

File No. 240893

Committee Item No. 2

Board Item No. 4

COMMITTEE/BOARD OF SUPERVISORS

AGENDA PACKET CONTENTS LIST

Committee: Rules Committee

Date Oct 28, 2024

Board of Supervisors Meeting

Date November 19, 2024

Cmte Board

- Motion
- Resolution
- Ordinance
- Legislative Digest
- Budget and Legislative Analyst Report
- Youth Commission Report
- Introduction Form
- Department/Agency Cover Letter and/or Report
- Memorandum of Understanding (MOU)
- Grant Information Form
- Grant Budget
- Subcontract Budget
- Contract/Agreement
- Form 126 - Ethics Commission
- Award Letter
- Application
- Form 700
- Information/Vacancies (Boards/Commissions)
- Public Correspondence

OTHER (Use back side if additional space is needed)

- Impact Report
- Technology Policy
- _____
- _____
- _____
- _____
- _____
- _____
- _____
- _____

Completed by: Victor Young

Date Oct 24, 2024

Completed by: _____

Date _____

1 [Administrative Code - Surveillance Technology Policy - Use of Web Filtering Software -
2 Juvenile Probation Department]

3 **Ordinance approving the Surveillance Technology Policy for Juvenile Probation**
4 **Department's use of web filtering software.**

5 NOTE: **Unchanged Code text and uncodified text** are in plain Arial font.
6 **Additions to Codes** are in *single-underline italics Times New Roman font*.
7 **Deletions to Codes** are in *strikethrough italics Times New Roman font*.
8 **Board amendment additions** are in double-underlined Arial font.
9 **Board amendment deletions** are in ~~strikethrough Arial font~~.
10 **Asterisks (* * * *)** indicate the omission of unchanged Code
11 subsections or parts of tables.

12 Be it ordained by the People of the City and County of San Francisco:

13 Section 1. Background.

14 (a) Administrative Code Chapter 19(B) establishes requirements that City departments
15 must follow before they may use or acquire new Surveillance Technology. Under
16 Administrative Code Section 19B.2(a), a City department must obtain Board of Supervisors
17 approval by ordinance of a Surveillance Technology Policy before: (1) seeking funds for
18 Surveillance Technology; (2) acquiring or borrowing new Surveillance Technology; (3) using
19 new or existing Surveillance Technology for a purpose, in a manner, or in a location not
20 specified in a Board-approved Surveillance Technology ordinance; (4) entering into
21 agreement with a non-City entity to acquire, share, or otherwise use Surveillance Technology;
22 or (5) entering into an oral or written agreement under which a non-City entity or individual
23 regularly provides the department with data or information acquired through the entity's use of
24 Surveillance Technology.

25 (b) Under Administrative Code Section 19B.2(b), the Board of Supervisors may
approve a Surveillance Technology Policy ordinance under Section 19B.2(a) only if: (1) the

1 department seeking Board approval first submits to the Committee on Information Technology
2 (“COIT”) a Surveillance Impact Report for the Surveillance Technology to be acquired or used;
3 (2) based on the Surveillance Impact Report, COIT develops a Surveillance Technology
4 Policy for the Surveillance Technology to be acquired or used; and (3) at a public meeting at
5 which COIT considers the Surveillance Technology Policy, COIT recommends that the Board
6 adopt, adopt with modification, or decline to adopt the Surveillance Technology Policy for the
7 Surveillance Technology to be acquired or used.

8 (c) Under Administrative Code Section 19B.4, the City policy is that the Board of
9 Supervisors will approve a Surveillance Technology Policy ordinance only if it determines that
10 the benefits that the Surveillance Technology ordinance authorizes outweigh its costs, that the
11 Surveillance Technology Policy ordinance will safeguard civil liberties and civil rights, and that
12 the uses and deployments of the Surveillance Technology under the ordinance will not be
13 based upon discriminatory or viewpoint-based factors or have a disparate impact on any
14 community or Protected Class.

15 Section 2. Surveillance Technology Policy for Juvenile Probation Department Use of
16 Web Filtering Software.

17 (a) Purpose. The Juvenile Probation Department (“SFJPD”) seeks Board of
18 Supervisors authorization under Administrative Code Section 19B.2(a) to use web filtering
19 software to: (1) to protect the safety of young people residing at the Juvenile Justice Center,
20 who are under the department’s care, by preventing access to content that may be harmful, in
21 the interest of public safety and the residents' well-being; (2) configure and apply web filters
22 across devices used by young people residing at the Juvenile Justice Center to enforce safe
23 web searches so that only content that is appropriate to their academic, vocational, or training
24 coursework is viewed; and (3) ensure that firewalls are not bypassed or hacked for
25 unintended use of the SFJPD network.

