Surveillance Technology Policy

Computer Management 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 Today's Business Solutions (TBS) Computer Time and Print Management 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:

The San Francisco Public Library system 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 Today's Business Solutions (TBS) Computer Time and Print Management 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 Today's Business Solutions (TBS) Computer Time and Print Management, 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 Today's Business Solutions (TBS) Computer Time and Print Management technology for the Department is limited to the following use cases and is subject to the requirements listed in this Policy.

Authorized Use(s):

– *The authorized use case for the TBS Computer Time and Print Management tool is to provide time-delimited public access to library computers and allow the public to print, copy, scan and fax documents, as well as track usage of computers and print resources throughout the library's 28 facilities for purposes of resource allocation and management.The five specific components within TBS Computer Time and Print Management are as follows:*
– *MyPC: Manages patron access to library computers and regulates amount of time each patron can use computers*
– *EZ Booking: Allows patrons to manage their reservations in MyPC, schedule public computer use, etc.*

COIT Policy Dates
COIT Review: June 16, 2022
BOS Approval: TBD

– *Papercut/EPrintIt: Manages public print jobs sent from library computers and patrons' personal devices, allowing them to print their documents on library printers* – *Papercut/ePrintIt: Allows select library staff members, in the interest of customer service and support, to retrieve and print jobs submitted to the system by users during the 24-hour period in which documents are retrievable. This allows staff to print jobs when printers fail, when print jobs do not meet user expectations, to intermediate when users are struggling with technology, etc.*
– *ScanEZ: Allows library patrons to scan, manipulate, manage, print, email, fax and save documents using either the library's flat-bed or document feeder scanners.*
– *Payment Kiosk: Allows patrons to pay for print and copy jobs processed through Papercut/EPrintIt and/or ScanEZ.*

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

Today's Business Solutions (TBS) Computer Time and Print Management adds to the Department's mission and provides important operational value in the following ways:

The computer time management portion of the technology is the mode by which the library is able to provide free, equitable access to public computing resources to its patrons. The print management solution is a comprehensive document management solution that allows library patrons to print from library computers and their own devices, as well as to create copies, send faxes, scan documents to electronic storage media, etc. Both of these functionalities support access to information as well as to services (e.g., government programs and resources, job applications, etc.).

In addition, Today's Business Solutions (TBS) Computer Time and Print Management promises to benefit residents in the following ways:

X	Library Services	This technology benefits residents by broadly supporting a wide range of Library Services - It allows patrons to access the internet free of charge, which in turn gives them access to resources that can benefit their education, health, employment, housing situation, and interaction with the criminal justice system. It provides inexpensive access to printing, copying, faxing, and scanning of documents, which also benefits the public in the aforementioned ways. It allows staff to be better able to serve the public with more useful tools, as

		well as to allow the library to provide more meaningful service to its patrons by more efficiently providing service and managing resources

Today's Business Solutions (TBS) Computer Time and Print Management will benefit the department in the following ways:

X	Financial Savings	This technology implementation allows the library to eliminate leases on expensive multi-function devices (MFDs) for the public in favor of simple output devices (printers) that couple with the TBS scan hardware to increase the range of functionality. By implementing this technology, the library is able to efficiently combine several products (computer time management; print management; public cloud printing solution) into one product and save on costs associated with separate systems
X	Improved Data Quality	The combination of systems eliminated the need for a labor-intensive in-house print management solution and unified computer use and printing in a way that benefits patrons and streamlines IT support. Also, the simple fact of a computer time management system means that front-line public service staff does not have to actively manage or supervise computer use -- a significant staff time savings.
X	Time Savings	Reporting on both computer usage and printing (aggregate number of sessions; number of hours used/day/week/month/year; time of day used; number of pages printed, etc.) is made significantly easier and more meaningful with the unified system and single data access portal.

To achieve its intended purpose, Today's Business Solutions (TBS) Computer Time and Print Management (hereinafter referred to as “surveillance technology”) allows patrons to use their library card numbers to schedule sessions and log into library public computers, and manages the amount of time they can use the computers. When they log in, the technology uses an API connection to the library's patron database to validate that the person logging in is an authorized user in good standing. The technology also tethers any print jobs they might send from public computers to their log-in credentials (library card number, PIN) for ease of retrieval.

