



Surveillance Technology Policy

Social Media Monitoring Software
San Francisco Department of Elections

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.

PURPOSE AND SCOPE

The San Francisco Department of Elections ("Department of Elections", or "The Department") is dedicated to providing equitable access to voting and election-related services and to conducting free, fair, and functional elections for the City and County.

The Surveillance Technology Policy ("Policy") defines the manner in which Social Media Monitoring 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 Monitoring Software, 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 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):

- 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 days when staff is off.
- Ensure consistency of messaging across all social media platforms.
- Respond to questions and comments from members of the public.
- Track post performance and analyze trends to improve content and strategy, and optimize use of Department resources.
- Create reports.

COIT Policy Dates

PSAB Dates: 3/23/2023

COIT Dates: TBD

BOS Dates: TBD

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 Software supports the Department's mission and provides important operational value in the following ways:

Social Media Monitoring Software enables The Department of Elections to plan, coordinate and schedule its social media postings, which inform the public about voting options, grant applications for community-based organizations, redistricting information, registration information, Department operations, and employment opportunities.

In addition, Social Media Monitoring Software promises to benefit residents in the following ways:

- **Information:** Hootsuite enables the Department to broadcast information about general election topics such as voter registration, voting options (by mail and in-person), language services and translated materials, accessible voting services and tools, and ranked choice voting in local contests. In the months and weeks leading up to each election, Hootsuite will also assist the Department in publicizing information about election-specific topics such as upcoming deadlines, contests on the ballot, and opportunities for civic engagement such as elections process observation. Hootsuite will also enable the Department to further engage with City residents who choose to use social media as a source of information by using Hootsuite to publish print and digital publications, instructional videos, web tools, and details about the Department's in-person, telephone, and email customer service. Hootsuite's centralized platform will connect all of the Department's social media accounts, enabling Department staff to more quickly, efficiently, and effectively provide information, respond to questions, and engage with City residents.
- **Education:** San Francisco voters and all members of the public benefit indirectly from the Department of Elections' use of Social Media Monitoring Software, as its use bolsters election-operations literacy. Information disseminated on social media by the official accounts of the Department can help improve the public's understanding of how elections are administered, and dispel incorrect or misleading information about elections processes.

COIT Policy Dates

PSAB Dates: 3/23/2023

COIT Dates: TBD

BOS Dates: TBD

- **Community Outreach:** Hootsuite will enable the Department to optimize its Community Outreach efforts by promoting and strengthening collaboration with local community-based organizations and City agencies, facilitating equitable participation in electoral processes, and optimizing strategies to reach the City's most vulnerable voters and potential registrants. Residents will benefit from the use of Hootsuite because it will allow the Department to focus and target its outreach efforts to residents who would otherwise be less likely to engage with the democratic process, thus furthering the Department's equitable goals. Hootsuite will further improve the Department's ability to promote community outreach events and solicit feedback from City residents and communities on the accessibility of Department programs, services, resources, and tools.
- **Employment and Volunteer Opportunities:** Every election, the Department hires hundreds of temporary employees to help assist its year-round workforce and recruits thousands of volunteer poll workers who serve at one of the City's polling places on Election Day. The Department will promote these employment and volunteer opportunities via social media in an effort to build an equitable and inclusive workplace in which all employees and volunteers can thrive and succeed.

Social Media Monitoring Software 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, the Department must mine social media data via each platform, which is laborious and inefficient. Social Media Monitoring Software 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 Software, hereinafter referred to as "surveillance technology"), is a social network manager that allows users to create custom views of all connected social networks. Surveillance technology can be used to post to multiple social media accounts, manage social media messaging, respond to voters, and coordinate the Department'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 Social Media Software.

Social Media Monitoring Software 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 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)
- 1842 – Voter Support/Outreach Manager (2)
- 1840 – Voter Support/Outreach Lead (2)
- 1403 – Voter Support/Outreach Coordinator (2)

B. Members of the public, including criminal defendants

The Department of Elections will comply with the California Public Records Act, the San Francisco Sunshine Ordinance, the California Elections Code, 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. Additionally, the Department’s account on the Social Media Monitoring Software platform is only accessible through user logins created by account administrators within the Department.

Data Sharing: The Department of Elections will endeavor to ensure that other agencies or departments that may receive data collected by the Department’s Social Media Monitoring 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 of Elections 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 of Elections 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 Department of Elections will comply with the California Public Records Act, the San Francisco Sunshine Ordinance, the California Elections Code, 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:

<p>Retention Period:</p> <ul style="list-style-type: none">• General/Administrative: Correspondence, miscellaneous - 5 years• General/Administrative: Statistical - 5 years	<p>Retention Justification:</p> <p>The retention period is tied to the Department's Record Retention and Destruction Schedule.</p>
--	--

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.

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

Data will be stored in the following location:

Social Media Monitoring Software contractors, such as Hootsuite, shall store the data in their 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.

COMPLIANCE

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

The staff listed below will be responsible for monitoring the platform to ensure that staff do not violate the Department's social media policies.

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

- 1842 – Voter Support/Outreach Manager (2)
- 1840 – Voter Support/Outreach Lead (2)

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 administration team will also send periodic reminders to authorized Staff on best practices regarding appropriate use.
- 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:

Members of the public can register complaints/concerns or submit questions in writing via the Department's email SFVote@sfgov.org, by mail or in person at the Department of Elections, City Hall, 1 Dr. Carlton B. Goodlett Place., Room 48, San Francisco 94102. They can also contact the Department through telephone at 415-554-4375. All questions and complaints are forwarded to the proper division for appropriate and timely responses.

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

Monitor Department communications portals to ensure that members of the public receive a timely response.

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.