Surveillance Technology Policy

Drones
Department of Public Works

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 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 Drones 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, 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 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):

- Disaster preparedness
- Environmental monitoring and documentation
- Inspect/survey properties & assets
- Project inspection and documentation
- Surveying/mapping data collection

Further, 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.

BUSINESS JUSTIFICATION

Drone technology will support our mission through the following:

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 structures by identifying potential maintenances issues at locations that are currently unsafe for an inspection staff;

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, engineers, electricians, PMs, CMs and other personnel;

4. Drones will support the maintenance efforts of City-owned structures by identifying potential maintenance issues at locations unsafe for inspection staff.

In addition, Drones promise to benefit residents in the following ways:

Education: drone imagery to promote Public Works projects and demonstrate use of tax dollars on projects.

Environment: drone imagery to collect data on street-trees for maintenance and safety reasons.

Public Safety: to inspect tree canopies for damaged limbs (fall risks), to perform safety inspections at locations or structures that are difficult/unsafe to access, 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.

Drones will benefit the department in the following ways:

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.

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

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.

Improved data quality: some locations which are difficult to access by personnel may be more easily photographed using drone technology, thereby achieving better data.

To achieve its intended purpose, Drones (hereinafter referred to as "surveillance technology") incorporate unmanned, remotely-operated aircraft with onboard visual recording equipment, for the purpose of capturing images from an aerial perspective

Department staff may use the technology for authorized use cases only, and is expressly prohibited from the following use cases:

- To intentionally capture images of a personal nature.

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:

Data Type(s)	**Format(s)**	**Classification**
Photographic and video data (no audio) of assets, landscapes, etc.	*JPEG, PNG, MOV, AVI, CSV*	Level 2
License plate numbers	*JPEG, PNG, MOV, AVI, CSV*	
Faces/distinguishing features	*JPEG, PNG, MOV, AVI, CSV*	

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:

- Information on the surveillance
- Description of the authorized use
- Type of data collected
- Will persons will be individually identified
- Data retention
- Department identification
- Contact information

Access: All parties requesting access must adhere to the following rules and processes:

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 access and use are restricted to:

- Only authorized drone operators, data editors, and PMs may access unedited data

Access requirements vary by party:

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.

- Data must always be scrubbed of PII as stated above prior to use

Department shall maintain access logs for surveillance technology and all data collected, processed, and/or stored by the surveillance technology. The name of the person making the log entry should be recorded, along with the date and time.

B. Members of the public, including criminal defendants

Data collected by surveillance technology will not be made available to members of the public, including criminal defendants.

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, data editors, or PMs may access unedited data

Data Sharing: 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.

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)

Department shall ensure all PII and restricted data is de-identified or adequately protected to ensure the identities of individual subjects are effectively safeguarded.

The Department currently participates in the following sharing practices:

A. Internal Data Sharing

Departments shares the following data with the recipients:

Image of assets (with PII removed or obscured	San Franicsco Public Works may share this type of data with any City department

Data sharing frequency will vary by case

Public Works is unaware of a specific legal standard in this regard. However, as responsible service providers Public Works believes asset owners have a right to

view pertinent information we have collected on their behalf regarding the condition of their asset(s).

Such a disclosure would be made in the best interests of our partner agencies, for whom Public Works has been contracted to provide inspection, maintenance, repair, or construction services.

The department does not share surveillance technology data with other departments or entities inside the City and County of San Francisco.

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:

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.	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.

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

Data will be stored in the following location:

- Local storage
- Cloud storage provider

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

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 Public Works servers by Drone

Data Editor. 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. 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.

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 method:

- 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.

Department shall assign the following personnel to oversee Policy compliance by the Department and third-parties:

- Senior Administrative Analyst

- BSM Deputy Bureau Manger

Sanctions for violations of this Policy include the following:

> **First offense**: violator shall be verbally notified by Public Works 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.
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:

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.

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 will be entered into the Department's RFA (Request for Action) system. The RFA system triages, and tracks complaints received by the Department and the complaint will be addressed per Department policy.

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: Surveillance Technology Policy Requirements

The following section shows all Surveillance Technology Policy requirements in order as defined by the San Francisco Administrative Code, Section 19B.

1. A description of the product and services addressed by the Surveillance Technology, including the identity of any provider(s) whose services are essential to the functioning or effectiveness of the Surveillance Technology equipment or services for the intended purpose.
Drone technology incorporates unmanned, remotely-operated aircraft with onboard visual recording equipment, for the purpose of capturing images from an aerial perspective. Specific model information as follows: The Intel Falcon 8+ drone is designed to provide consistent, stable flights with weak GPS signals, high winds as well as resistance to magnetic field. Falcone 8+ drone can provide detailed data for orthography and 3D reconstruction, with millimeter accuracy for ground sample distance. The Leica Aibot AX20 is built on a DJI UAV platform which can accommodate various sensor payloads for surveying, mapping and construction aerial data capture solutions. The DJI Mavic 2 Enterprise Dual is an aerial survey drone that combines navigation and positioning with a high-performance imaging system for use during surveying, mapping or inspection operations.

