID shall provide oversight by maintaining a centralized registry of all active undercover social media accounts for de-confliction purposes. The registry shall include any assigned central complaint numbers (CCNs) or incident summary (IS) numbers, name of primary investigating member responsible for the account, date that the account was created, social media platform used to create the account, and log in credentials (i.e., username and password).

2. Commanding officials shall monitor the use of undercover social media accounts in use by their members. Commanding officials shall conduct a documented review of all accounts every 30 days to ensure:

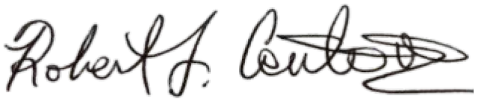
   a. That members are operating accounts pursuant to this order and not in a manner which could be interpreted as biased, unprofessional, or otherwise in violation of policy; and

   b. That each investigation warrants the continued use of an undercover account.

III. DEFINITIONS

When used in this directive, the following terms shall have the meanings designated.

	Term	Definition
1.	Fictitious account	Social media identity that has been created by a member of MPD for the purpose of concealing his or her identify as a law enforcement officer in order to engage in overt monitoring of social media.
2.	Monitor	Observing social media accounts and content including sending requests to follow individual social media accounts.
3.	Post	Uploaded content or added response uploaded by another user.
4.	Profile	Information that a user provides about him or herself on a social media or similar site.
5.	Social media	Online sources that allow people to communicate, share, and exchange information with others via some form of online or cellular network platform (e.g., Facebook, Twitter, Instagram, LinkedIn). Information may include, but is not limited to, text, photographs, video, audio, and other multimedia files, message or online bulletin boards, and other similarly developed formats, to communicate with others using the same groups while also networking with other users based upon similar interests (e.g., geographical location, skills, occupation, ideology, beliefs).
6.	Undercover account	Social media identity that has been created by a member of MPD for the purpose of concealing his or her identify as a law enforcement officer in order to gain information.



Robert J. Contee III
Chief of Police

RJC:KDO:MOC:SMM

Amendment #	*Page #*	*Description of Change*	*Effective Date of Change*	*Name and Title of Authorizing Member*
1	2	Revise Part II.A.6 to reference DC Official Code § 5-333.01, *et seq.*	10/11/2024	Maureen O'Connell, Director, Policy and Standards Branch