Surveillance Technology Policy

Social Media Monitoring Software
Fire Department

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 Monitoring Software itself as well as any associated data, and the protection of City and County of San Francisco residents' civil rights and liberties.

This Surveillance Technology Policy applies to the use of social media monitoring software and technology by the Fire Department.

PURPOSE AND SCOPE

The Surveillance Technology Policy ("Policy") defines the manner in which the surveillance technology will be used to support the missions of the Fire Department, hereby referred to as "the Department", by describing the intended purpose, authorized and restricted uses, and requirements.

This Policy applies to all Department personnel that use, plan to use, or plan to secure Social Media Monitoring Software, (hereinafter referred to as "surveillance technology"), including employees, contractors, and volunteers. The only areas of the policy that 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 the surveillance technology for the Department is limited to the following use cases and is subject to the requirements listed in this Policy.

Authorized Use(s):

– *Publish the Department's content on social media*
– *Communicate with social media users about Department news and share information on services offered through various social media channels*
– *Analyze data gathered from social media sources and print media to assess the effectiveness of outreach and optimize messaging to the public to achieve the Department's communication objectives*
– *Respond to social media users' posts about possible emergencies, fire code violations, and other situations in the purview of the Fire Department.*

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

Surveillance Oversight Review Dates
PSAB Review: 8/24/2023
COIT Review: TBD
Board of Supervisors Approval: TBD

Department 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.

BUSINESS JUSTIFICATION

Reason for Technology Use

The surveillance technology supports the Department's missions by allowing the Department to communicate with members of the public, including City residents, workers, and visitors, about city services on platforms which the public already uses. By employing social media monitoring technology to aggregate data and communicate across social media platforms, the technology allows Department to quickly communicate a consistent message across platforms, respond to constituent concerns in a timely manner, use post engagement information to strategize on the most effective way to reach specific audiences, and collect vital information on the public's concerns and need for government services.

Description of Technology

A social media monitoring technology is a technology from which a department can review all their social media accounts in one place, search all accounts and public content at once by typing in key words through a dashboard interface, schedule posts in advance on social media platforms and analyze the engagement with those posts. While the specific functions of each tool may vary, the technology often allows conversations to be labeled for later reference and can save content posted to social media platforms by other users. Search terms can be saved so that they can be repeated in the future, supporting customized monitoring across social media platforms.

Examples of social media monitoring technologies potentially used by the Department include:

- AgoraPulse
- Archive Social
- Buffer
- Critical Mention
- Falcon/ Brandwatch
- Hootsuite
- Later.com
- Meltwater
- Meta Business Manager and Meta Business Suite
- Sendible
- Sprout Social
- Tweetdeck

Resident Benefits

The social media monitoring software allows the Department to communicate with the public about services and programs offered by the Department, improving the accessibility of these services.

The distinct services provided by the Department, made more accessible through the surveillance technology, include the following benefits:

Benefit	Description
Education	The technology allows the department to inform the public about city and county – provided programs, services, facilities and or benefits using social media services that the public already uses.
Community Development	The technology allows the department to communicate with San Francisco residents about city and county-provided programs, services, facilities, and/or benefits. It also allows the department to gather community feedback via social media engagement by residents with the department's social media accounts.
Public Safety	The technology allows the department to quickly respond to questions/problems raised by residents in multiple public forums.

Department Benefits

The surveillance technology will benefit the department in the following ways:

Benefit	Description
Financial Savings	The social media monitoring software presents financial benefits by reducing the number of staff assigned to the Department's social media work.
Time Savings	The social monitoring software helps the Department save time by allowing social media management with fewer staff members than would be needed if the software was not being used.

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.

Data Collection:

The 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):

Data Type(s)	*Format(s)*	*Classification*
Social media handles, profiles, and posts (which can include name, date of birth, age, location, marital and employment status)	HTML, JPG, PNG, GIF, MOV, MP3, MP4.	Level 1-3
Biometric information, insofar that it is captured by the social media platform, e.g., Facebook and Instagram.	HTML, JPG, PNG, GIF, MOV, MP3, MP4.	Level 3

Access:

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

- **Training:** The Department will train their staff with access to the social media monitoring technology on how to properly use the technology, which will include information from the manufacturer on how to use their technology as well as information about this surveillance technology policy and the authorized use cases.
- **Documented Guidelines:** The Department will create a written social media guideline document for the reference of their employees regarding appropriate and prohibited uses, information about the data lifecycle for the technology, and a discussion of how to avoid any applicable civil liberties concerns.