2. A description of the purpose(s) for which the Surveillance Technology equipment or services are proposed for acquisition, including the type of data that may be collected by the Surveillance Technology equipment or services.

Drone technology will support our mission through the following:

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 structures by identifying potential maintenance issues at locations that are currently unsafe for an inspection staff;

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, engineers, electricians, PMs, CMs and other personnel;

4. Drones will support the maintenance efforts of City-owned structures by identifying potential maintenance issues at locations unsafe for inspection staff.

Data Type(s)	**Format(s)**	**Classification**
Photographic and video data (no audio) of assets, landscapes, etc.	*JPEG, PNG, MOV, AVI, CSV*	Level 2
License plate numbers	*JPEG, PNG, MOV, AVI, CSV*	
Faces/distinguishing features	*JPEG, PNG, MOV, AVI, CSV*	

3. The uses that are authorized, the rules and processes required prior to such use, and uses of the Surveillance Technology that will be expressly prohibited.

Authorized uses:

- Disaster preparedness
- Environmental monitoring and documentation
- Inspect/survey properties & assets
- Project inspection and documentation
- Surveying/mapping data collection

Use of drone technology to intentionally capture images of a personal nature will always be prohibited.

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 the 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.

4. A description of the formats in which information collected by the Surveillance Technology is stored, copied, and/or accessed.

Data Type(s)	**Format(s)**	**Classification**
Photographic and video data (no audio) of assets, landscapes, etc.	*JPEG, PNG, MOV, AVI, CSV*	Level 2
License plate numbers	*JPEG, PNG, MOV, AVI, CSV*	
Faces/distinguishing features	*JPEG, PNG, MOV, AVI, CSV*	

5. The specific categories and titles of individuals who are authorized by the Department to access or use the collected information, including restrictions on how and under what circumstances data collected with Surveillance Technology can be analyzed and reviewed, and the rules and processes required prior to access or use of the information.

Employee Job Classification & Title	7334 Stationary Engineer, 5310-13 Surveyor class series, 1823-27 Analyst class series; 0922-0954 Manager class series; 5201-12 Engineer class series
Department:	San Francisco Public Works: Bureau of Street Use & Mapping Bureau of Urban Forestry Bureau of Building Repair Bureau of Engineering
If applicable, contractor or vendor name:	

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 the 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.

6. The general safeguards that protect information from unauthorized access, including encryption and access control mechanisms.
Only authorized drone operators, data editors, or PMs may access unedited data.
7. The limited time period, if any, that information collected by the Surveillance Technology will be routinely retained, the reason such retention period is appropriate to further the purpose(s) enumerated in the Surveillance Technology Policy, the process by which the information is regularly deleted after that period lapses, and the specific conditions that must be met to retain information beyond that period
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. Scrubbed data will be maintained in Public Works servers for historical purposes. 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 Public Works servers by Drone Data Editor. 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. 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.
8. How collected information can be accessed or used by members of the public, including criminal defendants
Only data with no PII may be accessible or available for use by the public, including criminal defendants. No unedited data will be accessed by the public, including criminal defendants.

9. Which governmental agencies, departments, bureaus, divisions, or units that may receive data collected by the Surveillance Technology operated by the Department, including any required justification or legal standard necessary to share that data and how it will ensure that any entity receiving such data complies with the Surveillance Technology Policy.
Data acquired by this technology will not be shared with entities outside the City and County of San Francisco All SF Departments for which Public Works may provide services described in 3.27 response. The frequency of data sharing will vary by case. The type of data that will be disclosed is images of assets (with PII removed or obscured). We are unaware of a specific legal standard in this regard. However, as responsible service providers Public Works believes asset owners have a right to view pertinent information we have collected on their behalf regarding the condition of their asset(s). Such a disclosure would be made in the best interests of our partner agencies, for whom Public Works has been contracted to provide inspection, maintenance, repair, or construction services. Public Works policy will prevent sharing data with any entities data that has not been edited to remove PII
10. The training required for any individual authorized to use the Surveillance Technology or to access information collected by the Surveillance Technology
Training is required for authorized individuals to use or access the information collected. Drone data collection and use shall be explained in Departmental Drone Policy. All authorized users must sign off on policy prior to use.
11. The mechanisms to ensure that the Surveillance Technology Policy is followed, including internal personnel assigned to ensure compliance with the policy, internal recordkeeping of the use of the technology or access to information collected by the technology, technical measures to monitor for misuse, any independent person or entity with oversight authority, and the sanctions for violations of the policy
Public Works policy will prevent sharing data with any entities data that has not been edited to remove PII

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.

- Senior Administrative Analyst
- BSM Deputy Bureau Manger

First offense: violator shall be verbally notified by Public Works 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.

Only authorized drone operators, data editors, or PMs may access unedited data.

12. What procedures will be put in place by which members of the public can register complaints or concerns, or submit questions about the deployment or use of a specific Surveillance Technology, and how the Department will ensure each question and complaint is responded to in a timely manner.

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.

Constituent calls and complaints to the Bureau of Street-Use and Mapping (BSM) are received by counter personnel will be entered into the Department's RFA (Request for Action) system. The RFA system triages, and tracks complaints received by the Department and the complaint will be addressed per Department policy.