# Surveillance Technology Policy

Social Media Monitoring Platform, such as Hootsuite
Public Library

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 Platform, such as Hootsuite 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 San Francisco Public Library system is dedicated to free and equal access to information, knowledge, independent learning and the joys of reading for our diverse community.

The Surveillance Technology Policy ("Policy") defines the manner in which the Social Media Monitoring Platform, such as Hootsuite 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 Monitoring Platform, such as Hootsuite, 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 Monitoring Platform, such as Hootsuite technology for the Department is limited to the following use cases and is subject to the requirements listed in this Policy.

*Authorized Use(s):*

- Plan and execute more effective and strategic campaigns across social media platforms.
- Schedule multiple social media posts in advance.
- Create and monitor multiple streams of content across various platforms.
- 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.
- 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 Monitoring Platform, such as Hootsuite supports the Department's mission and provides important operational value in the following ways:

HootSuite enables SFPL to plan, coordinate and schedule its social media postings, which inform the public about the abundance of free programs and resources the library offers. For example, the Library hosted approximately 18,000 public programs a year prior to the pandemic.

In addition, Social Media Monitoring Platform, such as Hootsuite promises to benefit residents in the following ways:

- **Information:** Hootsuite enables the Library to broadcast information about vital resources for the community such as free job, business and finance support; early literacy programs, including one-on-one tutoring; ESL courses; technology classes and access to other robust educational and research databases.
- **Education:** Residents indirectly benefit from SFPL using Hootsuite because it can better target social media outreach to raise visibility of City and Library services, which include free services like Career Online High School, digital, financial and career literacy workshops, early literacy programs such as storytimes and one-on-one tutoring.
- **Community Development:** Residents indirectly benefit from SFPL using Hootsuite because it can better target social media outreach to raise visibility of City and Library services. Additionally, our neighborhood branches provide a robust system of community hubs. Connecting neighborhood residents through public programming helps strengthen our communities and contributes to the City's resiliancy. For those who do not access traditional media, social media can be a critical tool to connect people to information and then to each other through participation in the Library's programs.
- **Public Safety:** Occasionally, library locations serve as Weather Relief Centers. Social media is one vehicle whereby we spread the word about these essential resources. The Library's social media also supports the larger citywide public safety messaging as evidenced during the pandemic year where the Library shared out key messages related to COVID and vaccine access. The Library also relies on social media to inform the public on the rare occasion when a location must shut down due to a power outage, emergency evacuation and other public safety events.
- **Jobs**: The Library promotes employment opportunities via social media as well as its free resources and programs that help and support people in their job searches.

Social Media Monitoring Platform, such as Hootsuite will benefit the department in the following ways:

- **Financial Savings:** Staff time to manually input social media posts into individual social media posts on days that fall outside the standard 40-hour work week (weekends) would likely require approximately 8 hours of overtime per week (32 hours per month).
- **Time Savings**: Staff time to manually input social media posts into individual social media platforms represents a savings of 15 hours a week (between at least 3 staff) or 60 hours per month.
- **Improved Data Quality**: Currently SPFL must mine social media data on engagement via each platform, which is laborious and inefficient. Hootsuite will allow data to be mined and analyzed in a much more efficient and effective manner (often in real-time).

To achieve its intended purpose, Social Media Monitoring Platform, such as Hootsuite, hereinafter referred to as "surveillance technology"), is a social network manager that allows users to create custom views of all connected social networks. HootSuite 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.

**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: Departments shall minimize the use, collection, and retention of Personally Identifiable Information (PII) to what is strictly necessary to accomplish the intended purpose of the surveillance technology.

Department shall only collect data required to execute the authorized use case. All data collected by the surveillance technology, including PII, shall be classified according to the City's Data Classification Standard.

Should information be incidentally collected that is not necessary to accomplish the intended purpose of the surveillance technology, including information that may be used to identify persons or private information, Department shall remove all incidental PII from raw data.

The surveillance technology collects the following data types:

- **Classified Data Types**: Social media handles and profiles, personal information (name, date of birth, age, and marital and employment status if included in social media profile); individual and group characteristics and biometric information such as facial recognition, in so far that it is captured by the social media platform, e.g., Facebook and Instagram.
- **Data Formats**: HTML, JPG, PNG, GIF, MOV, MP3, MP4.
- **Security Classification**: Level 1: Name, Social Media Handle, Social profile. Level 2 (Internal Use): Correspondence sent and received through HootSuite

None of the other categories (Sensitive Data, Protected Data and Restricted) would apply to HootSuite since it aggregates data which has already been made public on social media platforms.

Access: All parties requesting access must adhere to the following rules and processes (please refer to the data sharing section to ensure all information covered in that section is also included below):

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

Data must always be scrubbed of PII as stated above prior to public 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:

- 0952 - Deputy Director II (1)
- 9251 - Director of Communications (1)
- 1314 - Public Information Officer (1)
- 5330 - Graphics Supervisor (1)
- 5322 - Graphics Artist (2)
- 3610 - Library Assistant (1)
- 3632 - Librarian Manager (10)

*B. Members of the public, including criminal defendants*

The Public Library 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. Anyone, including criminal defendants, may access such data. 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, including by criminal defendants.

Members of the public, including criminal defendants, 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, at minimum, apply the following safeguards:

The Department of Human Resources Employee Handbook addresses Employee Use of City Resources and City Computers and Data Information Systems. The Department of Technology identifies Hootsuite as a City resource since both are accessible only through user logins created by account administrators.

Data Sharing: The Public Library will endeavor to ensure that other agencies or departments that may receive data collected by the Public Library's Hootsuite Policy 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 Public Library 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 Public Library 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, scrub faces, 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 Public Library 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.

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.

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

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

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: |
|---|---|
| • General/Administrative: Correspondence, miscellaneous - 2 years<br>• General/Administrative: Statistical - 5 years | The retention period is tied to the SFPL Records Retention and Destruction Policy https://sfpl.org/sites/default/files/2020-03/administration-records-retention-policy.pdf. |

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. PII data collected by the surveillance technology may be retained beyond the standard retention period only in the following circumstance(s):

- Data will not be retained beyond this period.

Departments must establish appropriate safeguards for PII data stored for longer periods.

Data will be stored in the following location:

HootSuite stores the data in its own cloud storage.

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

Practices:

- Reports generated typically download to a folder of temporary files, sometimes called "downloads" on individual devices. These folders are typically deleted by the user on a regular basis.

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.

No training is required.

**COMPLIANCE**

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

The Director of Communications and Public Information Officer will be responsible for monitoring the platform to ensure that staff do not violate the Library's social media policies.

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

- 9251 - Director of Communications
- 1314 - Public Information Officer

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. The Public Affairs team will also send periodic reminders to staff on best practices regarding appropriate use.
- Second Offense: Staff will be put on probation for 3 months from using the plaform.
- 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:

Members of the public can register complaints/concerns or submit questions in writing via the library's chat service, or "Comments and Suggestions" page online, or in person at the City Librarian's Office, Main Library, 100 Larkin Street, San Francisco 94102. They can also contact the library through telephone at 415-557-4400 or email at info@sfpl.org. All questions and complaints are forwarded to the proper SFPL division for appropriate and timely responses.

Members of the public can also contact the Public Affairs team at publicaffairs@sfpl.org.

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

Multiple staff monitor SFPL communications portals to ensure that members of the public receive a response within 24 hours.

*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.