Chicago Police Department

# USE OF SOCIAL MEDIA OUTLETS

**General Order G09-01-06**

| | | | |
|---|---|---|---|
| **ISSUE DATE:** | 22 October 2020 | **EFFECTIVE DATE:** | 22 October 2020 |
| **RESCINDS:** | 29 February 2020 Version | | |
| **INDEX CATEGORY:** | 09 - Information Management | | |
| **CALEA:** | | | |

## I. PURPOSE

This directive:

A. establishes guidelines and responsibilities of Department members using social media outlets, including:

1. the use of Department-authorized and personal social media accounts.

2. prohibitions and restrictions on posting content, including posting content that is disparaging to a person or group based on any legally protected class.

3. the use of social media for investigations.

B. satisfies the CALEA law enforcement standard in chapter 54.

C. *Introduces use of Department forms:*

1. *Social Media Covert Identity Authorization (*CPD-41.307*)*

2. *Social Media Information Request (*CPD-11.310*)*

## II. POLICY

A. Social media outlets, when used in a proper manner, can reinforce the Department's relationship with the public, build community support, and assist in solving crime. Department members have a constitutional right to express their views under the First Amendment. However, Department members may be subject to discipline for violating the provisions of this directive. Any social media participation made pursuant to a Department member's official duties is not considered protected speech under the First Amendment.

B. For the purposes of this directive, the term "social media outlets" means any electronic communication (such as personal Web sites, outlets for social networking, and microblogging) through which participants utilize online communities to share information, ideas, personal messages, and other content through an electronic format. These formats include, but are not limited to, text, video, photographs, audio, digital documents, etc.

C. When using social media, whether on or off duty, Department members are prohibited from posting, displaying, transmitting, or otherwise disseminating:

1. any communications that discredit or reflect poorly on the Department, its vision, mission, values, or goals.

2. confidential information related to Department training, activities, or on-going investigations without express written permission.

3. content that is disparaging to a person or group based on race, color, sex, gender identity, age, religion, disability, national origin, ancestry, sexual orientation, marital status, parental status, military status, source of income, credit history, criminal record, criminal history, or any other protected class consistent with the Department directives titled "Human Rights and Human Resources" and "Prohibition Regarding Racial Profiling and Other Bias-Based Policing."

D. The policies outlined in this directive address the full breadth and scope of social media rather than any one particular format. The Department recognizes that as technology advances, new methods for social media participation will emerge.

## III. USE OF SOCIAL MEDIA OUTLETS

A. When using social media, whether on or off duty, Department members should be mindful that their communications become part of the worldwide electronic public domain. Department members should be aware that privacy settings and social media sites are subject to constant modifications, and they should never assume that personal information posted on such sites is protected or secure.

B. Department members should expect that any information that they create, transmit, download, exchange, or discuss that is available online in a public forum may be accessed by the Department without prior notice.

C. Department-Authorized Social Media Accounts

1. All Department social media outlets will be approved by the Superintendent or a designee.

2. The use of Department computers and Department-issued electronic communication devices by Department members to access any social media outlet is prohibited absent prior supervisory approval. Supervisory approval will be on an individual basis or based on a specific job assignment or responsibility.

3. Social media content will adhere to applicable laws, the Rules and Regulations of the Chicago Police Department, and any relevant Department policies, including all information-technology and records-management policies.

a. Access to Department social media accounts and the internet will be consistent with the Department directives titled "Use of the Internet," "Department-Issued Electronic Communication Devices," and "Social Media Outlet: Twitter."

b. Department records-retention schedules will apply to social media content and is subject to the Local Records Act (50 ILCS 205/1), consistent with the Department directive titled "Records Managemen t."

c. Content will be managed, stored, and retrievable in compliance with the Illinois Freedom of Information Act (5 ILCS 140/1) and consistent with the Department directive titled "Freedom of Information."

4. Department members authorized to administer Department social media outlets will:

a. conduct themselves at all times as representatives of the Department and, accordingly, adhere to applicable Department Rules and Regulations and Department directives.

b. not make statements indicating the guilt or innocence of any suspect or arrestee, or comments concerning pending prosecutions.

c. comply with all copyright, trademark, and service-mark restrictions in posting materials to electronic media.

d. ensure that all relevant privacy protections are maintained.

