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):

– *Plan and execute more effective and strategic campaigns across social media platforms. Plan and execute more effective and strategic campaigns across social media platforms.*
– *Schedule multiple social media posts in advance*

Surveillance Oversight Review Dates
PSAB Review: Recommended on 08/26/2022
COIT Review: 09/15/2022
Board of Supervisors Approval: TBD

– *Create and publish/post multiple streams of content across various social media 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.*
– *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.
☐	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.
☐	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):

Data Type(s)	*Format(s)*	*Classification*

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**
• General/Administrative: Correspondence, miscellaneous - 2 years • General/Administrative: Statistical - 5 years	SFHSA posts and performance reports are considered business data subject to Sunshine and public records laws and are retained according to those requirements.

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 <u>not</u> 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.

Appendix A: San Francisco Human Services Agency (HSA) Social Media Policy & Guidelines for HSA Staff: Internal. Last Updated: January 2019.

San Francisco Human Services Agency (HSA)

Social Media Policy & Guidelines for HSA Staff

1. SOCIAL MEDIA MANAGEMENT

City and government officials of various departments, including the San Francisco Human Services Agency, have embraced social media as a means to improve openness, accessibility, and transparency. Strategic and proper use of social media helps us foster a positive relationship with the public and key audiences like customers, taxpayers/voters, overseers, government peers, and employees. Social media complements existing practices such as media relations, events, and internal communications. We have put together some core principles to help guide your participation in social media, both personally as well as when you are acting in an official capacity on behalf of HSA.

HSA Commitments:

1) HSA will be transparent in every social media engagement.
2) HSA will protect our client's privacy as it pertains to all laws, rules, and regulations.
3) HSA will reasonably monitor our behavior in the social media space, establish appropriate protocols, and keep appropriate records of our participation as dictated by law.

The HSA Communications staff is responsible for the content and upkeep of HSA's social media sites on the following channels:

1) Facebook
2) Twitter
3) Instagram
4) YouTube
5) LinkedIn

2. PERSONAL USE

All HSA employees may have personal social networking and social media sites. These sites should remain personal in nature and be used to share personal opinions or non-work related information. Following these principles will help ensure a distinction between sharing personal and HSA views. HSA employees must never use their HSA email account or password in conjunction with a personal social networking or social media site. Whether you are an authorized spokesperson or not, when speaking about our agency on your personal social networks, keep the following in mind:

- Use a disclaimer such as: "The postings on this site are my own and don't reflect or represent the opinions of the agency for which I work."
- State your name and, if relevant, role, when discussing HSA business.
- When you see posts or commentary on topics that require subject matter expertise about programs, policies, and/or statistics, please avoid the temptation to respond to these directly unless you respond with approved messaging from HSA. When in doubt, contact the Communications team: HSAcommunications@sfgov.org
- Protect yourself: Be careful about what personal information you share online.
- Honor our differences: HSA will not tolerate discrimination (including age, sex, race, color, creed, religion, ethnicity, sexual orientation, gender identity, national origin, citizenship, disability, marital status, or any other legally recognized protected basis under federal, state, or local laws, regulations or ordinances).

3. PROFESSIONAL USE

HSA employees must adhere to this policy when posting on any HSA social media and social networking site. Employees must not use official HSA social media or social networking sites for political purposes, to conduct private commercial transactions, or to engage in private business activities.

What You Should Never Disclose:

• Personal Information: The work and clientele that we serve is a highly personal and sensitive topic. Never share personal information about yourselves, our customers, cases, or projects.

• Legal Information: Anything to do with a legal issue, legal case, or attorneys without first checking with the Communications team or the City Attorney.

• Confidential Information: Do not publish, post, or release information that is considered confidential or for internal use only.

HSA employees should be mindful that inappropriate usage of official HSA social media and social networking sites can be grounds for immediate removal of administrative access and further discipline. If social media and social networking sites are used for official HSA business, the entire HSA site, regardless of any personal views, is subject to best practices guidelines and standards.

Only individuals authorized by HSA may publish content to an HSA website or social media page.

