

BOARD of SUPERVISORS



City Hall
1 Dr. Carlton B. Goodlett Place, Room 244
San Francisco 94102-4689
Tel. No. (415) 554-5184
Fax No. (415) 554-5163
TDD/TTY No. (415) 554-5227

MEMORANDUM

RULES COMMITTEE

SAN FRANCISCO BOARD OF SUPERVISORS

TO: Supervisor Matt Dorsey, Chair
Rules Committee

FROM: Victor Young, Assistant Clerk *Victor Young*

DATE: July 17, 2023

SUBJECT: **COMMITTEE REPORT, BOARD MEETING**
Tuesday, July 18, 2023

The following file should be presented as a **COMMITTEE REPORT** at the Board Meeting on Tuesday, July 18, 2023. This item was acted upon at the Rules Committee Meeting on Monday, July 17, 2023, at 10:00 a.m., by the votes indicated.

Item No. 79 File No. 230689

[Administrative Code - Surveillance Technology Policy - Social Media Management Software]

Ordinance approving Surveillance Technology Policy for Human Services Agency use of social media management software.

RECOMMENDED AS COMMITTEE REPORT

Vote: Supervisor Shamann Walton - Aye
Supervisor Ahsha Safai – Absent
Supervisor Matt Dorsey - Aye

c: Board of Supervisors
Angela Calvillo, Clerk of the Board
Alisa Somera, Legislative Deputy Director
Anne Pearson, Deputy City Attorney

File No. 230689

Committee Item No. 2

Board Item No. _____

COMMITTEE/BOARD OF SUPERVISORS

AGENDA PACKET CONTENTS LIST

Committee: Rules Committee

Date July 17, 2023

Board of Supervisors Meeting

Date _____

Cmte Board

- Motion
- Resolution
- Ordinance
- Legislative Digest
- Budget and Legislative Analyst Report
- Youth Commission Report
- Introduction Form
- Department/Agency Cover Letter and/or Report
- Memorandum of Understanding (MOU)
- Grant Information Form
- Grant Budget
- Subcontract Budget
- Contract/Agreement
- Form 126 - Ethics Commission
- Award Letter
- Application
- Form 700
- Information/Vacancies (Boards/Commissions)
- Public Correspondence

OTHER (Use back side if additional space is needed)

- Surveillance Technology Polcy
- _____
- _____
- Surveillance Impact Report - Human Services Agency
- _____
- _____
- _____
- _____
- _____

Completed by: Victor Young

Date July 13, 2023

Completed by: _____

Date _____

1 [Administrative Code - Surveillance Technology Policy - Social Media Management Software]

2

3 **Ordinance approving Surveillance Technology Policy for Human Services Agency use**
4 **of social media management software.**

5 NOTE: **Unchanged Code text and uncodified text** are in plain Arial font.
6 **Additions to Codes** are in *single-underline italics Times New Roman font*.
7 **Deletions to Codes** are in ~~*Times New Roman font*~~.
8 **Board amendment additions** are in Arial font.
9 **Board amendment deletions** are in ~~Arial font~~.
10 **Asterisks (* * * *)** indicate the omission of unchanged Code
11 subsections or parts of tables.

12 Be it ordained by the People of the City and County of San Francisco:

13

14 Section 1. Background.

15 (a) Terms used in this ordinance have the meaning set forth in Administrative Code
16 Chapter 19B (“Chapter 19B”).

17 (b) Chapter 19B regulates Departments’ acquisition and use of Surveillance
18 Technology. Under Section 19B.2(a), Departments must obtain Board of Supervisors approval
19 by ordinance of a Surveillance Technology Policy before: (1) seeking funds for Surveillance
20 Technology; (2) acquiring or borrowing new Surveillance Technology; (3) using new or
21 existing Surveillance Technology for a purpose, in a manner, or in a location not specified in a
22 Surveillance Technology ordinance; (4) entering into agreement with a non-City entity to
23 acquire, share, or otherwise use Surveillance Technology; or (5) entering into an oral or
24 written agreement under which a non-City entity or individual regularly provides the
25 Department with data or information acquired through the entity’s use of Surveillance
Technology.

1 (c) Under Section 19B.2(b), the Board of Supervisors may approve a Surveillance
2 Technology Policy ordinance under Section 19B.2(a) only if: (1) the Department seeking
3 Board of Supervisors approval first submits to the Committee on Information Technology
4 (“COIT”) a Surveillance Impact Report for the Surveillance Technology to be acquired or used;
5 (2) based on the Surveillance Impact Report, COIT develops a Surveillance Technology
6 Policy for the Surveillance Technology to be acquired or used by the Department; and (3) at a
7 public meeting at which COIT considers the Surveillance Technology Policy, COIT
8 recommends that the Board of Supervisors adopt, adopt with modifications, or decline to
9 adopt the Surveillance Technology Policy for the Surveillance Technology to be acquired or
10 used.