1 (b) Surveillance Impact Report. The Juvenile Probation Department submitted to
2 COIT a Surveillance Impact Report for Web Filtering Software. A copy of the Juvenile
3 Probation Department Surveillance Impact Report for Web Filtering Software is in Board File
4 No. 240893, and is incorporated herein by reference.

5 (c) Public Hearings. Between January 25, 2024, and March 21, 2024, inclusive, COIT
6 and its Privacy and Surveillance Advisory Board (“PSAB”) conducted three public hearings at
7 which they considered the Surveillance Impact Report referenced in subsection (b) and
8 developed a Surveillance Technology Policy for the Juvenile Probation Department’s use of
9 web filtering software. A copy of the Surveillance Technology Policy for the Juvenile
10 Probation Department’s use of the Web Filtering Software (“San Francisco Juvenile Probation
11 Department (SFJPD) Web Filtering Software Policy”) is in Board File No. 240893, and is
12 incorporated herein by reference.

13 (d) COIT Recommendation. On March 21, 2024, COIT voted to recommend the San
14 Francisco Juvenile Department (SFJPD) Web Filtering Software Policy to the Board of
15 Supervisors for approval.

16 (e) Findings. The Board of Supervisors hereby finds that the stated benefits of the
17 Juvenile Probation Department’s use of web filtering software outweigh the costs and risks of
18 use of such Surveillance Technology; that the San Francisco Juvenile Department (SFJPD)
19 Web Filtering Software Policy will safeguard civil liberties and civil rights; and that the use and
20 deployment of the web filtering software, as set forth in the San Francisco Juvenile
21 Department (SFJPD) Web Filtering Software Policy, will not be based upon discriminatory or
22 viewpoint-based factors or have a disparate impact on any community or a protected class.

23 Section 3. Approval of Policy.

24 The Board of Supervisors hereby approves the San Francisco Juvenile Probation
25 Department (“SFJPD”) Web Filtering Software Policy. Section 4. Effective Date. This

1 ordinance shall become effective 30 days after enactment. Enactment occurs when the
2 Mayor signs the ordinance, the Mayor returns the ordinance unsigned or does not sign the
3 ordinance within ten days of receiving it, or the Board of Supervisors overrides the Mayor's
4 veto of the ordinance.

5
6 APPROVED AS TO FORM:
7 DAVID CHIU, City Attorney

8 By: /S/ Jana Clark
9 JANA CLARK
10 Deputy City Attorney

n:\legana\as2024\2500053\01785372.docx

11
12
13
14
15
16
17
18
19
20
21
22
23
24
25

LEGISLATIVE DIGEST

[Administrative Code - Surveillance Technology Policy - Use of Web Filtering Software - Juvenile Probation Department]

Ordinance approving Surveillance Technology Policy for Juvenile Probation Department use of web filtering software.

Existing Law

Under Administrative Code Section 19B.2(b), the Juvenile Probation Department (“SFJPD”) must seek Board of Supervisors approval of a Surveillance Technology Policy to use web filtering software.

Amendments to Current Law

The proposed SFJPD Surveillance Technology Policy would authorize SFJPD to use the technology to (1) to protect the safety of young people residing at the Juvenile Justice Center, who are under JUV’s care, by preventing access to content that may be harmful in the interest of public safety and the residents' well-being (2) configure and apply web filters across devices used by young people residing at the Juvenile Justice Center to enforce safe web searches so that only content that is appropriate to their academic, vocational, or training coursework is viewed; and (3) ensure that firewalls are not bypassed or hacked for unintended use of the SFJPD network.

On January 25, 2024, and February 22, 2024, the Committee on Information Technology (“COIT”) and its Privacy and Surveillance Advisory Board conducted two public hearings at which they considered the Surveillance Impact Report for SFJPD’s use of web filtering software and developed a Surveillance Technology Policy.

On March 21, 2024, COIT voted to recommend that the Board of Supervisors adopt SFJPD’s Surveillance Technology Policy for the use of web filtering software.

