Surveillance Technology Policy

Sensource Patron Counter System,
Public Library

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 Sensource Patron Counter System 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

The San Francisco Public Library (SFPL) is dedicated to free and equal access to information, knowledge, independent learning and the joys of reading for our diverse community.

The Surveillance Technology Policy ("Policy") defines the manner in which the Sensource Patron Counter System 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 Sensource Patron Counter System, 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 Sensource Patron Counter System technology for the Department is limited to the following use cases and is subject to the requirements listed in this Policy. There are no additional uses employed by or authorized by the Library.

Authorized Use(s):

– To tally the entry and exit of Library visitors at all 28 public facilities.
– To track usage of meeting rooms, elevators and restrooms for purposes of resource allocation.

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

Sensource Patron Counter System supports the Department's mission and provides important operational value in the following ways:

The Sensource Patron Counter System allows SFPL to track meaningful operational metrics that show patron entrance/exit traffic throughout our 28 public facilities.

In addition, Sensource Patron Counter System promises to benefit residents in the following ways:

- X Community Development: The ability to track accurate patron counts by location in real-time is integral to provision of Library services planning with respect to resource allocation (e.g., staffing, planning for programs, ensuring public safety related to space capacity, etc.).
- X Criminal Justice: Library services benefit the residents of the community in numerous ways, including but not limited to education (programming), health (programming), workforce development/jobs (adult programming), community engagement/development (programming), environmental concerns (programming), housing (programming), criminal justice (programming) and public safety (ensuring crowd sizes are appropriate for spaces).
- X Education: See above.
- X Environment: See above.
- X Health: See above.
- X Housing: See above.
- X Jobs: See above.
- X Library Services: See above.
- X Public Safety: See above.

Sensource Patron Counter System will benefit the department in the following ways:

- X Financial Savings: Visitor traffic is a core metric within the library industry, reported at the national, state and local levels as a key performance indicator. The Sensource Patron Counter System allows for considerable financial and time savings, as what was previously a manual data collection and analysis process has become automated, allowing for real-time review and data analysis.
- X Improved Data Quality: Data quality has become much more reliable and valid through automation.
- X Staff Safety: Staff safety with respect to planning and managing busy times and crowding with respect to popular programming (e.g., Night of Ideas) is also a benefit to department operations
- X Time Savings: See "Financial Savings".

To achieve its intended purpose, Sensource Patron Counter System (hereinafter referred to as "surveillance technology") uses a proprietary camera system (shown in more detail in the SIR) to tally visitor counts in real time at all 28 San Francisco Public Library facilities. The aggregated tally data (not video images) is stored on a cloud-based server and is accessible through web-connected devices.

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:

- SFPL collects only aggregate data showing the total number of persons entering/exiting through a viewable space serviced by the Sensource Patron Counter System. These data are stored in software on the cloud owned and maintained by Sensource, Inc., and then pulled on to SFPL local servers for review, analysis and reporting. The cameras provide a real-time video stream that shows humanoid forms of people walking through the Sensource viewing area from above, in addition to location data (where the individuals are walking through), but SFPL does not collect these data and such real-time viewing is limited to administrator access in real time**. Also note that the video images are not recorded or stored.** Sensource data in the real-time stream are Level 3 – Sensitive. Aggregate data pulled out of Sensource for review, analysis and reporting are Level 1 - Public.

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
- Patrons are notified that activities in a location may be recorded.

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):

- Only staff designated by the City Librarian and/or Chief Operating Officer and Director of Facilities have access to the Sensource Patron Counter System, which is password-protected and limited to staff responsible for maintaining the devices as well as those validating and collecting aggregate visitor data.

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:

- 0964 City Librarian (1)
- 0953 Chief Operating Officer (1)
- 0952 Deputy Director (2)
- 0932 Manager IV (2)
- 1823 Senior Data Analyst (1)
- 1822 Senior Administrative Assistant (2)
- 1840 Junior Management Assistant (1)
- 1801 Analyst Trainee (1)
- 3618 Library Technical Assistant (2)
- 3630 Librarian I (1)
- 3634 Librarian III (3)

B. Members of the public, including criminal defendants

The Public Library 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:

The SFPL Facilities division, under guidance from the Chief Operating Officer, maintains a list of staff with password-protected access to the Sensource Patron Counters System, and reviews/updates that list annually for accuracy and alignment with business needs. Further, the Department of Human Resources Employee Handbook addresses Employee Use of City Resources and City Computers and Data Information Systems. Staff are expected to abide by these guidelines as a condition of employment.

Data Sharing: The Public Library will endeavor to ensure that other agencies or departments that may receive data collected by SFPL 's Sensource People Counter 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 Public Library 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 Public Library 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 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 Public Library 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 non-PII, Level 1 data with the recipients:

Type	**Recipient**
Monthly and annual aggregate totals of visits by location.	Controller's Office. SFPL provides performance measures to CON twice a year that shows monthly and annual visits to SFPL facilities. These data are measured by the Sensource Patron Counter System.

Data sharing occurs at the following frequency:

Twice annually.

B. External Data Sharing

Department shares the following non-PII, Level 1 data with the recipients:

Type	Recipient
Aggregate totals of visitors in text format.	California State Library. American Library Association. Public Library Association. Others, upon request. As noted, library visits is a key performance indicator that is shared widely for benchmarking and analysis within the industry. These data are shared in the aggregate, with no PII concerns.

Data sharing occurs at the following frequency:

At least annually, as well as upon request. .

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

San Francisco Public Library endeavors to comply with all relevent privacy statutes at the federal, state and local levels..

Before data sharing with any recipient, 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 by other means that can accomplish the same purpose.
- X Ensure shared data will be done in a cost-efficient manner and exported in a clean, machine-readable format.
- X Evaluate what data can be permissibly shared with members of the public should a request be made in accordance with San Francisco's Sunshine Ordinance.
- X Review all existing safeguards to ensure shared data does not increase the risk of potential civil rights and liberties impacts on residents.

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:

Retention Period	Retention Justification

Permanent records.	SFPL keeps aggregate visitor total data indefinitely for historical review and sharing 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:

- Software as a Service Product
- Local Storage

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

Practices:

- N/A

Processes and Applications:

- There is no PII related to the aggregated data so no deidentification required.

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 staff accessing Sensource are given a one-time training on how to use the software and the proper use cases for the aggregate visitor data. This training includes but is not limited to the following components: logging into the system; reviewing available dashboards and how to manipulate filters for their specific needs; how to interpret the dashboards and data within; how to export data; uses for data.

COMPLIANCE

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

The Director of Facilties is responsible for monitoring the Sensource Patron Counter System to ensure that staff do not violate the Library's privacy and compliance policies. .

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

- 0953 - Chief Operating Officer
- 0932 - Director of Facilities

Sanctions for violations of this Policy include the following:

- First Offense: Staff who use the system inappropriately will receive initial counseling on appropriate use of Sensource within the organization.
- Second Offense: Staff will be put on probation for 3 months from using the system.
- Third Offense: Staff will be prohibited from using the system.

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 or concerns can be submitted to the Department by:

Members of the public can register complaints/concerns or submit questions in writing via the library's chat service, or "Comments and Suggestions" page online, or in person at the City Librarian's Office, Main Library, 100 Larkin Street, San Francisco 94102. They can also contact the library through telephone at 415-557-4400 or email at info@sfpl.org. All questions and complaints are forwarded to the proper SFPL division for appropriate and timely responses.

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

Multiple staff monitor SFPL communications portals to ensure that members of the public receive a response within 24 hours.

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.