11 (d) Under Section 19B.4, the City policy is that the Board of Supervisors will approve a
12 Surveillance Technology Policy ordinance only if it determines that the benefits that the
13 Surveillance Technology ordinance authorizes outweigh its costs, that the Surveillance
14 Technology Policy ordinance will safeguard civil liberties and civil rights, and that the uses and
15 deployments of the Surveillance Technology under the ordinance will not be based upon
16 discriminatory or viewpoint-based factors or have a disparate impact on any community or
17 Protected Class.

18
19 Section 2. Surveillance Technology Policy Ordinance for Human Services Agency
20 (“HSA”) Use of Social Media Management Software.

21 (a) Purpose. HSA seeks Board of Supervisors approval under Section 19B.2(a) to use
22 social media management software to (1) plan and execute more effective and strategic
23 campaigns across social media platforms; (2) schedule multiple social media posts in
24 advance; (3) create and publish or post multiple streams of content across various social
25 media platforms; (4) maintain an active social media presence that is automated, specifically

1 on weekends and holidays when staff are not working; (5) ensure consistency of messaging
2 across all social media platforms; (6) track social media post performance and analyze social
3 media trends to improve content and strategy; (7) monitor public posts for references to HSA's
4 social media presence and for specific search terms or hashtags related to HSA's work in the
5 community; (8) access and respond to correspondence sent through social media platforms;
6 and (9) create reports.

7 (b) Surveillance Impact Report. HSA submitted to COIT a Surveillance Impact Report
8 for social media management software. A copy of this Surveillance Impact Report is on file
9 with the Clerk of the Board of Supervisors in Board File No. 230689.

10 (c) Public Hearings. On August 26, 2022, and September 15, 2022, COIT and its
11 Privacy and Surveillance Advisory Board conducted two public hearings at which they
12 considered the Surveillance Impact Report referenced in subsection (b) and developed a
13 Surveillance Technology Policy for HSA's use of social media management software. A copy
14 of this Surveillance Technology Policy ("HSA Sprout Social_STP_FINAL 08.11.22") is on file
15 with the Clerk of the Board of Supervisors in Board File No. 230689.

16 (d) COIT Recommendation. On September 15, 2022, COIT voted to recommend that
17 the Board of Supervisors adopt HSA's Surveillance Technology Policy, referenced in
18 subsection (c), for the use of social media management software.

19 (e) Findings. The Board of Supervisors hereby finds that the stated benefits of HSA's
20 use of social media management software outweigh the costs and risks of use of such
21 Surveillance Technology; HSA's Surveillance Technology Policy for the use of social media
22 management software will safeguard civil liberties and civil rights; and that the uses and
23 deployments of social media management software, as set forth in HSA's Surveillance
24 Technology Policy for the use of social media management software, are not and will not be
25

1 based upon discriminatory or viewpoint-based factors or have a disparate impact on any
2 community or a Protected Class.
3

4 Section 3. Approval of Policy. The Board of Supervisors hereby approves HSA’s
5 Surveillance Technology Policy for the use of social media management software.
6

7 Section 4. Effective Date. This ordinance shall become effective 30 days after
8 enactment. Enactment occurs when the Mayor signs the ordinance, the Mayor returns the
9 ordinance unsigned or does not sign the ordinance within ten days of receiving it, or the Board
10 of Supervisors overrides the Mayor’s veto of the ordinance.
11

12
13 APPROVED AS TO FORM:
14 DAVID CHIU, City Attorney

15 By: _____
16 VALERIE J. LOPEZ
17 Deputy City Attorney

18
19
20
21
22
23
24
25
n:\legana\as2023\2300245\01671579.docx

LEGISLATIVE DIGEST

[Administrative Code - Surveillance Technology Policy - Social Media Management Software]

Ordinance approving Surveillance Technology Policy for Human Services Agency use of social media management software.

Background Information

Pursuant to Administrative Code Section 19B.2(b), the Human Services Agency ("HSA") seeks Board of Supervisors approval of a Surveillance Technology Policy regarding the use of social media management software. The proposed Surveillance Technology Policy would authorize HSA to (1) plan and execute more effective and strategic campaigns across social media platforms; (2) schedule multiple social media posts in advance; (3) create and publish or post multiple streams of content across various social media platforms; (4) maintain active social media presence that is automated, specifically on weekends and holidays when staff are not working; (5) ensure consistency of messaging across all social media platforms; (6) track social media post performance and analyze social media trends to improve content and strategy; (7) monitor public posts for references to HSA's social media presence and for specific search terms or hashtags related to HSA's work in the community; (8) access and respond to correspondence sent through social media platforms; and (9) create reports.

