Bureau Order

UNIT INDEX NUMBER	23-01
DATE ISSUED	04/6/23
DATE REVISED	3/27/23

SUBJECT:
Investigative Social Media Accounts

ISSUED TO:
Airport Bureau

ISSUED BY:
Deputy Chief Mikail Ali

AIRPORT BUREAU – INVESTIGATIVE SOCIAL MEDIA ACCOUNTS

The use of social media in law enforcement related investigations is a valuable tool to the San Francisco Police Department. Social media is used by investigators across the Department, particularly the Investigations Bureau. Information obtained from investigative social media accounts can provide critical evidence in cases involving homicide, human trafficking, missing persons, firearms and firearms-related offenses, narcotics, special investigations, internet crimes, crimes against children, etc.

The law is constantly evolving with the advancement of technology, evolution of social media, the passage of new statutes, and the issuance of state and federal court rulings. SFPD members are responsible for maintaining their familiarity with clearly established rights as determined by case law and when there is a discrepancy with this policy, members shall adhere to the most current California and federal law.

Members shall maintain working knowledge of current law and Department policy specifically as it relates to: the First Amendment and Fourth Amendment of the United States Constitution, CalECPA (California Penal Code sections 1546-1546.4), and DGO 8.10 Guidelines for First Amendment Activity.

The following policies are meant to govern the use of investigative social media accounts. This policy does not affect the access to information or collection of evidence from open-source platforms.

Barring a warrant, exigent circumstances, or approval as outlined within this policy, members shall only access, download, and save open-source information or publicly available material that is posted in a publicly accessible format.

While it is the policy of the Airport Bureau to work with San Mateo County Sheriff's Office to investigate criminal cases, members assigned to the Airport Bureau shall comply with the contents of this order.

DEFINITIONS:

Social media: Online platforms that facilitate social networking platforms, blogging and/or photo and video-sharing, Podcasts, RSS Feeds or other similar platforms. Social media includes, but is not limited to, proprietary social media sites, applications such as Facebook, Instagram, LinkedIn, Snapchat, MySpace, Twitter, and YouTube as well as collaboration services such as Wikipedia and Blogspot or any emergent social media platform or service now in existence or that become available in the future.

Open-source: For the purpose of this policy, open-source social media is social media content that can be accessed, viewed, and saved by SFPD members or the general public through sources generally available to the public such as Google, Safari, Firefox, etc. This information is available without the creation of a profile or a registration requirement.

Investigative social media account: Social media accounts that are created and maintained by a member of SFPD for the purpose of concealing his or her identify as a law enforcement officer in order to access social media as part of a legitimate law enforcement investigation. Some investigative social media accounts are also undercover accounts.

Undercover account: Investigative social media accounts that will actively engage with a suspect, witness, or victim of an investigation or potential crime in order to gain information. Examples include, but are not limited to: ICAC Unit creating a profile for a "to catch a predator" operation, SVU communicating with a human trafficking victim, or an undercover buy operation.

APPROVAL PROCESS:

The following process is required for approval to use investigative social media accounts and/or undercover accounts.

Investigative social media accounts approval:

Members assigned to the Airport Bureau shall write a memo, requesting to use investigative social media accounts, to be reviewed and approved by the Captain within the member's chain of command.

The memo should include: their current investigative assignment and the reasons why the use of investigative social media accounts is necessary to carrying out their duties.

Approved memos shall be forwarded to the Captain of Strategic Investigations for review and deconfliction, and to log the account consistent with the Oversight and De-Confliction section below.

Approved use of social media accounts applies strictly to a member's current assignment and is not transferable. Reassigned members shall re-request permission to use investigative social media accounts.

Undercover social media accounts approval:

Members using undercover accounts require approval to use investigative social media accounts as referenced above. Additionally, members need specific written approval from their Captain to create and use an undercover account and must do so in conjunction with a specific

investigation or enforcement operation. Approval shall be forwarded to the Captain of Strategic Investigations.

Exigent circumstances:
In the event of exigent circumstances (an emergency), members may access an investigative social media account or an undercover account without prior approval. In these circumstances, members shall acquire written approval as soon as reasonably possible and shall document the reasons why the use of an investigative social media account and/or undercover account was necessary.

USE OF SOCIAL MEDIA:
Members shall use investigative social media accounts for legitimate law enforcement related purposes only. All other use of investigative social media accounts is strictly prohibited.

On-duty:
Members should access investigative social media accounts while on duty. If a member discovers credible leads or relevant information to another investigative unit, members should forward that information.

If circumstances exist requiring a member to use an investigative social media account while off-duty, members are required to have articulable facts to support its use. Such facts may include: a tip from a confidential informant that needs to be verified, the occurrence of a violent crime, a spike in recent violent crime, specific focus on a high-risk individual, noticeable uptick in violent crime between known groups, etc. If members obtain information that requires immediate action or indicates an on-going public safety concern, members shall provide that information to appropriate on-duty personnel.

If a member discovers evidence that is relevant to a potential law enforcement investigation while off-duty, the member should document it and attempt to verify/re-access that information while next on-duty.

Equipment:
Members shall use only Department or federal law enforcement equipment when accessing investigative social media accounts.

Documentation and preservation of evidence:
Depending on the nature of the investigation and the evidence on social media, members should submit a preservation order and/or obtain a search warrant for evidence observed through the use of investigative social media accounts. CalECPA, as codified in California Penal Code sections 1546-1546.4, sets forth the search warrant requirements for social media content.

For the purposes of evidence collection, chain of custody, and its potential use in court, members shall documentwhere and when any evidence is collected. This documentation may be in a Chronological of Investigation, incident report, or through the use of the Investigative Social Media Account Form.

Use of undercover accounts:

Undercover accounts shall only be used as part of an approved investigation or operation. Members are encouraged to register all undercover accounts with WSIN for the purpose of deconfliction.

Members shall not:

1. Monitor a suspect for non-law enforcement purposes.
2. Use their own personal social media account or personal account information to access social media content for investigations.
3. Create a profile in someone's likeness without their express written or recorded consent.
4. Use an individual's personal account without their express written or recorded consent. If exigent circumstances exist, and written or recorded consent is not possible, members shall document the reasons why in the appropriate Chronological of Investigation or incident report.

BIASED FREE POLICING:
Members are reminded that police action that is biased is illegal and violates the fundamental rights of all individuals guaranteed under the United States Constitution. SFPD is committed to just, transparent, and bias-free policing. DGO 5.17, Bias-Free Policing Policy, applies to all activity members engage in including the use of investigative social media accounts.

CONTINUOUS TRAINING:
Members shall attend training prior to using investigative social media accounts. Given the evolution of case law, Department policy, and emerging technology, members are encouraged to continue to remain up to date on training as it relates to the use of investigative social media accounts.

OVERSIGHT AND DE-CONFLICTION: The Captain of Strategic Investigations, or their designee, shall provide oversight by maintaining a confidential centralized registry of all active investigative and undercover social media accounts used throughout the Department. The registry shall include the investigating member responsible for the account, their approved memo, the date the account was created, social media platform, and account name and password.

On a semiannual basis, the Captain of Strategic Investigations, or their designee, shall conduct a documented review of all accounts to ensure:

1. The member is operating the account pursuant to this order and not in a manner which could be interpreted as biased, unprofessional, or otherwise in violation of Department policy; and
2. The account is being used for a legitimate law enforcement purpose and its continued use is necessary.