Surveillance Technology Policy

Fire Department
Unmanned Aircraft Systems (Drones)

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 Drones or Unmanned Aerial Vehicles 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: to protect the lives and property of the people of San Francisco from fires, natural disasters, and hazardous materials incidents; to save lives by providing emergency medical services; to prevent fires through prevention and education programs; and to provide a work environment that values health, wellness and cultural diversity and is free of harassment and discrimination.

The Surveillance Technology Policy ("Policy") defines the manner in which the Drones or Unmanned Aerial Vehicles 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 Drones or Unmanned Aerial Vehicles, 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 Drones or Unmanned Aerial Vehicles technology for the Department is limited to the following use cases and is subject to the requirements listed in this Policy.

Authorized Use(s):

1. Disaster Response: Assessment and District Surveys
2. Emergency Response: Building Fire Reconnaissance
3. Search & Rescue: Aerial or water borne drones.
4. Training: Assessment and evaluation of emergency response

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.

Surveillance Oversight Review Dates
COIT Review: July 17, 2020
Board of Supervisors Review: August 4, 2021

BUSINESS JUSTIFICATION

Drones or Unmanned Aerial Vehicles support the Department's mission and provides important operational value in the following ways:

The mission of the SFFD Drone Program is to facilitate saving lives and property, enhance Firefighter safety and improve emergency response actions by providing aerial reconnaissance and observation to the Incident Commander to support strategic and tactical decisions at emergencies, major incidents and/or disasters. The SFFD will use uniformed personnel or an authorized contractor to operate the Drone.

In addition, Drones or Unmanned Aerial Vehicles promise to benefit residents in the following ways:

X	Education	Drone imagery to promote Fire Department safety messaging and disaster preparedness
☐	Community Development	
☐	Health	
X	Environment	Drone imagery to identify any hazardous material response and mitigation
☐	Criminal Justice	
☐	Jobs	
☐	Housing	
X	Other	Public Safety: emergency response as indicated in authorized use cases

In addition, the following benefits are obtained:

Benefit		Description
X	Financial Savings	Drones can be far more time efficient and cost effective when conducting emergency response and gaining rapid situational awareness in a disaster.
X	Time Savings	Deploying a drone can provide time savings locating victims in a variety of environments as well as gain situational awareness and hazard assessment.
X	Staff Safety	Drones can be deployed to dangerous locations instead of personnel, such as rooftops, at the sides of building/bridges, along cliff areas or areas prone to erosion.
X	Data Quality	Some locations which are difficult to access by personnel may be more easily photographed using drone technology, thereby achieving better data.

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 kept 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 some or all of the following data types:

Data Type(s)	*Format(s)*	*Classification*
Photographic and video data (no audio) of assets, landscapes, etc.	JPEG, PNG, MOV, AVI, CSV	Level 2

Notification:	Departments shall notify the public of intended surveillance technology operation at the site of operations through signage in readily viewable public areas. Department notifications shall identify the type of technology being used and the purpose for such collection. Because of the urgent nature of fighting fires, Fire Department will likely not be able to implement public noticing. In these scenarios, Fire Department may implement public noticing after the fact or may seek other options of letting the public know about Drone use.

Department includes the following items in its public notice:

X Information on the surveillance technology

X Description of the authorized use

X Type of data collected

X Will persons be individually identified

X Data retention

X Department identification

X Contact information

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):

- Distinctive personal features or license plate information collected inadvertently (if any) will be blurred using an approved editing software prior to use or storage of images (drone "data") for any business purposes.

- Once PII have been obscured or removed from images, data may be used by department based on use cases identified above and may be stored on servers for future use. RAW (unedited) data shall not be used or retained.

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:

- Drone Program Manager, Fire Department Operations
- It is possible drone contractors may be retained as part of a professional services contract.

B. Members of the public

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: - Only authorized drone operators or MIS may access unedited data.
Data Sharing:	Fire Department will endeavor to ensure that other agencies or departments that may receive data collected by SFFD's Drone 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. 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) 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.

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.

The Fire Department will process raw data collected by drones as expeditiously as possible, removing or obscuring all PII. Only post-processed (i.e., "scrubbed") data will be maintained by the Fire Department per federal (FEMA) and state (OES) and local reimbursement and investigation requirements. Unedited data shall be deleted upon completion of processing.

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:

- The Fire Department will process raw data collected by drones as expeditiously as possible, removing or obscuring all PII. Only post-

processed (i.e., "scrubbed") data will be maintained by the Fire Department per federal (FEMA) and state (OES) and local reimbursement and investigation requirements. Unedited data shall be deleted upon completion of processing.

- Scrubbed data will adhere to the SFFD Records Management Policy. The Fire Department will consider images collected with surveillance technology as current records and, unless required for an ongoing investigation, they will be retained for period of 1 year.

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):

- N/A

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

Data will be stored in the following location:

X 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:

- Raw (unprocessed) data will be collected by the drone in the field, and stored on an onboard storage disc (i.e, "SD" card). Raw data (from the drone disc) will be downloaded from onboard storage disc onto secure Fire Department servers by Drone Data Editor.
- Once the subject image frames, still and/or video, have been identified for business needs, the Fire Department Data editor will review all selected frames and identify each instance of PII (faces or license plates). All instances of PII will be blurred or obscured using editing software, such that no recognizable human features or license plate information remain.
- After processing and saving of edited data, all raw data will be permanently erased. Before replacing the SD storage cards into the drone, data editor will ensure the discs are completely free of all data.

	Processes and Applications: All instances of PII will be blurred or obscured using editing software, such that no recognizable human features or license plate information remain.
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. Drone data collection and use shall be explained in Departmental Drone Policy. All authorized users must sign off on policy prior to use.

COMPLIANCE

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

- Drone Operators will be assigned to maintain updates and perform required maintenance. A procedural pre-mobilization and post-mobilization safety check will be performed at each operation.
- Department shall assign the following personnel to oversee Policy compliance by the Department and third-parties.
    - Supervisor- Management of Information Services

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 offence and privileges to operate drone hardware shall be suspended for 60 days.
- Third offense: (following reinstatement of operator privileges): violator shall be permanently banned from drone 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.
Sensitive Data:	Data intended for release on a need-to-know basis. Data regulated by privacy laws or regulations or restricted by a regulatory agency or contract, grant, or other agreement terms and conditions.
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:

Department Members of the 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:

Constituent calls and complaints to the Fire Department are routed to the Drone 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.

Drone Program Manager, drone operators, and Fire Department management shall review log on a quarterly basis to discuss best practices, evaluate for learning lessons and opportunities to improve and refine the drone 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.