Surveillance Technology Policy

Automated Speed Enforcement
Municipal Transportation Agency

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 Automated Speed Enforcement (hereinafter referred to as "surveillance technology" or ASE or ASE 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 connect San Francisco through a safe, equitable, and sustainable transportation system.

The Surveillance Technology Policy ("Policy") defines the manner in which the surveillance 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 the surveillance technology 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 the surveillance 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. *Enforce speed limits on City streets in accordance with California Vehicle Code sections 22425-22434 (Speed Safety System Pilot Program)*
2. *Analysis of and reporting on speed enforcement, as required under the Speed Safety System Pilot Program.*

Prohibited use cases include any uses not stated in the Authorized Use Case section.

Department 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.

BUSINESS JUSTIFICATION

Reason for Technology Use

Surveillance Oversight Review Dates
PSAB Review: TBD (list all dates at PSAB, and write "Recommended: MM/DD/202X" for rec date)
COIT Review: TBD (list all dates at COIT, and write "Recommended: MM/DD/202X" for rec date)
Board of Supervisors Approval: TBD

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

In line with its mission, the Department uses ASE technology to efficiently enforce vehicle speed laws. This use supports the Department's mission to achieve zero traffic-related fatalities (Vision Zero Policy), as traffic enforcement is a critical component of the "three E's" of Vision Zero--education, engineering, and enforcement. Speed is the leading contributor to traffic collisions causing serious injuries and fatalities, and this technology is intended to reduce vehicle speeding.

Description of Technology

"Speed safety system" or "system" means a fixed or mobile radar or laser system or any other electronic automated detection equipment to detect a violation of speed laws and utilizes cameras to obtain a clear photograph of a speeding vehicle's rear license plate. These cameras are only triggered by speeding vehicles. They do not record data unless triggered by a speeding vehicle.

Resident Benefits

The surveillance technology promises to benefit residents in the following ways:

	Benefit	Description
☐	Education	
☐	Community Development	
☒	Health	Health: speed cameras have been proven in hundreds of cities to reduce rates of serious injuries and fatalities due to speed. As speed is the primary factor in collisions in San Francisco, this technology could reduce the risk of roadway collisions, improving overall citywide public health.
☐	Environment	
☒	Criminal Justice	Criminal Justice: removes bias from enforcement of traffic violations and limits contact with uniformed police officers
☐	Jobs	
☐	Housing	
☒	Public Safety	Public Safety: speed cameras have been proven to reduce the likelihood of a speed-related collision, thus improving overall public safety on roadways.

Department Benefits

The surveillance technology will benefit the department in the following ways:

	Benefit	Description
☐	Financial Savings	
☒	Time Savings	Helps staff remotely identify speeding violations at multiple locations, improving effectiveness and efficiency of speed enforcement.
☒	Staff Safety	Enforces speed limits without the potential for in-person traffic stops.
☒	Data Quality	Improves accuracy of data related to speeding vehicle speeding over the posted speed limits. Provides data to inform policies and regulations and allows for more immediate data to demonstrate the impacts of various traffic control measures on streets over time.
☒	Other	Provides data regarding the effectiveness of speed safety cameras over a five-year pilot period, which will inform future statewide policies regarding automated speed enforcement.

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 within two versions of most current version of technology.

Data Collection: Department shall only collect data required to execute the authorized use cases. All data collected by the surveillance technology, including PII, shall be classified according to the City's Data Classification Standard.

The surveillance technology collects some or all of the following data type(s):

Data Type(s)	*Format(s)*	*Classification*
Digital Images of rear license plate	Photographic, JPEG	*Level 3*

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 technology
- ☒ Description of the authorized use
- ☐ Type of data collected
- ☐ Data retention
- ☒ Department identification
- ☒ Contact information
- ☐ Persons individually identified

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

- • Authorized users must complete mandatory training and obtain login credentials.
  • Only authorized users may use ASE technology or access data.
  • Authorized users must log into tablet or computer, as applicable, to access ASE technology data.

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:

- 104X - IT Staff
- 109X - Operations Support Admin
- 182X - Administrative Analyst
- 528X - Transportation Planning Professsionals
- 816X - Hearing Officer
- 821X - Enforcement staff
- 91XX - Managers
- 950X - Citations Clerk

B. Members of the public

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. 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.