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:

- H039 - Fire Captain - Public Information Officer (1)

B. Members of the public

Department will comply with the California Public Records Act, the San Francisco Sunshine Ordinance, the requirements of the federal and State Constitutions, and federal and State civil procedure laws and rules.

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.

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.

Department shall require all elected officials, employees, consultants, volunteers, and vendors working with the technology on its behalf to read and confirm that they understand all authorized and prohibited uses dictated by this policy. 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.

More specifically, Department training will include:

All department staff with authorized access to the technology will receive training on how to use the social media monitoring technology, including information on data security best practices.

Data Security: Surveillance technology data collected and retained by the Department shall be protected by the safeguards appropriate for its classification level(s) as defined by the National Institute of Standards and Technology (NIST) security framework 800-53, or equivalent requirements from other major cybersecurity framework selected by the department. Access to the surveillance technology will be restricted to only necessary department personnel and will be monitored by the department for misuse, either by city and county staff or by external malicious actors.

Department shall ensure compliance with these security standards through the following:

Only necessary department personnel will have access to the social media monitoring technology login information. Only software with encryption will be used. No sensitive information or Personally Identifiable Information ("PII") should be solicited through the social media monitoring technology by the department.

Data Storage: The Department included in this policy may store information in one or more of the following ways: Cloud Storage Provider, DT Data Center, Local Storage, and/or Software as a Service.

Data Sharing: The Department will endeavor to ensure that other agencies or departments that may receive data collected by the surveillance technology 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.

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)*

Department shall ensure all PII and restricted data is de-identified or adequately protected to ensure the identities of individual subjects are effectively safeguarded from entities that do not have authorized access under this policy.

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 legal obligations.

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

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

- Review of all existing safeguards to ensure shared data does not increase the risk of potential civil rights and liberties impacts on residents.
- 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.
- Ensure data will be shared in a cost-efficient manner and exported in a clean, machine-readable format.

The Department does not share data either internally with city and county departments or externally with entities outside of 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. Department data retention standards should align with how the department prepares its financial records and should be consistent with any relevant Federal Emergency Management Agency (FEMA) or California Office of Emergency Services (Cal OES) sections.

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

Retention Period	Retention Justification
A report summarizing the social media activity via the social media monitoring software's analysis is circulated to department leadership, who can view the document for a maximum of 30 days.	This is a monthly report and only needs to be retained until the next report is issued.

PII data shall not be kept in a form which permits identification of data subjects for any longer than is necessary for the purposes for which the personal data are processed.

Data Disposal:	Upon completion of the data retention period, Department shall dispose of data in the following manner: Any file that is downloaded from the social media monitoring software must be deleted in no longer than the maximum time allowed by the retention period. A department must check for these files on a regular basis and this process must be a part of the training that department employees authorized to use the surveillance technology are given. All materials are deleted after the requisite retention period.

COMPLIANCE

The Department are responsible for ensuring compliance with this policy within their own Department, and across third-party entities acting on their behalf.

Department Compliance

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

The department will conduct an annual review of technology policy and best practices to ensure compliance and will require training for all authorized personnel.

Interdepartmental, Intergovernmental & Non-Governmental Entity Compliance

To ensure that entities receiving data collected by the surveillance technology comply with the Surveillance Technology Policy, Department shall not share data with other entities.

Oversight Personnel

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

1070 - IS Project Director / 0941 - Chief Information Officer

Sanctions for Violations

Sanctions for violations of this Policy include the following:

- First offense: violator shall be verbally notified by Fire Department management of nature of violation.
- Second offense: violator shall be notified in writing of second offense and privileges to run queries in Critical Mention will be suspended for 30 days.
- Third offense: disciplinary action may be taken depending upon the severity of second/third offences.

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 Inquiries

Questions or complaints can be submitted through the Department website: https://sf-fire.org/report-fire-safety-concerns-complaints

Department shall acknowledge and respond to complaints and concerns in a timely and organized response, and in the following manner:

All comments received through the Department website are actively monitored and responded to within two weeks or less.

Inquiries from City and County of San Francisco Employees

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