This ordinance would approve the SFJPD Surveillance Technology Policy.



Surveillance Technology Policy

Web Filtering Software
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 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. 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
<input checked="" type="checkbox"/> 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.
<input type="checkbox"/> Community Development	
<input type="checkbox"/> Health	
<input type="checkbox"/> Environment	
<input type="checkbox"/> Criminal Justice	
<input type="checkbox"/> Jobs	
<input type="checkbox"/> Housing	
<input type="checkbox"/> Public Safety	

Department Benefits

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

Benefit	Description
<input type="checkbox"/> Financial Savings	
<input type="checkbox"/> Time Savings	
<input type="checkbox"/> Staff Safety	
<input type="checkbox"/> Data Quality	
<input checked="" type="checkbox"/> 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](#).

<i>Data Type(s)</i>	<i>Format(s)</i>	<i>Classification</i>
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.

– **Internal Data Sharing:**

Data is shared on the following schedule:

Need to know basis and/or pursuant to a court order.

Data may be shared on a need-to-know basis pursuant to an ongoing investigation and/or court proceeding with the following:

- Police Department,
- District Attorney, and
- Public Defender

To ensure that entities receiving data collected by the surveillance technology comply with the Surveillance Technology Policy, the 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.**

– **External Data Sharing:**

Data is shared on the following schedule:

Need to know basis and/or pursuant to a court order.

Data may be shared on a need-to-know basis pursuant to an ongoing investigation and/or court proceeding with the following:

- Police Department,
- District Attorney, and
- Public Defender

To ensure that entities receiving data collected by the surveillance technology comply with the Surveillance Technology Policy, the 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
<p>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.</p>	<p>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.</p> <p>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):</p> <p>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.</p>

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):
 - o 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.

- o 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 the 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.

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 <u>not</u> 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.

Surveillance Oversight Review Dates

PSAB Review: 10/5/2023, 2/22/2024

COIT Review: Recommended 3/21/2021

Board of Supervisors Approval: TBD



Surveillance Impact Report

Web Filtering Software
Juvenile Probation Department

As required by San Francisco Administrative Code, Section 19B, departments must submit a Surveillance Impact Report for each surveillance technology to the Committee on Information Technology ("COIT") and the Board of Supervisors.

The Surveillance Impact Report details the benefits, costs, and potential impacts associated with the Department's use of Web Filtering Software (hereinafter referred to as "surveillance technology").

PURPOSE OF THE TECHNOLOGY

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 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.

The Department shall use the surveillance technology only for the following authorized purposes:

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.

Surveillance technology may be deployed in the following locations, based on use case:

- The web filtering tool will be deployed only in the Secure Commitment Track Residential Units.

Description of Technology

This is a product description of the technology:

- GoGuardian allows for the application of a web filter across all users and operating system or browser regardless of device type - all from one interface. It provides an 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 enforce web searches relating to the young persons' academic studies.

This is a description of how the technology works:

- 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.

Third-Party Vendor Access to Data

Data collected or processed by the surveillance technology will not be handled or stored by an outside provider or third-party vendor on an ongoing basis. The Department will remain the sole Custodian of Record.

IMPACT ASSESSMENT

The impact assessment addresses the conditions for surveillance technology approval, as outlined by the Standards of Approval in San Francisco Administrative Code, Section 19B:

1. The benefits of the surveillance technology outweigh the costs.
2. The Department's Policy safeguards civil liberties and civil rights.
3. The uses and deployments of the surveillance technology are not based upon discriminatory or viewpoint-based factors and do not have a disparate impact on any community or Protected Class.

The Department's use of the surveillance technology is intended to support and benefit the residents of San Francisco while minimizing and mitigating all costs and potential civil rights and liberties impacts of residents.

A. Benefits

The Department's use of the surveillance technology has the following benefits for the residents of the City and County of San Francisco:

	Benefit	Description
<input checked="" type="checkbox"/>	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.
<input type="checkbox"/>	Community Development	
<input type="checkbox"/>	Health	
<input type="checkbox"/>	Environment	
<input type="checkbox"/>	Criminal Justice	
<input type="checkbox"/>	Jobs	
<input type="checkbox"/>	Housing	
<input type="checkbox"/>	Public Safety	

B. Civil Rights Impacts and Safeguards

The Department has considered the potential impacts and has identified the technical, administrative, and physical protections as mitigating measures:

The Department considers the Loss of Autonomy as a potential civil rights/liberties impact associated with the use of the web-filtering software for the following reason:

The young persons, whose web-activity will be monitored on a random basis, will not have control over what websites they visit other than those that are relevant to their academic/vocational coursework or that are safe and appropriate for viewing. Similarly, they will not be able to control the monitoring and viewing by Department staff of the websites visited.