Members of the public 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.

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.

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 dictated by this policy. 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.

The Department will ensure employees and vendors are trained on how to use the ASE technology correctly and ensure ASE data is used for its intended use only. Training includes explaining how employees and vendors can use data and how to report problems with the ASE system.

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) as defined by the National Institute of Standards and Technology (NIST) security framework 800-53, or equivalent requirements from other major cybersecurity frameworks selected by the department.

Department shall ensure compliance with these security standards through the following:

Administrative Safeguards: The Department will secure any PII against unauthorized access, processing, disclosure, and accidental loss, destruction, or damage. ASE data collected and retained by the Department will be protected by the safeguards

appropriate for its classification level(s).
To protect ASE data from unauthorized access and control, including misuse, the Department shall, at minimum, apply the following safeguards:
• Authorized users will login credentials with MFA, if available, and use complex passwords to access the ASE technology. • All access to and activity in the ASE system will be logged and be audited.

Data Storage: Data will be stored in the following locations and encrypted at rest (at the following locations):

☒ 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

☐ Cloud Storage Provider

Data Sharing: In accordance with California Vehicle Code section 22425(l)(1), data, including photographic or administrative records, made by the surveillance technology shall be confidential and shall not be shared unless required by law. The Department shall use and allow access to such data only for the purposes authorized under section 22425.

A. Internal Data Sharing:

The department will not share surveillance technology data with other departments or entities inside the City and County of San Francisco. The department will analyze the data internally and share anonymized reports with other Vision Zero departments, such as San Francisco Police Department (SFPD), Office of the Medical Examiner (OME), and Department of Public Health (DPH).

B. External Data Sharing:

The department will not share surveillance technology data externally with entities outside the City and County of San Francisco unless a warrant/subpoena was issued.

Data Retention: The retention schedule for data generated by the surveillance technology is prescribed by California Vehicle Code section 22425(l), as follows:

Retention Period	Retention Justification
Photographic evidence: up to 60 days after final disposition of notice of	Retention period established under California Vehicle Code section 22425(l).

speeding violation; up to five days if no notice of speeding violation is issued.	
Confidential information received from the Department of Motor Vehicles to issue notices of violation): up to 120 days after final disposition of notice of speeding violation.	Retention period established under California Vehicle Code section 22425(l).

Exceptions to Retention Period - Department does not plan to retain data beyond what is described in the retention period above.

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

- Upon completion of the applicable data retention period, the Department will automatically dispose of raw ASE data (e.g., ASE data that has not been anonymized or aggregated).
- In accordance with the California Vehicle Code section 22425(l)(3), photographic evidence and other confidential information from DMV will destroyed in a manner that maintains the confidentiality of any person included in the record or evidence.

COMPLIANCE

Department Compliance

Department shall oversee and enforce compliance with this Policy using the following methods: The Department will assign the positions listed below to oversee, or assign staff members under their direction to oversee, compliance with this Policy.

• 9180 Director of Parking Enforcement and Traffic

• 5290 Program Manager for SFMTA Speed Safety Cameras

Interdepartmental, Intergovernmental & Non-Governmental Entity Compliance

In accordance with California Vehicle Code section 22425(l)(5), information collected and maintained by the Department using the surveillance technology shall not be disclosed to any other persons, including, but not limited to, any other state or federal government agency or official for any purpose, except as required by state or federal law, court order, or in response to a subpoena in an individual case or proceeding.

Oversight Personnel

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

- 9180 Director of Parking Enforcement and Traffic
- 5290 Program Manager for SFMTA Speed Safety Cameras

Sanctions for Violations

Sanctions for violations of this Policy include the following:

• Violations of this Policy may result in disciplinary action commensurate with the severity of violation. Sanctions include written warning, suspension, and termination of employment.

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

Under California Vehicle Code section 22425(l)(5), the Department cannot disclose or share data from the ASE with anyone, including state or federal government agencies or officials for any purpose, except as required by state or federal law, court order, or in response to a subpoena in an individual case or proceeding.

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 not 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 Inquiries

Public complaints or concerns may be submitted to the Department by calling 311 or visiting 311.org.

Department shall acknowledge and respond to complaints and concerns in a timely and organized response, and in the following manner:

Department will respond to 311 complaints.

Inquiries from 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.