Surveillance Technology Policy

Public Works
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 vehicles ("UAV" or "Drone" technology) 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: enhance the quality of life in San Francisco as responsible stewards of the public's physical assets by providing outstanding service in partnership with the community. We design, build, manage, maintain, green, protect and improve the City's public spaces (infrastructure, public right of way and facilities) with skill, pride, innovation, and responsiveness.

The Surveillance Technology Policy ("Policy") defines the manner in which the Unmanned aerial vehicles or 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 department personnel that use, plan to use, or plan to secure Unmanned aerial vehicles or Drone technology, including employees, suppliers, contractors, and volunteers while working on behalf of the City with the Department.

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. Disaster preparedness and response
2. Environmental monitoring and documentation
3. Inspect/Survey properties & assets
4. Project inspection and documentation
5. Surveying/Mapping data collection

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: TBD

BUSINESS JUSTIFICATION

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

1. In times of disaster preparedness or post-disaster mitigation, drones will provide critical emergency response functions such as logistical support for emergency routing, life safety, and cleanup efforts, not only assisting in protecting physical assets and public spaces but human life as well;
2. Drones will support the maintenance efforts of City-owned streets and trees pursuant to our mission of greening and improving City public spaces;
3. Drones will support the objective of maintaining city owned properties and landscapes by safely providing detailed photographic data and documentation to assist in the planning of corrective or new construction work by roofers, architects, engineers, electricians, PMs, CMs and other personnel.

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

X	Education	Drone imagery to promote Public Works projects and demonstrate use of tax dollars on projects.
▪	Community Development	
▪	Health	
X	Environment	Drone imagery to collect data on street-trees for maintenance and safety reasons.
▪	Criminal Justice	
▪	Jobs	
▪	Housing	
X	Other	Public Safety: to inspect tree canopies for damaged limbs (fall risks), to provide support when determining safety routes during emergencies, to collect data and information during emergencies (particularly in the event of loss of cellular communications) and during post-disaster cleanup operations.

In addition, the following benefits are obtained:

Benefit		**Description**
X	Financial Savings	Drones can be far more time efficient and cost effective when conducting asset inspections, by mitigating the need for traffic control, expensive scaffolding/swing stage or other equipment, and can provide more detailed photographs/videos of the assets or areas in need of maintenance or repairs than can be done manually, minimizing labor costs.

X	Time Savings	Deploying a drone can provide time savings over setting up and employing equipment such as scaffolds/swing stages/scissor-lift vehicles, etc.
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.

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:	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. 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*

Images/video of CCSF projects, assets, trees, etc.	JPGE, MOV, AVI	Level 1
Images/video of CCSF projects, assets, trees, etc.	JPGE, MOV, AVI	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.

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 use.

A. Department employees

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.

1. 7333-35 Stationary Engineer
2. 5310-13 Surveyor class series
3. 5201-18 Engineers class series

4. 1823-27 Analyst class series
5. 0922-0954 Manager class series
6. 3435 BUF Inspectors
7. 5120 Architectural Administrator
8. 5260-74 Architect Class Series
9. San Francisco Public Works: Bureau of Street Use & Mapping, Bureau of Urban Forestry, Bureau of Building Repair, Bureau of Engineering, Bureau of Architecture, Streets and Environmental Services, Streets and Sewer Repair

Contractors: The following providers are required to support and maintain the surveillance technology and its associated data to ensure it remains functional:

- At this point, Public Works does not anticipate using specific contractors whose services may be required
- However, if Public Works does use contractors, they will follow Public Works' Surveillance Technology Policy

B. Members of the public

Public Works 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 PM may access unedited data.

Data Sharing:	Public Works will endeavor to ensure that other agencies or departments that may receive data collected by Department of Public Work's unmanned aerial vehicles policy 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. Public Works 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) Public Works 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 STs 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. Public Works 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: The department does not share surveillance technology data containing non-obscured ("raw" or unedited) PII with other departments or entities inside the City and County of San Francisco.

Data sharing occurs at the following frequency: N/A

B. External Data Sharing:

Department shares the following data with the recipients:

- In emergency scenarios, Public Works may provide data to departments such as SFMTA, SFPUC, SF Port, SF Airport, SFDBI, and public access based on the Sunshine Ordinance. This data will be scrubbed and all PII will be removed, per Public Works' data processing protocols.

Data sharing occurs at the following frequency: Data sharing will vary by case.

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

- Public Works 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 Public Works 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:

- Public Works will process raw data collected by drones as expeditiously as possible, and will commit to remove or obscure all PII within one year of collection. Only post-processed (i.e., "scrubbed") data will be maintained by Public Works per federal (FEMA) and state (OES) and local reimbursement and investigation requirements. Unedited data shall be deleted upon completion of processing.
- Scrubbed data will be maintained in Public Works servers for historical purposes.

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
- 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:

Practices:

1. Raw (unprocessed) data will be collected by the drone in the field, and stored on an onboard storage disc (i.e, "SD" card).
2. Raw data (from the drone disc) will be downloaded from onboard storage disc onto secure Public Works servers by Drone Data Editor.
3. Still or video frames will be identified for use by the appropriate Public Works data consumer (based upon pre-approved Public Works use cases.)

Such data may include, as examples, images of buildings and structures, overhead images of topographic features, images of City tree canopy/limbs, and/or video images featuring Public Works project locations for use in Public Works TV episodes or other promotional materials.

Once the subject image frames, still and/or video, have been identified for business needs, the Public Works 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 distinctly identifying 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 to unedited data with PII present 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.

Data editors will be trained to properly utilize the editing software to ensure that all PII has been removed from still or video drone images before those images are released to other agencies or the public, or stored on servers for long term retention.

COMPLIANCE

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

1. Two individuals 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.
2. Department shall assign one or more of the following personnel to oversee Policy compliance by the Department and third-parties.
    a. Senior Administrative Analyst,
    b. BSM Deputy Bureau Manger,
    c. BOE Deputy Bureau Manager,
    d. BOE structural section manager,
    e. BOA Deputy Bureau Manager,
    f. BUF Deputy Bureau Manager,
    g. Architectural Administrator,
    h. Architects and Engineers

Sanctions for violations of this Policy include the following:

1. First offense: violator shall be verbally notified by Public Works management of nature of violation.
2. Second offense: violator shall be notified in writing of second offence and privileges to operate drone hardware shall be suspended for 60 days.
3. 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 by members of the public can register complaints / concerns or submit questions at San Francisco Public Works Bureau of Street-Use and Mapping (BSM) 1155 Market Street, 3rd Floor San Francisco, CA 94103, 415-554-5810 or via calls/emails to 311.org. As of July 15, Public Works will be located at 49 South Van Ness, Suite 300, San Francisco, CA 94102.

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 Bureau of Street-Use and Mapping (BSM) are received by counter personnel and routed to the bureau's Drone Program manager. Program manager will discuss concerns or complaints with constituent, enter details regarding nature of conversation on excel spreadsheet stored in Public Works shared drive, referred to as the drone Constituent Feedback Log ("CFL"). If additional action is required or requested by caller, Public Works commits to a follow-up (by email or telephone) within 48 hours. Department shall be prepared to host a viewing of edited imagery if caller is insistent, to demonstrate that no PII was collected. Depending upon the urgency or sensitivity of call, Drone Program manager shall notify bureau of details and discuss resolution before follow-up with caller. The final outcome and action(s) taken shall be logged onto CFL.

Public Works drone operators and Public Works 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.