Surveillance Technology Policy

Web Filtering Software
Juvenile Probation

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 Web Filtering Software (hereinafter referred to as "surveillance 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 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 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):

To monitor young people's use of the internet so that only content that is appropriate to their academic/vocational coursework is viewed.
To configure and apply web filters across devices used to enforce safe web searches.
To ensure that firewalls are not bypassed or hacked for unintended use of the department's network.

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

Surveillance Oversight Review Dates
PSAB Review: 10/5/2023, Recommended 2/22/2024
COIT Review: Recommended 3/21/2024
Board of Supervisors Approval: TBD

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

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

The web filtering tool enables the Department to protect the safety of young people housed in Juvenile Hall, who are under our care, by preventing access to content that may be harmful in the interest of public safety and the residents' well-being,

Description of Technology

The technology allows for the application of a web filter across all users, operating systems, and browsers - regardless of device type. It provides one interface to manage device assignments, track repair inventory, and generate analytics reports. It also allows the configuration of filtering policies across an entire group, in order to uniformly enforce web searches relating to the young persons' academic studies.

Resident Benefits

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

	Benefit	Description
☒	Education	The tool filters out content that is not conducive to completing their online academic coursework. The tool also enables filtering out content that may be harmful in the interest of public safety and the young peoples' well-being, including, - Social media, internet games, YouTube, chat rooms, instant messengers, Snapchat, blog websites, as well as anything depicting violence or nudity; - Messages or data that contain inappropriate, defamatory, discriminatory, obscene, pornographic, harassing or illegal material, and engaging in activity that may harass, threaten, or abuse others.
☐	Community Development	
☐	Health	
☐	Environment	

☐	Criminal Justice
☐	Jobs
☐	Housing
☐	Public Safety

Department Benefits

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

	Benefit	Description
☐	Financial Savings	
☐	Time Savings	
☐	Staff Safety	
☐	Data Quality	
☒	Other	The tool filters out content that is not conducive to completing online academic or vocational coursework. The tool also enables filtering out content that may be harmful in the interest of public safety and the young peoples' well-being.

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.

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.

Data Type(s)	*Format(s)*	*Classification*
Web pages that were visited/accessed	CSV or PDF formats	Level 2
Time/Date spent on each webpage(s)	CSV or PDF formats	Level 2

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

- System Administration & Staff Training:
  - 1093 - IT Operations Support Admin II
  - 1053 - Sr. IT Business Analyst
- Application Managers:
  - 8580 - Director of Facilities
  - 8578 - Assistant Director of Facilities
  - 8318 - Counselor 2
  - 8320/8562 - Counselor
  - 8322 - Sr. Counselor

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:

- System Administration & Staff Training:
  - 1093 - IT Operations Support Admin II
  - 1053 - Sr. IT Business Analyst
- Application Managers:
  - 8580 - Director of Facilities
  - 8578 - Assistant Director of Facilities
  - 8318 - Counselor 2
  - 8320/8562 - Counselor
  - 8322 - Sr. Counselor

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.

More specifically, Department training will include:

The following one-time onboarding services are provided by GoGuardian:
-Implementation: Device Deployment & Product Onboarding (software installation and internal set-up).
-Product Training Services: GoGuardian provides overview and training for Department IT staff.

Staff Training shall be conducted by Department IT Staff to reduce the possibility that the program is used contrary to its authorized use.
All authorized individuals requiring access will receive training on security policies and procedures prior to using the technology (e.g., small group meetings, 1-on-1s).

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: Staff Training shall be conducted by Department IT Staff to reduce the possibility that the program is used contrary to its authorized use. All authorized individuals requiring access will receive training on security policies and procedures prior to using the technology (e.g., small group meetings, 1-on-1s).

Technical Safeguards: Only authorized & trained staff shall have access to the GoGuardian web filtering tool.

Data Storage: Data will be stored in the following location:

- ☐ 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: Department will endeavor to ensure that other agencies or departments that may receive data collected by the surveillance technology 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.

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 from entities that do not have authorized access under this policy.

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 legal obligations.

Before sharing data with any recipients, 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.
- Consider alternative methods other than sharing data that can accomplish the same purpose.
- Redact names, scrub faces, and ensure all PII is removed in accordance with the department's data policies.
- Review of all existing safeguards to ensure shared data does not increase the risk of potential civil rights and liberties impacts on residents.
- 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.
- Ensure data will be shared in a cost-efficient manner and exported in a clean, machine-readable format.

A. Internal Data Sharing:

Data is shared on the following schedule:
X Need to know basis and/or pursuant to a court order

Data may be shared on a need-to-know basis and/or pursuant to a court order with:

-- Police Department,
-- District Attorney, and
-- Public Defender
pursuant to an ongoing investigation and/or court proceeding.

