Investigative Social Media Accounts

6.21.01 PURPOSE

The purpose of this order is to establish the policy and procedures for the approval, use, and oversight of investigative social media accounts in criminal investigations.

6.21.02 POLICY

The use of investigative social media accounts in law enforcement related investigations are a valuable tool to the San Francisco Police Department. Investigative social media accounts are used by members/employees 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 following procedures 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 social media.

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

Members/employees assigned to the Airport Bureau shall comply with the contents of this order notwithstanding any collaboration with the San Mateo County Sheriff's Office to investigate criminal cases.

The term "member," used throughout this Department General Order, refers to sworn members of the Department. The term "employee" refers to a non-sworn employee of the Department.

6.21.03 DEFINITIONS

Social media: A category of internet-based services that incorporate use-generated content and user participation. These services allow users to create public or semi-public profiles within a finite system, articulate a list of other users and groups with whom they share a connection, and view and navigate this list and lists made by others within the system. On these sites, users create online communities to share information, ideas, personal messages, and other content. Social media sites include, but are not limited to: Facebook, Instagram, TikTok, Twitter, YouTube, Snapchat, LinkedIn, and Reddit.

Open-source social media: For the purpose of this policy, open-source social media is social media content that can be accessed, viewed, and saved by 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/employee of SFPD for the purpose concealing his or her identify as law enforcement to access social media for a legitimate law enforcement purpose as part of an actual or potential criminal investigation. Some investigative social media accounts are also undercover accounts but merely requesting to "follow" or "friend" another account does not transform an investigative social media account into an undercover account.

Undercover account: A subset of investigative social media accounts that are created and used to proactively engage in verbal/written communication with a suspect, witness, or victim of an actual or potential criminal investigation 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 a narcotics undercover buy operation.

Exigent Circumstances: The term "exigent circumstances" describes an emergency situation requiring swift action to prevent imminent danger to life or serious damage to property, or to prevent the imminent escape of a suspect or destruction of evidence.

Legitimate law enforcement purpose includes an investigation intended to address unlawful conduct, either past, present, or future, including whether a person has knowledge of such past, present, or future unlawful conduct, or to address public safety issues, whether they amount to criminal conduct or not. A reasonable law enforcement purpose would include acquiring information or intelligence which may be useful in allocating resources for public safety and acquiring information or intelligence which may be useful for future criminal investigations.

6.21.04 APPROVAL PROCESS

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

A. Investigative social media accounts approval:
If requesting approval, members/employees shall write a memo, requesting to use investigative social media accounts, to be reviewed and approved by the Captain within the member/employee's chain of command, or if no Captain, an employee with a rank-equivalent to a Captain or above.

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/employee's current assignment and is not transferable. Reassigned members/employees shall re-request permission to use investigative social media accounts.

B. Undercover social media accounts approval:
Members/employees using undercover accounts require approval to use investigative social media accounts as referenced above. Additionally, members/employees 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.

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

6.21.05 USE OF INVESTIGATIVE SOCIAL MEDIA

A. Use:
Members/employees shall use investigative social media accounts for legitimate law enforcement related purposes only. All other use of investigative social media accounts is strictly prohibited.

B. On and off duty access:

1. Members/employees should access investigative social media accounts while on duty. If a member/employee discovers credible leads or relevant information to another investigate unit, members/employees should forward that information.

2. If circumstances exist requiring a member/employee to use an investigative social media account while off-duty, members/employees 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 know groups, etc. If members/employees obtain information that requires immediate action or indicates an on-going public safety concern, member/employees shall provide that information to appropriate on-duty personnel.

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

b. Existing overtime policies and protocols apply for off-duty use of investigative social media accounts.

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

D. Documentation and preservation of evidence:
Depending on the nature of the investigation and the evidence on social media, members/employees 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/employees shall document where 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, etc.

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

6.21.06 PROHIBITIONS AND BIAS FREE POLICING REQUIREMENTS

A. Members/employees shall not:

1. Use their own personal social media account or personal account information to access social media content for investigations.

2. Create a profile that falsely impersonates any real person.

3. 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/employees shall document the reasons why in the appropriate Chronological of Investigation or incident report.

B. Bias Free Policing

Members/employees 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.

6.21.07 CONTINUOUS TRAINING

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/employees are responsible for maintaining their familiarity with clearly established rights as determined by case law and when there is a discrepancy with this this policy, members/employees shall adhere to the most current California and federal law.

Members/employees 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).

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

6.21.08 OVERSIGHT AND DE-CONFLICTION

A. Registry:
The Captain of Strategic Investigations, or their designee, shall provide oversight by maintaining a privileged and confidential centralized registry, within the meaning of Evidence Code section 1040 et. seq., of all active investigative and undercover social media accounts used throughout the Department. The registry shall include:

- the investigating member/employee responsible for the account(s),
- the approved approval memo,
- the date the account(s) was created,
- social media platform(s) used,
- the account name(s) and password(s)
- documentation of each review of the account(s).

B. Oversight:
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/employee 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.

If, during the semiannual review, it is determined that an account is no longer necessary or being used, the Captain of Strategic Investigations, or their designee, shall order the member/employee to suspend or shut the account down.

References:

DGO 2.01, *General Rules of Conduct*
DGO 5.16, *Obtaining Search Warrants*
DGO 5.17, *Bias-Free Policing Policy*
DGO 8.10, *Guidelines for First Amendment Activity*
Penal Code sections 1546-1546.4