4. VIOLATIONS

Post Removal Policy and Retention Process

HSA's general practice is not to delete comments, even ones off-topic from the original post or critical of HSA's policies, procedures, or actions. No Authorized Account Administrator shall delete comments, posts, or other public interactions with Official HSA Social Media Accounts, unless the comment, post, or public interaction is in violation of the content standards as outlined in HSA's Social Media Policies.

In the event of violative content having to be hidden or removed, the Authorized Account Administrator will document the entirety of the original post and all removable content with screenshots or such means dictated by the HSA Communications Department Manager, before removal of the violative content. The Authorized Account Administrator will save records of violative content in an HSA network drive specified by the HSA Communications Director and will denote the date/time of removal.

No Authorized Account Administrator may block, mute, or otherwise prevent any users from following, viewing posts, having their posts viewed by HSA, or otherwise engaging with Official HSA Social Media Accounts.

Enforcement of the restrictions and prohibitions contained in these Social Media Policy shall be conducted by HSA in a fully content neutral fashion; whereby HSA shall not favor or disfavor any speech based on the speaker's position.

Violations of this policy include comments that:

- Use obscene, threatening, or harassing language.
- Promote discrimination on the basis of race, creed, color, age, religion, gender, marital status, status with regard to public assistance, national origin, physical or mental disability, or sexual orientation.
- Contain sexual content or links to sexual content.
- Contain demonstrably false statements of fact about HSA.
- Promote or advertise a business, or propose a commercial transaction.
- Promote or support political positions or campaigns, measures, or propositions.
- Violate a legal ownership interest of any party, such as trademarked or copyrighted material.
- Reveal information that may tend to compromise the safety or security of the public or public systems.
- Violate privacy by revealing classified or private personal information of the commenter's or someone else's, including home address, home or cell phone number, personal email address, or personal identification numbers.

4. PRIVACY & PERMISSIONS

Employees – whether posting to their own, third-party, or HSA social media sites – must never reveal classified or private personal information of another person, including home address, home or cell phone number, personal email address, or personal identification numbers.
Employees must obtain a signed, media consent release from any individual who permits use of their personal information or identifying images, videos, or audio recordings. Individuals under the age of 18 will need their legal guardian to sign the form. Contact HSAcommunications@sfgov.org for a copy of the HSA Media Release form.

5. OVERSIGHT & ENFORCEMENT

Employees representing HSA departments through HSA social media sites must maintain a high level of ethical conduct and professional decorum. Failure to do so is grounds for revoking the privilege to participate in HSA social media sites, blogs, or other social media features.
When presenting information, employees must uphold professional standards for good grammar, spelling, brevity, clarity and accuracy, and avoid jargon, obscure terminology, or acronyms.
HSA employees recognize that the content and messages they post on social media websites are public and may be cited as official HSA statements. Social media should not be used to circumvent other HSA communication policies.
All HSA social media shall be (1) approved by HSA Communications (2) published using approved social networking platforms and tools, and (3) administered by HSA Communications.

6. PUBLIC RECORDS DISCLOSURE

HSA social media sites are subject to the California Public Records Act. Any content maintained in a social media format that is related to City business may be a public record subject to public disclosure.
For Public Records Act requests or questions, email the HSA Sunshine Ordinance Officer at HSAsunshine@sfgov.org.

7. MORE INFORMATION

For questions or concerns regarding HSA social media sites and policy, contact HSAcommunications@sfgov.org.

Appendix B: San Francisco Human Services Agency (HSA) Social Media Policy & Guidelines: External. Last Updated: January 2019.

San Francisco Human Services Agency (HSA)

Social Media Policy & Guidelines

1. SOCIAL MEDIA MANAGEMENT

City and government officials of various departments, including the San Francisco Human Services Agency, have embraced social media as a means to improve openness, accessibility, and transparency. Strategic and proper use of social media helps us foster a positive relationship with the public and key audiences like customers, taxpayers/voters, overseers, government peers, and employees.
Social networks such as Facebook, Twitter, Instagram, and YouTube give the San Francisco Human Services Agency a cost-effective means for communicating with these audiences. Blog and video platforms allow any agency to connect with people on a more personal and easily understandable level. Social media complements existing practices such as media relations, events, and internal communications.