On August 26, 2022, and September 15, 2022, the Committee on Information Technology ("COIT") and its Privacy and Surveillance Advisory Board conducted two public hearings at which they considered HSA's Surveillance Impact Report for social media management software and developed a Surveillance Technology Policy for HSA's use of social media management software.

On September 15, 2022, COIT voted to recommend that the Board of Supervisors adopt HSA's Surveillance Technology Policy for the use of social media management software.

n:\legana\as2023\2300245\01671581.docx



Committee on Information Technology

Office of the City Administrator

To: Members of the Board of Supervisors

From: Carmen Chu, City Administrator

Jillian Johnson, Director, Committee of Information Technology

Date: May 1, 2023

Subject: Legislation introduced to approve Surveillance Technology Policy for the Human Services Agency's Social Media Management Software

In compliance with Section 19B of the City and County of San Francisco's Administrative Code, the City Administrator's Office is pleased to submit the Surveillance Technology Policy for the Human Services Agency's Social Media Management Software.

To engage the public in discussion on the role of government surveillance, the Committee on Information Technology (COIT) and its subcommittee the Privacy and Surveillance Advisory Board (PSAB) held 2 public meetings between August and September 2022 to review and approve the policy. All details of these discussions are available at sf.gov/coit.

The following page provides greater detail on the review process for the Surveillance Technology Policy, and COIT's recommended course of action.

If you have questions on the review process please direct them to Jillian Johnson, Director of the Committee on Information Technology (COIT).

Social Media Management Software

Department	Authorized Uses
Human Services Agency	<ol style="list-style-type: none"> 1. Plan and execute more effective and strategic campaigns across social media platforms. 2. Schedule multiple social media posts in advance. 3. Create and publish/post multiple streams of content across various social media platforms. 4. Maintain active social media presence that is automated, specifically on weekends when staff is off. 5. Ensure consistency of messaging across all social media platforms. 6. Track post performance and analyze trends to improve content and strategy. 7. Monitor public posts for references to SFHSA’s social media presence and for specific search terms/“hashtags” related to SFHSA’s work in the community. 8. Access and respond to correspondence sent through social media platforms 9. Create reports.

Social Media Management Software Public Meeting Dates

Date	Meeting
August 26, 2022	Privacy and Surveillance Advisory Board (PSAB)
September 15, 2022	Committee on Information Technology (COIT)

COIT recommends the following action be taken on the policy:

- Approve the Social Media Management Software Surveillance Technology Policy for the Human Services Agency.



Surveillance Technology Policy

Social Media Management Software,
San Francisco Human Services Agency

The City and County of San Francisco values privacy and protection of San Francisco residents’ civil rights and civil liberties. As required by San Francisco Administrative Code, Section 19B, the Surveillance Technology Policy aims to ensure the responsible use of social media management software itself as well as any associated data, and the protection of City and County of San Francisco residents’ civil rights and liberties.

PURPOSE AND SCOPE

The Department’s mission is the following: We are committed to delivering essential services that support and protect people, families, and communities. We partner with neighborhood organizations and advocate for public policies to improve well-being and economic opportunity for all San Franciscans. The San Francisco Human Services Agency (SFHSA) Communication Division’s mission is to effectively convey information about the vital services that support and protect the people, families, and communities of San Francisco. Our team is responsible for informing San Franciscans of relevant program updates and information, while presenting this information in a timely and highly accessible manner.

The Surveillance Technology Policy (“Policy”) defines the manner in which the social media management software will be used to support this mission, by describing the intended purpose, authorized and restricted uses, and requirements.

This Policy applies to all to department personnel that use, plan to use, or plan to secure social media management software, including employees, contractors, and volunteers. Employees, consultants, volunteers, and vendors while working on behalf of the City with the Department are required to comply with this Policy.

POLICY STATEMENT

The authorized use of social media management software technology for the Department is limited to the following use cases and is subject to the requirements listed in this Policy.

Authorized Use(s):

- | |
|--|
| <i>– Plan and execute more effective and strategic campaigns across social media platforms. Plan and execute more effective and strategic campaigns across social media platforms.</i> |
| <i>– Schedule multiple social media posts in advance</i> |
| <i>– Create and publish/post multiple streams of content across various social media platforms.</i> |

COIT Policy Dates

Approved:

– Maintain active social media presence that is automated, specifically on weekends when staff is off.
– Ensure consistency of messaging across all social media platforms.
– Track post performance and analyze trends to improve content and strategy.
– Monitor public posts for references to SFHSA’s social media presence and for specific search terms/“hashtags” related to SFHSA’s work in the community.
– Access and respond to correspondence sent through social media platforms
– Create reports.