To ensure that entities receiving data collected by the surveillance technology comply with the Surveillance Technology Policy, Department shall: Comply with all applicable laws, rules, and regulations regarding the confidentiality of juvenile records.

Data sharing occurs at the following frequency: As needed.

B. External Data Sharing:

Data is shared on the following schedule:
X Need to know basis and/or pursuant to a court order

Data may be shared on a need-to-know basis and/or pursuant to a court order with:

-- Police Department,
-- District Attorney, and
-- Public Defender
pursuant to an ongoing investigation and/or court proceeding.

To ensure that entities receiving data collected by the surveillance technology comply with the Surveillance Technology Policy, Department shall: Comply with all applicable laws, rules, and regulations regarding the confidentiality of juvenile records.

Data sharing occurs at the following frequency: As needed.

Data Retention: Department may store and retain raw PII data only as long as necessary to accomplish a lawful and authorized purpose. Department data retention standards should align with how the department prepares its financial records and should be consistent with any relevant Federal Emergency Management Agency (FEMA) or California Office of Emergency Services (Cal OES) sections.

The Department's data retention period and justification are as follows:

Retention Period	Retention Justification
PII are not collected, shared, nor stored in GoGuardian. Summary Web Usage Reports, which contain deidentified data, are available to be reviewed by authorized staff only.	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, which mandates that records be destroyed or maintained for varying time periods depending on whether a petition was filed, the nature of the sustained offense, whether the record was ordered sealed and/or destroyed by the Court (and the dates so ordered by the Court), and the age of the subject of the petition. The minimum retention period is 2 years. 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 depending on whether a petition was filed, the nature of

	the sustained offense, whether the record was ordered sealed and/or destroyed by the Court (and the dates so ordered by the Court), and the age of the subject of the petition. See WICs 300, 601, 602, 389, 781, 786, 793, 786.5 and HSC 11357.

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.

Exceptions to Retention Period - PII data collected by the surveillance technology may be retained beyond the standard retention period only in the following circumstance(s):

- Data collected in the implementation of this 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 depending on whether a petition was filed, the nature of the sustained offense, whether the record was ordered sealed and/or destroyed by the Court (and the dates so ordered by the Court), and the age of the subject of the petition. See WICs 300, 601, 602, 389, 781, 786, 793, 786.5 and HSC. For program implementation purposes, the Department shall create and keep its own tracking document with the unique identifies set up in the web filtering software by Young Person's PIN. In this way, the technology's web usage reports could be linked to individuals, and thus be associated with the young person's juvenile hall record. These 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.

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

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

- Practices: PII is not entered nor stored in the technology. Deidentified and aggregated data in the form of usage reports will be for internal use only (Level 2). While every young person at Juvenile Hall who is a user and has a user ID or profile that can be associated with their name, this is not immediately associated with their name.

- When retention period ends, case files are shredded. When records are sealed, the Department instructs the vendor to remove all identifiers from the data.
- Processes and Applications: PII is not entered nor stored in the technology. Deidentified and aggregated data in the form of usage reports will be for internal use only (Level 2). While every young person at Juvenile Hall who is a user and has a user ID or profile that can be associated with their name, this is not immediately associated with their name.

COMPLIANCE

Department Compliance

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

The 8580 - Director of Facilities will be responsible for enforcing the Surveillance Technology policy through its incorporation into the overall Department policies. All staff involved in the implementation of the web filtering tool will be informed on this Surveillance Technology policy. Violation of the policy will be subject to standard JPD departmental policies, which may include disciplinary action up to and including termination. Every situation is evaluated on a case-by-case basis depending on circumstances surrounding any violations. 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.

Interdepartmental, Intergovernmental & Non-Governmental Entity Compliance

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

Share data on a need-to-know basis and/or pursuant to a court order

Oversight Personnel

Department shall be assigned the following personnel to oversee Policy compliance by the Department and third-parties.
8580 - Director of Facilities

Sanctions for Violations

Sanctions for violations of this Policy include the following:

Violation of the policy will be subject to standard departmental policies, which may include disciplinary action up to and including termination. Every situation is evaluated on a case-by-case basis depending on circumstances surrounding any violations.

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 Inquiries

Members of the 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 Department 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.

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.

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

To ensure that all questions and complaints are responded to in a timely matter, the Department shall follow the process outlined below: All complaints and questions are directed to the Chief Probation Officer wherein each inquiry is assigned a number and tracked according to AB-953 by date. A receipt letter is sent to each inquirer upon delivery of the inquiry to the Chief Probation Officer verifying that it has been received. The inquiry investigation is then assigned by the Chief Probation Officer to staff who will report back directly to the Chief Probation Officer. Once the inquiry has been investigated, a follow-up letter shall be sent to the inquirer, which will include outcomes from the investigation.

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.