The HSA Communications staff is responsible for the content and upkeep of HSA's social media sites on the following channels:

6) Facebook
7) Twitter
8) Instagram
9) YouTube
10) LinkedIn

HSA's social media channels enable HSA to inform the public on topics including but not limited to HSA:

- News
- Programs
- Policies
- Services
- Emergency responses
- Events

2. GUIDELINES & MODERATION OF THIRD-PARTY CONTENT

HSA's social media sites serve as a *limited public forum* and all content published is subject to monitoring. HSA reserves the right to restrict or remove any content that is deemed in violation of this Social Media Policy or any applicable law. HSA Communications will make a determination about the appropriateness of comments

based on its application of this Social Media Policy & Guidelines, and that determination is final and not subject to outside review. HSA Communications will apply this Social Media Policy & Guidelines in a viewpoint neutral manner that is consistent over time. Any content removed based on these guidelines will be retained by the HSA Social Media Administrator for a reasonable period of time, including the time, date, and identity of the poster, when available.
Use of the above-listed social media sites is subject to the terms of use of those sites, including privacy policies. Any terms of service that those sites place on user participation apply to comments made by any user, and these sites may enforce their own terms of service.

3. VIOLATIONS

Post Removal Policy and Retention Process

HSA's general practice is not to delete comments, even ones off-topic from the original post or critical of HSA's policies, procedures, or actions. No Authorized Account Administrator shall delete comments, posts, or other public interactions with Official HSA Social Media Accounts, unless the comment, post, or public interaction is in violation of the content standards as outlined in HSA's Social Media Policies.

In the event of violative content having to be hidden or removed, the Authorized Account Administrator will document the entirety of the original post and all removable content with screenshots or such means dictated by the HSA Communications Department Manager, before removal of the violative content. The Authorized Account Administrator will save records of violative content in a HSA network drive specified by the SFHSA Communications Department Manager and will denote the date/time of removal.

No Authorized Account Administrator may block, mute, or otherwise prevent any users from following, viewing posts, having their posts viewed by HSA, or otherwise engaging with Official HSA Social Media Accounts.

Enforcement of the restrictions and prohibitions contained in this Social Media Policy shall be conducted by HSA in a fully content neutral fashion; whereby HSA shall not favor or disfavor any speech based on the speaker's position.

Violations of this policy include comments that:

- Use obscene, threatening, or harassing language.
- Promote discrimination on the basis of race, creed, color, age, religion, gender, marital status, status with regard to public assistance, national origin, physical or mental disability, or sexual orientation.
- Contain sexual content or links to sexual content.
- Contain demonstrably false statements of fact about SFHSA.
- Promote or advertise a business, or propose a commercial transaction.
- Promote or support political positions or campaigns, measures, or propositions.
- Violate a legal ownership interest of any party, such as trademarked or copyrighted material.
- Reveal information that may tend to compromise the safety or security of the public or public systems.
- Violate privacy by revealing classified or private personal information of the commenter's or someone else's, including home address, home or cell phone number, personal email address, or personal identification numbers.

4. PUBLIC RECORDS DISCLOSURE

HSA social media sites are subject to the California Public Records Act. Content maintained in a social media format that is related to City business may be a public record subject to public disclosure.
For Public Records Act requests, email the Sunshine Ordinance Officer, at HSAsunshine@sfgov.org.

5. DISCLAIMERS

HSA social media pages are not monitored 24/7. HSA is not responsible for comments by site visitors.

Content Standards Disclaimer

All Authorized Account Administrators shall ensure that Official HSA Social Media Accounts and SFHSA.org display the following statements regarding content standards in a location, or locations, appropriate for describing content standards when such location is available and reasonable:

"Please do not report emergencies on social media pages.
HSA reserves the right to remove and/or restrict inappropriate comments including those that violate the HSA Social Media Policy Guidelines found at https://www.sfhsa.org/about/media-center, comments which may reasonably interfere with, inhibit, or compromise law enforcement investigations, tactics, responses to incidents and/or the safety of law enforcement officers and staff.
Keep in mind that all posted comments are public records and subject to disclosure. Users of this site do not retain any rights over their postings. Postings are intended for public view and any information posted constitutes a waiver of any rights to privacy or confidentiality.
All social media platforms used by HSA are designated as Limited Public Forums"

6. MORE INFORMATION

For questions or concerns regarding HSA social media sites and policy, contact HSAcommunications@sfgov.org.