Surveillance Technology Policy

Department of Technology
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 Unmanned Aerial Vehicle (UAV) or Drone Technology (referred to hereafter as "Drones") 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 of Technology's (DT's) mission is to: provide innovative, reliable, and secure business solutions that support and empower City agencies and departments in their delivery of high-quality government services for the public.

The Surveillance Technology Policy ("Policy") defines the manner in which the Drone technology 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 Drone technology, 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

Unmanned Aerial Vehicles and Drone 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. Drone technology is authorized for use during Video production, specifically the capture of video stills and photographs as elements of SFGovTV's video productions. The completed videos will be broadcast on SFGovTV's cable channels and made available on the station's YouTube account. Marketing and promotional videos created for other City departments may also feature drone footage or photographs.

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

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

The DT's video channel SFGovTV provides the public critical information about government and civic life program through cable channels and web streaming. Drone technology will allow SFGovTV to produce improved video programming. Specifically, drone technology will allow the station to capture video and still photographs as elements of the City video productions program.

In addition, unmanned aerial vehicles and Drone technology promises to benefit residents in the following ways:

☐	Education	
☐	Community Development	
☐	Health	
☐	Environment	
☐	Criminal Justice	
☐	Jobs	
☐	Housing	
X	Other	Civic Engagement SFGovTV's use of drone technology will allow residents to have an improved view of City operations and civic life.

In addition, the following benefits are obtained:

Benefit		Description
X	Financial Savings	Drones will be far more cost effective than alternative methods of original aerial photography. By mitigating the need for traffic control, expensive scaffolding/swing stage or other equipment, and other means that can be done manually, Drones will minimize labor costs.
X	Time Savings	Drones do not require as much time for set-up as other aerial alternatives.
X	Staff Safety	Drones expose staff to much less risk than alternatives such as constructing and climbing scaffolding or manned aircraft.
☐	Data Quality	

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. To ensure physical safety of the public, DT will operate drones in a manner consistent with the San Francisco Film Commission's guidelines for filming with a drone in all drone flight that is on, from, within and over City property. https://filmsf.org/filming-droneuas
Data Collection:	Department 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 1

Notification:	Department 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.

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):

1. 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.
2. 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 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.

1767 Media Production Specialist , Technology

B. Members of the public

Technology 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.

Data collected by surveillance technology will be made available to members of the public, including criminal defendants. Data can be accessed by the public in the following ways:

1. Scrubbed data will be available through channels and web streaming.

Anyone, including criminal defendants, may access such data.

	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 operator(s) and General Manager may access unedited data.
Data Sharing:	Technology will endeavor to ensure that other agencies or departments that may receive data collected by DT's Drones will act in conformity with this Surveillance Technology 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. Technology 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). Technology shall ensure all PII and restricted data is de-identified or adequately protected to ensure the identities of individual subjects are effectively safeguarded. 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 departments requesting data not-contained in programming via cablecast or video streaming, DT 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.

For Departments accessing data contained in programming via cablecast or video streaming, DT 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.
☐	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.
☐	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.
☐	Ensure data will be shared in a cost-efficient manner and exported in a clean, machine-readable format.

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:

Department shares the following data with the recipients:

- We anticipate that programming will be shared with various departments
- Data scrubbed of any inadvertently collected PII will be disclosed

Data sharing occurs at the following frequency: Continuously

B. External Data Sharing:

Department shares the following data with the recipients:

- Scrubbed data will be integrated in video programming. DT anticipates that video programming which includes video captured by drone will be publicly available through cable channels and web video streaming.

Data sharing occurs at the following frequency: Continuously.

To ensure that entities receiving data collected by the surveillance technology comply with the Surveillance Technology Policy, Department shall:

1. Raw data collected by drones will be scrubbed of any inadvertently collected PII as soon as possible and deleted as soon as possible.
2. Seek to delete metadata stored on the drone within 24 hours of capture and in all circumstances delete within 72 hours.

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:

- Raw data collected by drones will be scrubbed of any inadvertently collected PII as soon as possible and deleted as soon as possible.
- Programming using scrubbed data are considered permanent records and will be archived indefinitely.

Programming is intended as an enduring record of city operations.

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

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

☐ Software as a Service Product

X Cloud Storage Provider

Data Disposal:

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

1. 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 DT device. Still or video frames will be identified for use by the SFGovTV producer. Such data may include, as examples, images of buildings and structures, overhead images of topographic features.
2. Once the subject image frames, still and/or video, have been identified for business needs, the producer 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.
3. 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. With the exception of data shared through cable cast, web steaming or other distribution of programming, 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:

1. One individual with that has reviewed and signed the drone policy and received drone flight certification will be responsible for compliance with policies, procedures and record keeping.
2. Department shall assign the following personnel to oversee Policy compliance by the Department and third-parties:
    a. General Manager, SFGTV

Sanctions for violations of this Policy include the following:

- First offense: violator shall be verbally notified by DT management of nature of violation.
- Second offense: violator shall 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:

Complaints or concerns can be submitted to the Department:

Members of the public can register complains, concerns or ask questions by calling (415) 554-4188, emailing sfgovtv@sfgov.org or going to 311.org

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

- SFGovTV will monitor drone program related complaints and respond within two business days.

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.