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*
Scanned Images	XML, PDF, HTM, Plain Text, TIFF, JPEG, PNG, GIF, CSV	Level 1-3

- Print/copy/scan: most level 1 - Examples of patron prints/scans/etc. listed previously (e.g., tax returns, medical records) could be classified as Level 3, depending on content.

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:

- Description of the authorized use
- Information on the surveillance technology

Patrons must accept the library's Rules for public computer use each time they log into the library's computers.

Both the Computer Use Rules and Responsibilities for the Public, which users accept when logging into library computers, and the ePrintIt portal for web printing, inform users that documents submitted to the TBS system may be retrieved for up to 24 hours, after which time they are purged from the system.

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):

- All public service staff have access to the computer reservation and print modules of the system. Only staff designated by the City Librarian and/or Chief Operating Officer and the Chief Information Officer have access to the reporting capabilities of the system where aggregate data is stored.

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 Chief Information Officer (1)
- 3634 Librarian III/Digital Strategist (1)
- 1095 IT Operations Support Admin V / Desktop Support (1)
- 1094 IT Operations Support Admin IV (1)
- 1093 IT Operations Support Admin III (5)
- 1823 Senior Administrative Analyst (1)

B. Members of the public, including criminal defendants

The Public Library 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.

The Department will not produce documents for a Sunshine Ordinance or California Public Records Act request if such request is directed at obtaining private patron documents sent for printing, scanning, or copying by library users; these documents are the private personal documents of the user; they are not related to library's normal course of business, nor are they considered city records.

The Department will follow its existing Privacy Policy with respect to subpoenas, USA PATRIOT Act requests, administrative orders and any such legal request by a judicial body of law.

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 Information Technology Division, under guidance from the Chief Operating Officer, maintains a list of staff with password-protected access to the aggregate data available in the TBS Computer Time and Print Management system, and reviews and 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 Department will endeavor to ensure that other agencies or departments that may receive data collected by The Public Library's Today's Business Solutions (TBS) Computer Time and Print Management 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 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 Public Library 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 Public Library 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:

Type	Recipient
Monthly and annual aggregate totals of public computer use by location.	Controller's Office: SFPL provides performance measures to CON twice a year that show monthly and annual computer use. These data are measured by the TBS Computer Time and Print Management system.

Data sharing occurs at the following frequency:

- Twice annually.

B. External Data Sharing

Department shares the following data with the recipients:

Type	Recipient
Monthly and annual aggregate totals of public computer use and print volumes by location in text format.	California Library Association, American Library Association, Public Library Association, Urban Library Council, and others upon request in accordance with California Public Records Act (CPRA) and San Francisco Sunshine Ordinance.

Data sharing occurs at the following frequency:

- Annually; 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 relevant privacy statutes at the federal, state, and local levels.

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 public computer use and print volume data is retained indefinitely for historical purposes.

PII data shall not be kept in a form which permits identification of data subjects for any longer than is necessary for the purposes for which the personal data are processed. PII data collected by the surveillance technology may be retained beyond the standard retention period only in the following circumstance(s):

- n/a

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

Data will be stored in the following location:

X Local Storage

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

Practices:

- N/A as data is kept permanently

Processes and Applications:

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

Staff accessing TBS Computer Time and Print Management are given a one-time training on how to use the software and proper use cases for accessing aggregate user data. This training includes but is not limited to: logging into the system; reviewing available dashboards; reviewing available report types; how to interpret data in the system; how to export data; uses for data.

COMPLIANCE

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

The Chief Information Officer (CIO) is responsible for monitoring the TBS Computer Time and Print Management system to ensure 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
- 0952 - Chief Information Officer

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 TBS Computer Time and Print Management within the system.
- Second Offense: Staff will be put on probation from using the system for 3 months.
- 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 St., San Francisco, 94102. They also can contact the library by phone 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 the 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.