Prohibited use cases include any uses not stated in the Authorized Use Case section.

Departments may use information collected from technology only for legally authorized purposes, and may not use that information to unlawfully discriminate against people based on race, ethnicity, political opinions, religious or philosophical beliefs, trade union membership, gender, gender identity, disability status, sexual orientation or activity, or genetic and/or biometric data. Additionally, departments may not use automated systems to scan footage and identify individuals based on any of the categories listed in the preceding sentence.

BUSINESS JUSTIFICATION

Social media management software supports the Department’s mission and provides important operational value in the following ways:

Social media management software is essential to helping the SFHSA Communications team increase awareness and understanding of the many SFHSA programs with a wider audience. Social media management software will be used to monitor our channels in real time, plan and schedule publication of content, and track public engagement and opinion. Most importantly, we will be able to track social media analytics, which will help us understand which messages resonate most with our audience, helping us refine our communications strategy. Social media management software will allow us to be more efficient and strategic in achieving our mission of informing our clients about vital program information.

In addition, Social media management software promises to benefit residents in the following ways:

Benefit	Description
X Education	Through social media management software we would be able to publish content in a quick and streamlined manner to help our audience better understand the benefits/services/programs that are available to them. In doing so, we help educate our audience about specific program information and critical updates.

X	Community Development	Through the social media management software we can build a community by informing San Franciscans of relevant and local events open to the public, and encourage others to send us any questions they may have about the benefits/services/programs that are available.
X	Health	Through the social media management software's monitoring feature, we can stay up to date on any critical and time-sensitive health and safety information/news, like the COVID-19 health orders that are shared by the San Francisco Health Department or the San Francisco Department of Emergency Management. We would also be able to publish and plan content about our health and safety related programs. SFHSA also relies on social media to inform the public on the occasion when a location must shut down due to a power outage, emergency evacuation or other public safety events.
X	Environment	Through the social media management software's monitoring feature, we can become aware of any local weather-related news or new/relevant environmental guidelines that we can share with our audience to keep them informed. For example, if there are heavy storms that will impact San Franciscans, we can share safety messages.
<input type="checkbox"/>	Criminal Justice	
X	Jobs	Through the social media management software's content publishing feature, we can schedule job postings and share information about social programs available to connect individuals to jobs.
X	Housing	Through the social media management software's monitoring feature, we can monitor what our sister agency, the Department of Homelessness and Supportive Housing, is publishing and share important updates on any emergency shelters available, or programs that are available to San Franciscans who need housing.
X	Public Safety	See: Health section.
<input type="checkbox"/>	Other	

Social media management software will benefit the department in the following ways:

Benefit	Description
Financial Savings	

X Time Savings Staff time to manually input social media posts into individual social media platforms represents a savings of 8 hours a week or 32-40 hours per month

Staff Safety

X Data Quality Currently, SFHSA must mine social media data on engagement via each platform, which is laborious and inefficient. Social media management software will allow data to be mined and analyzed in a much more efficient and effective manner (often in real-time).

Other

To achieve its intended purpose, social media management software (also referred to below as “surveillance technology”) allows users to create custom views of all connected social networks. Social media management software can be used to post to multiple social media accounts, manage social media messaging, and coordinate the organization’s social media marketing. The software aggregates social media feeds so that content and trends can be viewed holistically.

POLICY REQUIREMENTS

This Policy defines the responsible data management processes and legally enforceable safeguards required by the Department to ensure transparency, oversight, and accountability measures. Department use of surveillance technology and information collected, retained, processed or shared by surveillance technology must be consistent with this Policy; must comply with all City, State, and Federal laws and regulations; and must protect all state and federal Constitutional guarantees.

Specifications: The software and/or firmware used to operate the surveillance technology must be up to date and maintained.

Safety: Surveillance technology must be operated in a safe manner. Surveillance technology should not be operated in a way that infringes on resident civil rights, including privacy, or causes personal injury or property damage.

Data Collection: Department shall only collect data required to execute the authorized use cases. All data collected by the surveillance technology, including PII, shall be classified according to the City’s [Data Classification Standard](#).

