Surveillance Technology Policy

SCRAM Global Positioning System (SCRAM GPS)
Juvenile Probation Department

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 SCRAM Global Positioning System ("SCRAM GPS") itself as well as any associated data by the Juvenile Probation Department ("Department"), and the protection of City and County of San Francisco residents' civil rights and liberties.

PURPOSE AND SCOPE

The Juvenile Probation Department's mission is to serve the needs of youth and families who are brought to our attention with care and compassion; to identify and respond to the individual risks and needs presented by each youth; to engage fiscally sound and culturally competent strategies that promote the best interests of the youth; to provide victims with opportunities for restoration; to identify and utilize the least restrictive interventions and placements that do not compromise public safety; to hold youth accountable for their actions while providing them with opportunities and assisting them to develop new skills and competencies; and contribute to the overall quality of life for the citizens of San Francisco within the sound framework of public safety as outlined in the Welfare & Institutions Code.

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

Authorized Use(s):

- Youth are only placed on electronic monitoring in San Francisco with a court order. The Court may order a youth to be placed on electronic monitoring as an alternative to detention.
- Electronic monitoring (EM) may also be added as a condition of probation if additional supervision is warranted. EM data is analyzed on a daily basis by probation officers to ensure compliance with:
    - Court ordered curfews

- Inclusion zones: addresses/areas where the minor has approval to be present, for example their home, school, work.
- Exclusion zones: addresses/areas where the minor should not be present, including Stay Away orders
- Schedules: To monitor school attendance, program participation, work.

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.

BUSINESS JUSTIFICATION

SCRAM GPS supports the Department's mission and provides important operational value in the following ways:

Electronic monitoring, as ordered by the Court, is used as an alternative to detention or as a measure of stepped up supervision for youth on probation, supporting the Department's mission to respond to individual risks and needs, engage in fiscally sound strategies that promote the best interest of youth, support victims, and to utilize the least restrictive interventions and placements that do not compromise public safety, and contribute to the quality of life of the citizens of San Francisco.

In addition, SCRAM GPS promises to benefit residents in the following ways:

- Criminal Justice, Public Safety: Electronic monitoring enables the Court to utilize the least restrictive intervention to respond to juvenile delinquency and promote public safety. This technology benefits residents by safely reducing the detention of youth in juvenile hall and advancing community safety.

SCRAM GPS will benefit the department in the following ways:

- Improved Data Quality, Time Savings: Electronic monitoring benefits department operations by providing alternatives to detention pursuant to the order of the Court in a manner that is responsive to individual risks and needs, and by engaging in fiscally sound strategies that promote the best interest of youth, support victims, utilize the least restrictive interventions and placements that do not compromise public safety, and contribute to the quality of life of the citizens of San Francisco.

To achieve its intended purpose, SCRAM GPS (hereinafter referred to as "surveillance technology") consists of placing FCC-certified ankle bracelets on participants that monitor location through global positioning system (GPS) technology. The bracelets are placed in such a way that they cannot be removed. At least once per minute, 24 hours per day, 7 days per week, the bracelet transmits location information via the cellular network to a central computer. The information is compared with the court

ordered curfew schedule and/or inclusion/exclusions zones. SCRAM provides a web-based interface for JPD to access the monitoring data.

POLICY REQUIREMENTS

This Policy defines the responsible data management processes and legally enforceable safeguards required by the Department to ensure transparency, oversight, and accountability measures. Department use of surveillance technology and information collected, retained, processed or shared by surveillance technology must be consistent with this Policy; must comply with all City, State, and Federal laws and regulations; and must protect all state and federal Constitutional guarantees.

Specifications: The software and/or firmware used to operate the surveillance technology must be 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 Types: Geolocation data (periodic latitude and longitude points)
- Date Format: Stored in binary in a SQL database
- Data Security Classification: Level 4

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:

- Department identification
- Description of the authorized use
- Information on the surveillance technology
- Type of data collected

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):

- Youth are only placed on electronic monitoring in San Francisco with a court order, and Sworn Probation Services Personnel only access or use data pursuant to the court order.

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

A. Department employees

Once collected, the following roles and job titles are authorized to access and use data collected, retained, processed or shared by the surveillance technology:

- (21) Class 8444 Deputy Probation Officers
- (6) Class 8434 Supervising Probation Officers
- (1) Senior Supervising Probation Officer
- (1) Director of Probation Services
- (1) Chief Probation Officer

B. Members of the public, including criminal defendants

The Juvenile Probation Department will comply with the California Public Records Act, the San Francisco Sunshine Ordinance, the requirements of the federal and State Constitutions, and federal and State civil procedure laws and rules.

Collected data that is classified as Level 1-Public data may be made available for public access or release via DataSF's Open Data portal. Anyone, including criminal defendants, may access such data. Open Data has a Public Domain Dedication and License, and makes no warranties on the information provided. Once public on Open Data, data can be freely shared, modified, and used for any purpose without any restrictions. Any damages resulting from use of public data are disclaimed, including by criminal defendants.