D. Department Members' Personal Social Media Accounts

In addition to the prohibitions outlined in Item II-C, when using their personal social media accounts, Department members are prohibited from posting, displaying, transmitting, or otherwise disseminating:

1. Department information, records, documents, video recordings, audio recordings, or photographs to which they have access as a result of their employment without the written permission from the Communications Division or the Superintendent or a designee.

2. any references to any other Department member's employment by the Department without that person's consent.

3. any intellectual property of the Department or the City of Chicago without the specific authorization of the Superintendent or a designee. Department or City of Chicago intellectual property includes but is not limited to logos, uniforms, official photographs, audio/ video files, or any text documents (paper or electronic)

4. any information representing themselves as an official spokesperson of the Department and the City of Chicago unless specifically authorized by the Superintendent or a designee.

## IV. USE OF SOCIAL MEDIA OUTLETS FOR INVESTIGATIVE PURPOSES

A. Social media is a valuable investigative tool when seeking evidence or information about:

1. missing persons;

2. wanted persons;

3. gang violence and retaliation;

4. crimes perpetrated online (e.g., cyberbullying, cyberstalking);

5. photos or videos of a crime posted by a participant or observer;

6. criminal participation and retaliation;

7. acquiring information or intelligence that may be useful for criminal investigations or allocating resources for public safety;

8. aiding the coordination and deployment of police resources; and

9. administrative and criminal investigations by the Bureau of Internal Affairs.

10. *criminal investigations by the Bureau of Detectives and the Bureau of Counterterrorism.*

B. Exempt commanding officers of units that conduct investigations using social media will establish standard operating procedures and unit-level protocols created in consultation with the Legal Affairs Section and the Information Services Division.

C. Department members utilizing a social media outlet as an investigative tool will:

1. use only Department-approved electronic equipment throughout the investigation;

2. conduct an investigation only while on duty;

3. follow the guidelines set forth in the Rules and Regulations of the Chicago Police Department and the the investigative and reporting guidelines outlined in the appropriate Department directives including, but not limited to:

a. "The First Amendment and Police Actions,"

b. "Investigations Directed at First Amendment-Related Information,"

c. "Other Police Action Which May Impact First Amendment Conduct."

4. barring a warrant, exigent circumstances, or prior authorization under Item IV-D-4, only use publicly available material or information that is posted in a publicly accessible format;

5. forward any credible leads to the appropriate investigative unit;

6. notify the Communications Division of social media posts that will likely generate media inquiries or interest; and

7. document the use of social media as an investigative tool in the appropriate reports.

D. Department members utilizing a social media outlet as an investigative tool will **not** :

1. monitor a suspect for *non-law enforcement purposes.*

2. use their personal social media account or personal account information to access the social media content.

3. use another individual's personal account without his or her consent and the approval of the appropriate bureau chief.

4. create an alias account or identity, contact a suspect, or actively participate in any discussion with a suspect using said account without the *approval of the highest-ranking exempt member the rank of chief or above within the member's chain of command. Furthermore:*

a. *Members applying for a social media account will:*

(1) *Complete Department form (CPD-41.307) "Social Media Covert Identity Authorization" ,*

(2) *Submit completed form through their appropriate chain of command to the highest-ranking exempt-member chief or above for approval to create the account, and*

**NOTE:** *Once a Social Media Covert Identity Authorization Form is approved by the members highest-ranking exempt-member chief or above, the member can create a covert identity social media account.*

(3) *Forward all approved forms to the Chief, Bureau of Counterterrorism.*

b. *The Chief, Bureau of Counterterrorism, will review the submitted account to ensure that accounts adhere to applicable Department Rules and Regulations and authorize the account to be managed by the Bureau of Counterterrorism.*

E. *Department members receiving information or intelligence through social media that may be useful for criminal investigations or allocating resources for public safety that may require further investigation outside the unit's investigative duties or abilities will:*

1. *complete Department form (CPD-11.310) Social Media Information Request, and*

2. *forward all submitted requests to Confidential Analytic Section, Intelligence Division at casadmin@chicagopolice.org for further investigation or dissemination to the appropriate investigative unit.*

(*Items indicated by italic/double underline were added or revised.*)

David O. Brown
Superintendent of Police

20-079 SPC