The surveillance technology collects some or all of the following data type(s):

<i>Data Type(s)</i>	<i>Format(s)</i>	<i>Classification</i>
---------------------	------------------	-----------------------

Social media references	Uniform resource locator (URL)	Level 1
Social media post aggregate statistics	Numeric statistics on post performance, e.g. number of likes, shares, views	Level 2
Correspondence sent and received through social media platforms	Format depends on the media types supported by the social media platform, e.g. text, photo, video, etc.	Level 2

Access: All parties requesting access must adhere to the following rules and processes:

- Onboarding and training, including a written social media guidelines document, to advise employees of appropriate and prohibited use.

A. Department employees

Once collected, the following roles and job titles are authorized to access and use data collected, retained, processed or shared by the surveillance technology:

- 9251 Public Relations Manager (1)
- 9252 Communications Specialist (1)
- 0932 Communications Director (1)

B. Members of the public

The Department will comply with the California Public Records Act, the San Francisco Sunshine Ordinance, the requirements of the federal and State Constitutions, and applicable federal and State laws and regulations for retention and public access.

Collected data that is classified as Level 1-Public data may be made available for public access or release via DataSF's [Open Data](#) portal. Open Data has a Public Domain Dedication and License, and makes no warranties on the information provided. Once public on Open Data, data can be freely shared, modified, and used for any purpose without any restrictions. Any damages resulting from use of public data are disclaimed.

Members of the public may also request access by submission of a request pursuant to San Francisco's [Sunshine Ordinance](#). No record shall be withheld from disclosure

in its entirety unless all information contained in it is exempt from disclosure under express provisions of the California Public Records Act or some other statute.

Data Security: Department shall secure PII against unauthorized or unlawful processing or disclosure; unwarranted access, manipulation or misuse; and accidental loss, destruction, or damage. Surveillance technology data collected and retained by the Department shall be protected by the safeguards appropriate for its classification level(s).

To protect surveillance technology information from unauthorized access and control, including misuse, Departments shall apply the following safeguards:

Login information will be stored in a password-secured file. SFHSA will implement a two-factor authentication process.

Data Sharing: The Department will endeavor to ensure that other agencies or departments that may receive data collected by social media management software will act in conformity with this Policy.

For internal and externally shared data, shared data shall not be accessed, used, or processed by the recipient in a manner incompatible with the authorized use cases stated in this Policy.

The Department shall ensure proper administrative, technical, and physical safeguards are in place before sharing data with other CCSF departments, outside government entities, and third-party providers or vendors. (See *Data Security*)

The Department shall ensure all PII and restricted data is de-identified or adequately protected to ensure the identities of individual subjects are effectively safeguarded.

Further, in sharing data, processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying an individual person, data concerning health or data concerning an individual person's sex life or sexual orientation shall be prohibited.

Each department that believes another agency or department receives or may receive data collected from its use of surveillance technologies should consult with its assigned deputy city attorney regarding their response.

Before sharing data with any recipients, the Department will use the following procedure to ensure appropriate data protections are in place:

- X Confirm the purpose of the data sharing aligns with the department's mission.
- X Consider alternative methods other than sharing data that can accomplish the same purpose.
- X Redact names and ensure all PII is removed in accordance with the department's data policies.

- X Review of all existing safeguards to ensure shared data does not increase the risk of potential civil rights and liberties impacts on residents.
- X Evaluation of what data can be permissibly shared with members of the public should a request be made in accordance with the San Francisco's Sunshine Ordinance.
- X Ensure data will be shared in a cost-efficient manner and exported in a clean, machine-readable format.

The Department will comply with the California Public Records Act, the San Francisco Sunshine Ordinance, the requirements of the federal and State Constitutions, and applicable federal and State laws and regulations.

The Department currently participates in the following sharing practices:

A. Internal Data Sharing

The department does not share surveillance technology data with other departments or entities inside the City and County of San Francisco.

B. External Data Sharing

The department does not share surveillance technology data externally with entities outside the City and County of San Francisco.

Data Retention: Department may store and retain raw PII data only as long as necessary to accomplish a lawful and authorized purpose.

The Department's data retention period and justification are as follows:

Retention Period	Retention Justification
<ul style="list-style-type: none"> • General/Administrative: Correspondence, miscellaneous - 2 years • General/Administrative: Statistical - 5 years 	<p>SFHSA posts and performance reports are considered business data subject to Sunshine and public records laws and are retained according to those requirements.</p>

Data will be stored in the following location:

- Local storage (e.g., local server, storage area network (SAN), network attached storage (NAS), backup tapes, etc.)
- Department of Technology Data Center
- X Software as a Service Product
- Cloud Storage Provider

Data Disposal: Upon completion of the data retention period, Department shall dispose of data in the following manner:

Practices:

- On a monthly basis, reports will be reviewed for data retention expiration. Files no longer subject to the data retention period will be deleted.

