



# Surveillance Technology Policy

Body-Worn Cameras  
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 body-worn cameras 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 to protect the lives and property of the people of San Francisco and its visitors from fires, natural disasters, accidents, hazardous materials incidents, and other causes requiring a rapid and skilled response by land or water; serve the needs of its most vulnerable residents through community paramedicine, and save lives and reduce suffering by providing emergency medical services; prevent harm through prevention services and education programs; and to provide a work environment that is free from harassment and discrimination, and values health, wellness, cultural diversity, and equity.

The Surveillance Technology Policy ("Policy") defines the manner in which the body-worn cameras 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 body-worn cameras, 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 body-worn camera technology for the Department is limited to the following use cases and is subject to the requirements listed in this Policy.

### *Authorized Use(s):*

- Use by Public Information Officer (PIO) at large incidents to capture video of surroundings and the totality of the incident (currently in use)
- Used by Fire Investigators at scenes of fires to which they are dispatched (potential future use)

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,

## COIT Policy Dates

Approved:

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**

Body-worn cameras support the Department's mission and provides important operational value in the following ways:

This technology is a tool used by Department staff in front-line operational response, to improve aspects of the Department (such as training) that directly support the mission statement.

In addition, body-worn cameras promise to benefit residents in the following ways:

- Public Safety: The Department can review incidents for ways to improve response or training opportunities, which then can improve overall emergency response.

Body-worn cameras will benefit the department in the following ways:

- Potential Training Opportunities: Department staff could review video from an incident as part of an after-action review to give points and potential training points for future response improvements.

To achieve its intended purpose, body-worn cameras (hereinafter referred to as "surveillance technology") is worn by the SFFD member to capture video. It is turned off and on solely by the member when they arrive on-scene.

## **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: Faces or license plates - While it is intended to only capture the scene of a fire, there may inadvertently be faces or license plate captured on video.
- Data Format: MOV, AVI
- Data Security Classification: Level 2

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):

- Data must always be scrubbed of PII as stated above prior to public use. Access to data is limited to Department PIO and IT manager.

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:

- H-20 Lieutenant (1)
- 1070 IS Project Manager (1)

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

The Fire 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. 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:

Access to data is extremely limited, to only the SFFD PIO and one of the Department's IT managers. Data is stored remotely with a vendor, and would be scrubbed of PII if used.

**Data Sharing:** The Fire Department will endeavor to ensure that other agencies or departments that may receive data collected by the Fire Department's Body-Worn Cameras 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 Fire 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 Fire 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, 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 Fire 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.

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 purpose of the data sharing aligns with the department's mission.
- 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.
- Redact names\, scrub faces\, and ensure all PII is removed in accordance with the department's data policies.
- Review all existing safeguards to ensure shared data does not increase the risk of potential civil rights and liberties impacts on residents.

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 |
|------------------|-------------------------|
|------------------|-------------------------|

|   |   |
|---|---|
| <p>Data collected is uploaded to server and will be accessed as needed by the two members of the project team.</p> <p>The Department is currently undergoing a review of its data retention policy.</p> | <p>Per currently guidelines, direction has been for a one-year retention period based on State mandates, but that is under review to the best of our knowledge.</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. PII data collected by the surveillance technology may be retained beyond the standard retention period only in the following circumstance(s):

- Currently, given the low volume of data, this video data is stored indefinitely.

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

Data will be stored in the following location:

Cloud Storage Provider: Data is securely automatically uploaded to a cloud server, where it can be accessed.

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

Practices:

- Due to the small volume of data relative to other data, video is currently stored indefinitely on the vendor's server. The Department is currently working on an update to its data retention policy.

Processes and Applications:

- The vendor has a redaction assistant built into its software to assist with removal/blurring of PII. This specifically covers screens, faces and license plates automatically

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.

- Access is extremely limited, currently with two members. If there was to be an additional member granted access, they would need to be trained on using the vendor's system. This training would encompass accessing the vendor's system, as well as viewing and retrieving videos. Department members granted access are currently given informal Department training on the needs for removing PII in general. In addition, this technology has previously fallen under the Department's social media policy, so a review of that policy is required

## **COMPLIANCE**

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

Department shall assign the following personnel to oversee Policy compliance by the Department and third parties: Supervisor- Management of Information Services

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

- 1070 IS Project Director
- 0941 Manager VI

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 operate body-cam hardware shall be suspended for 60 days.
- Third offense: (following reinstatement of operator privileges): violator shall be permanently banned from body cam operations and 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 <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:

Department Members or the general public can register complaints/concerns or submit questions via calls or emails at 311.org, or to the Department directly at FireAdministration@sfgov.org or 415-558-3200.

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

- Department shall acknowledge and respond to complaints and concerns in a timely and organized response. To do so, the Department shall:
  - Constituent calls and complaints to the Fire Department are routed to the Program manager.
  - Program manager will discuss concerns or complaints with constituent and record details regarding nature of conversation.
  - If additional action is required or requested by caller, the Fire Department commits to a follow-up (by email or telephone) in a timely manner.
  - Program Manager, body cam operators, and Fire Department management shall review log of complaints on a quarterly basis to discuss best practices, evaluate for



learning lessons and opportunities to improve and refine the body cam use program based on caller complaints, concerns and other community feedback.

*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.