Members of the public, including criminal defendants, may also request access by submission of a request pursuant to San Francisco's Sunshine Ordinance. No record shall be withheld from disclosure in its entirety unless all information contained in it is exempt from disclosure under express provisions of the California Public Records Act or some other statute.

Data Security: Department shall secure PII against unauthorized or unlawful processing or disclosure; unwarranted access, manipulation or misuse; and accidental loss, destruction, or damage. Surveillance technology data collected and retained by the

Department shall be protected by the safeguards appropriate for its classification level(s).

To protect surveillance technology information from unauthorized access and control, including misuse, Department shall, at minimum, apply the following safeguards:

The SCRAM GPS web-based interface includes security measures that allow only authorized personnel to access and use the data. SCRAM uses Transport Layer Security (TLS) for transmission, encrypted at rest.

Data Sharing: The Juvenile Probation Department will endeavor to ensure that other agencies or departments that may receive data collected by Juvenile Probation Department's SCRAM GPS Policy will act in conformity with this Policy.

For internal and externally shared data, shared data shall not be accessed, used, or processed by the recipient in a manner incompatible with the authorized use cases stated in this Policy.

The Juvenile Probation 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)

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

Further, in sharing data, processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying an individual person, data concerning health or data concerning an individual person's sex life or sexual orientation shall be prohibited.

Each department that believes another agency or department receives or may receive data collected from its use of surveillance technologies should consult with its assigned deputy city attorney regarding their response.

Before sharing data with any recipients, the Department will use the following procedure to ensure appropriate data protections are in place:

- *X* Confirm the purpose of the data sharing aligns with the department's mission.
- X Consider alternative methods other than sharing data that can accomplish the same purpose.
- X Redact names, scrub faces, and ensure all PII is removed in accordance with the department's data policies.

X Review of all existing safeguards to ensure shared data does not increase the risk of potential civil rights and liberties impacts on residents.

X Evaluation of what data can be permissibly shared with members of the public should a request be made in accordance with the San Francisco's Sunshine Ordinance.

X Ensure data will be shared in a cost-efficient manner and exported in a clean, machine-readable format.

The Juvenile Probation 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:

Data Type	Data Recipient
Geolocation data for the individual in question	Data regarding individual youth may be shared on a need to know basis and/or pursuant to a court order with the Police Department, District Attorney, and Public Defender, pursuant to an ongoing investigation and/or court proceeding.

Data sharing occurs at the following frequency:

- On a case-by-case basis.

B. External Data Sharing

Department shares the following data with the recipients:

Data Type	Data Recipient
Geolocation data for the individual in question.	Data regarding individual youth may be shared on a need to know basis and/or pursuant to a court order with the Superior Court, or other Law Enforcement Agencies outside of CCSF, pursuant to an ongoing investigation and/or court proceeding.

Data sharing occurs at the following frequency:

- On a case-by-case basis.

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

Data regarding individual youth is only shared on a need to know basis and/or pursuant to a court order with justice system partners who are subject to state laws regarding the confidentiality of juvenile records.

Before data sharing with any recipient, the Department 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.

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:

Data Retention Period	Data Retention Justification
Records are retained pursuant to the schedule defined in the Department Record Retention and Destruction policy, which is guided by state law, depending on the type of case and court orders regarding sealing and destruction. The minimum retention period is 2 years.	Juvenile case file record retention is dictated by state law.

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):

- Data is retained for the period defined by state law.

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

Data will be stored in the following location:

- Local storage.

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

- When retention period ends, case files are shredded.

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.

- All sworn Probation Services Personnel are provided training by SCRAM on how to install, removed, activate, and deactivate, an Electronic Monitor, as well as being able to navigate the SCRAM web-based interface prior to using the system prior to accessing or using the technology.

COMPLIANCE

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

The Director of Probation Services or designee will be responsible for enforcing the Surveillance Technology policy through its incorporation into the overall Department Policy for Probation Services. All sworn Probation Services personnel will be trained on the Surveillance Technology policy.

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

The Director of Probation Services (#8416) and the Senior Supervising Probation Officer (# 8415) oversee the Surveillance Technology policy.

Sanctions for violations of this Policy include the following:

Violation of the policy will be subject to standard JPD departmental policies, which may include disciplinary action up to and including termination.

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 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:

Complaints to the Department are accepted in any format, via any means: phone call, verbal to a staff member, email or by written Complaint Form from the SFJPD website. Members of the public can find more information about how to register complaints on the Department's web site: https://sfgov.org/juvprobation/complaints

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

All complaints are directed to the Chief Probation Officer wherein each complaint is assigned a number, and tracked according to AB-953 by date. A receipt letter is sent to each complainant upon delivery of the complaint to the Chief Probation Officer verifying their complaint has been received. The complaint investigation is then assigned by the Chief Probation Officer to staff who to report back directly to the Chief Probation Officer. Once the complaint has been investigated, a follow-up letter shall be sent to the complainant which includes outcomes from the investigation.

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.