Processes and Applications:

- Deleting the report removes all data from the local machine or network

Training: To reduce the possibility that surveillance technology or its associated data will be misused or used contrary to its authorized use, all individuals requiring access must receive training on data security policies and procedures.

At the very least, department shall require all elected officials, employees, consultants, volunteers, and vendors working with the technology on its behalf to read and formally acknowledge all authorized and prohibited uses. Department shall also require that all individuals requesting data or regularly requiring data access receive appropriate training before being granted access to systems containing PII.

Training is needed to learn how to use the service:

- How to create and schedule posts
- How to examine the analytical statistics for a post
- How to set up tracking for a keyword or hashtag
- How to review tracked mentions and conversations
- How to review and respond to direct messages

COMPLIANCE

Department shall oversee and enforce compliance with this Policy using the following methods:

- SFHSA will require staff to read and acknowledge all authorized and prohibited uses.
- The Communications Director (0932) will be responsible for oversight of policy as applied to social media management software.

Department shall be assigned the following personnel to oversee Policy compliance by the Department and third-parties.

- **Communications Director (0932)**

Sanctions for violations of this Policy include the following:

- First Offense: Staff who use the platform inappropriately will receive initial counseling on appropriate use of social media within the organization.
- Second Offense: Staff will be put on probation for 3 months from using the platform.
- Third Offense: Staff will be prohibited from using the platform.

If a Department is alleged to have violated the Ordinance under San Francisco Administrative Code Chapter 19B, Department shall post a notice on the Department’s website that generally describes any corrective measure taken to address such allegation.

Department is subject to enforcement procedures, as outlined in San Francisco Administrative Code Section 19B.8.

EXCEPTIONS

Only in exigent circumstances or in circumstances where law enforcement requires surveillance technology data for investigatory or prosecutorial functions may data collected, retained or processed by the surveillance technology be shared with law enforcement.

DEFINITIONS

Personally Identifiable Information: Information that can be used to distinguish or trace an individual’s identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual.

Raw Data: Information collected by a surveillance technology that has not been processed and cleaned of all personal identifiable information. The distribution and use of raw data is tightly restricted.

Exigent Circumstances: An emergency involving imminent danger of death or serious physical injury to any person that requires the immediate use of Surveillance Technology or the information it provides.

AUTHORIZATION

Section 19B.4 of the City’s Administrative Code states, “It is the policy of the Board of Supervisors that it will approve a Surveillance Technology Policy ordinance only if it determines that the benefits the Surveillance Technology ordinance authorizes outweigh its costs, that the Surveillance Technology Policy ordinance will safeguard civil liberties and civil rights, and that the uses and deployments of the Surveillance Technology under the ordinance will not be based upon discriminatory or viewpoint-based factors or have a disparate impact on any community or Protected Class.”

QUESTIONS & CONCERNS

Public:

Complaints or concerns can be submitted to the Department by:

Complaints or concerns can be submitted to the Department by email at HSACommunications@sfgov.org.

Department shall acknowledge and respond to complaints and concerns in a timely and organized response. To do so, Department shall:

Multiple staff monitor the HSA Communications mailbox to ensure that messages are received and responded to within one business day.

City and County of San Francisco Employees:

All questions regarding this policy should be directed to the employee's supervisor or to the director. Similarly, questions about other applicable laws governing the use of the surveillance technology or the issues related to privacy should be directed to the employee's supervisor or the director.



Surveillance Impact Report

Social media management software
San Francisco Human Services Agency

As required by San Francisco Administrative Code, Section 19B, departments must submit a Surveillance Impact Report for each surveillance technology to the Committee on Information Technology ("COIT") and the Board of Supervisors.

The Surveillance Impact Report details the benefits, costs, and potential impacts associated with the Department's use of social media management software.

DESCRIPTION OF THE TECHNOLOGY

The Department's mission is: We are committed to delivering essential services that support and protect people, families, and communities. We partner with neighborhood organizations and advocate for public policies to improve well-being and economic opportunity for all San Franciscans.

The San Francisco Human Services Agency (SFHSA) Communication Division's mission is to effectively convey information about the vital services that support and protect the people, families, and communities of San Francisco. Our team is responsible for informing San Franciscans of relevant program updates and information, while presenting this information in a timely and highly accessible manner.

In line with its mission, the Department uses social media management software to do the following:

Social media management software is essential to helping the SFHSA Communications team increase awareness and understanding of the many SFHSA programs with a wider audience.

Social media management software will be used to monitor our social media channels in real time, plan and schedule publication of content, and track public engagement and opinion. Most importantly, we will be able to track social media analytics, which will help us understand which messages resonate most with our audience, helping us refine our communications strategy. Social media management software will allow us to be more efficient and strategic in achieving our mission of informing our clients about vital program information.

The Department shall use social media management software only for the following authorized purposes:

Authorized Use(s):

- Plan and execute more effective and strategic campaigns across social media platforms.
- Schedule multiple social media posts in advance.
- Create and publish/post multiple streams of content across various social media platforms

Surveillance Oversight Review Dates

COIT Review: TBD

Board of Supervisors Review: TBD

- Maintain active social media presence that is automated, specifically on weekends when staff is off.
- Ensure consistency of messaging across all social media platforms.
- Track post performance and analyze trends to improve content and strategy.
- Monitor public posts for references to SFHSA's social media presence and for specific search terms/"hashtags" related to SFHSA's work in the community
- Access and respond to correspondence sent through social media platforms
- Create reports.

Prohibited use cases include any uses not stated in the Authorized Use Case section.

Further, processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, gender, gender identity, disability status, or an individual person's sex life or sexual orientation, and the processing of genetic data and/or biometric data for the purpose of uniquely identifying an individual person shall be prohibited.

The technology may be deployed in the following locations, based on use case:

- N/A - Social media management software is not found in a physical location.

Technology Details

The following is an example product description for "Sprout Social" social media management software:

Sprout Social is a powerful solution for social media management. Understand and reach your audience, engage your community and measure performance with the only all-in-one social media management platform built for connection.

A. How It Works

To function, social media management software is a social network manager that allows users to create custom views of all connected social networks. Social media management software can be used to post to multiple social media accounts, manage social media messaging, and coordinate the organization's social media marketing. The platform aggregates social media feeds so that content and trends can be viewed holistically.

All data collected or processed by social media management software will be handled or stored by an outside provider or third-party vendor on an ongoing basis.

IMPACT ASSESSMENT

The impact assessment addresses the conditions for surveillance technology approval, as outlined by the Standards of Approval in San Francisco Administrative Code, Section 19B:

1. The benefits of the surveillance technology outweigh the costs.
2. The Department's Policy safeguards civil liberties and civil rights.

- 3. The uses and deployments of the surveillance technology are not based upon discriminatory or viewpoint-based factors and do not have a disparate impact on any community or Protected Class.

The Department’s use of the surveillance technology is intended to support and benefit the residents of San Francisco while minimizing and mitigating all costs and potential civil rights and liberties impacts of residents.

A. Benefits

The Department’s use of social media management software has the following benefits for the residents of the City and County of San Francisco:

X	Education	Through social media management software we would be able to publish content in a quick and streamlined manner to help our audience better understand the benefits/services/programs that are available to them. In doing so, we help educate our audience about specific program information and critical updates.
X	Community Development	Through social media management software we can build a community by informing San Franciscans of relevant and local events open to the public, and encourage others to send us any questions they may have about the benefits/services/programs that are available.
X	Health	Through social media management software monitoring features, we can stay up to date on any critical and time-sensitive health and safety information/news, like the COVID-19 health orders that are shared by the San Francisco Health Department or the San Francisco Department of Emergency Management. We would also be able to publish and plan content about our health and safety related programs. SFHSA also relies on social media to inform the public on the occasion when a location must shut down due to a power outage, emergency evacuation or other public safety events.
X	Environment	Through social media management software monitoring features, we can become aware of any local weather-related news or new/relevant environmental guidelines that we can share with our audience to keep them informed. For example, if there are heavy storms that will impact San Franciscans, we can share safety messages
<input type="checkbox"/>	Criminal Justice	
X	Jobs	Through social media management software content publishing features, we can schedule job postings and share information about social programs available to connect individuals to jobs

X Housing

Through social media management software monitoring features, we can monitor what our sister agency, the Department of Homelessness and Supportive Housing, is publishing and share important updates on any emergency shelters available, or programs that are available to San Franciscans who need housing.

Other: Public Safety

See: Health section

B. Civil Rights Impacts and Safeguards

The Department has considered the potential impacts and has identified the technical, administrative, and physical protections as mitigating measures:

The department addresses the following potential civil rights/liberties as follows:

- Dignity Loss: we train our department on best practices for maintaining an individual's confidentiality through our social media channels. We do not share confidential information or information/images that will have an ill-effect on individuals.
- Economic Loss: as a standard policy, we do not share or request confidential information through our social media channels.
- Loss of Autonomy: as a standard policy, we do not share or request confidential information through social media channels. If an individual shares their personal information, we ask for their consent on sharing the information with the appropriate case workers (if applicable) and redirect conversations to appropriate, confidential channels.
- Loss of Trust: as a standard practice, we always obtain an individual's consent before sharing information about them (for example, if we're sharing a quote about a staff member about their experience working at SFHSA, or a quote from a client about their experience participating in a program). If the individual later decides they want that content to be removed from our channels, we immediately take action and remove that content.

SFHSA strives to mitigate all potential civil rights impacts through responsible technology and data use policies and procedures, and intends to use social media monitoring software exclusively for aforementioned authorized use cases. All other uses are prohibited.

Through social media management software, SFHSA only has access to posts that have been published by the social media users. Public posts include timelines and posts from public accounts. SFHSA does not have access to private direct messaging, or messages between private accounts that do not belong to SFHSA, or payments. SFHSA will not utilize geographic tags added by users to postings or commenter demographics to track or intercept residents, nor will SFHSA access such posts with the intention to maliciously surveil, track or monitor its residents.

The administrative safeguards are: Prior to granting account credentials the communications director will counsel authorized users of the technology on appropriate and inappropriate use, as documented in the "Human Services Agency Social Media Policy and Guidelines for HSA Staff."

The technical safeguards are: Access to the social media management software console will be controlled using the following safeguards:

- Only authorized staff in the SFHSA Communications Division will receive credentials to the console.
- Individual staff will each receive unique credentials (no credential sharing).
- Credentials will consist of username, password, and 2FA token (TOTP).
- Access to SFHSA’s account on social media management software will be restricted to SFHSA’s public IP address.
- Control will be implemented preventing account invitations from being sent to any email domain other than @sfgov.org.

SFHSA will select a social media management software provider that can successfully complete a city Cybersecurity Risk Assessment and scores highly in the social media management space.

The physical safeguards are: SFHSA will select a social media management software provider that has extensive physical safeguards for their service.

C. Fiscal Analysis of Costs and Benefits

The Department’s use of social media management software yields the following business and operations benefits:

Benefit	Description
Financial Savings	
X	Time Savings
	Staff time to manually input social media posts into individual social media platforms represents a savings of 8 hours a week or 32-40 hours per month.
Staff Safety	
X	Data Quality
	Currently SFHSA must mine social media data on engagement via each platform, which is laborious and inefficient. social media management software will allow data to be mined and analyzed in a much more efficient and effective manner (often in real-time).
Other	

The fiscal cost, such as initial purchase, personnel and other ongoing costs, include:

Number of FTE (new & existing)	The technology does not require additional FTE; however, it will be supported by one (1) FTE (9252 - Communications Specialist) who will utilize the technology approximately 20% of a typical work week. No IT support is anticipated.	
Classification	<ul style="list-style-type: none"> • 9251 Public Relations Manager (1) • 9252 Communications Specialist (1) • 0932 Communications Director (1) 	
	Annual Cost	One-Time Cost
Total Salary & Fringe	<p><i>One staff member will typically be responsible for using the technology, among other duties. The total salary and fringe for this individual is \$157,028.</i></p> <p><i>However, only approximately 20% of this individual's time will be spent utilizing this technology, which amounts to \$31,406.</i></p> <p><i>This represents a savings of approximately the same amount (\$31,000), as this technology is anticipated to allow the staff member to spend roughly half the time managing social media accounts than they would spend without the technology.</i></p>	
Software	\$1723.80	
Hardware/Equipment		
Professional Services		

Training		
Other		
Total Cost	\$33,129.80	None

The Department funds its use and maintenance of the surveillance technology through the General Fund.

COMPARISON TO OTHER JURISDICTIONS

Social media management software is currently utilized by other governmental entities for similar purposes.

BOARD of SUPERVISORS



City Hall
1 Dr. Carlton B. Goodlett Place, Room 244
San Francisco 94102-4689
Tel. No. (415) 554-5184
Fax No. (415) 554-5163
TDD/TTY No. (415) 554-5227

MEMORANDUM

TO: Linda Gerull, Executive Director, Department of Technology

FROM: Victor Young, Assistant Clerk

A handwritten signature in black ink that reads "Victor Young".

DATE: June 9, 2023

SUBJECT: LEGISLATION INTRODUCED

The Board of Supervisors' Rules Committee received the following proposed legislation:

File No. 230689

Ordinance approving Surveillance Technology Policy for Human Services Agency use of social media management software.

If you have comments or reports to be included with the file, please forward them to me at the Board of Supervisors, City Hall, Room 244, 1 Dr. Carlton B. Goodlett Place, San Francisco, CA 94102 or by email at: victor.young@sfgov.org.

cc: Karen Hong Yee, Department of Technology