The Juvenile Probation Department utilizes the web filtering tool only to fulfill our regulatory mandates as per Titles 15 and 24 to protect the wellbeing of young people in our care and establish protocols for communication with individuals outside the facility. All other uses are expressly prohibited.

The administrative safeguards are that 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). The technical safeguards are that only authorized & trained staff shall have access to the web filtering tool.

C. Fiscal Analysis of Costs and Benefits

The Department's use of the surveillance technology yields the following business and operations benefits:

Benefit	Description
<input type="checkbox"/> Financial Savings	
<input type="checkbox"/> Time Savings	
<input type="checkbox"/> Staff Safety	
<input type="checkbox"/> Data Quality	
<input checked="" type="checkbox"/> 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.

The fiscal cost, such as initial purchase, personnel and other ongoing costs, include:

Number of Budgeted FTE (new & existing) & Classification	System Administration & Staff Training: <ul style="list-style-type: none"> • 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 	
	Annual Cost	One-Time Cost
Total Salary & Fringe	\$0.00	\$0.00
Software	\$2,002.00	\$1,500.00
Hardware/Equipment	\$0.00	\$0.00
Professional Services	\$0.00	\$0.00
Training	\$0.00	\$500.00
Other	\$0.00	\$0.00
Total Cost	\$2,002.00	\$2,001.00

The Department funds its use and maintenance of the surveillance technology through: **General Fund.**

COMPARISON TO OTHER JURISDICTIONS

The surveillance technology is currently utilized by other governmental entities for similar purposes. Other government entities have used the surveillance technology in the following way: Marin County Probation Department also uses the technology for the same purpose in their adult education program and the San Francisco Juvenile Probation Department sought their experiences and insight with implementing the tool with their juvenile population. Additionally, the Oakland Unified School District also uses it on all laptops distributed by the district.

The effectiveness of the surveillance technology while used by other government entities is determined to be the following: The technology allows young people's free use of the Internet without the access of web-content that is unsafe. The technology has allowed other jurisdictions – both in juvenile justice and education settings - to operate their programs while ensuring that appropriate web-content is available to young people.

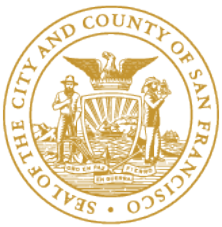
The Juvenile Probation Department utilizes the GoGuardian web filtering tool only to fulfill our regulatory mandates as per Titles 15 and 24 to protect the wellbeing of young people in our care and establish protocols for communication with individuals outside the facility.

Surveillance Oversight Review Dates

PSAB Review: 10/5/2023, 2/22/2024

COIT Review: Recommended 3/21/2021

Board of Supervisors Approval: TBD



City and County of San Francisco
Juvenile Probation Department

Web Filtering Software

Rules Committee Meeting

October 28, 2024

Technology Description

- The tool allows us to uniformly filter out certain websites across an entire group to only allow web searches relating to the young persons academic/training/vocational studies (e.g., during time of use of computer for online course/online training).
- The tool enables the Department to protect the safety of young people residing in the Juvenile Justice Center, 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.

Authorized Use Cases

Web filtering software shall be used to:

- monitor internet usage of young people residing at Juvenile Justice Center so that only content that is appropriate is viewed;
- configure and apply web filters across devices to enforce safe web searches;
- ensure that firewalls are not bypassed or hacked for unintended use of Department 's network.

Data Lifecycle Summarized

Type of Data Collected	<ul style="list-style-type: none">• Destination websites (no PHI, PII).
Who Has Access to That Data	<ul style="list-style-type: none">• Authorized Staff at the Juvenile Justice Center.
Who is the Data Shared with Outside of Dept	<ul style="list-style-type: none">• Shared with justice partners pursuant to an ongoing investigation and/or court proceeding including Police Department, District Attorney, Public Defender.
How Long Data is Retained by Dept	<ul style="list-style-type: none">• Retention of juvenile records guided by state law.• Records retention period varies depending on circumstances of young person's case.
How is Data Disposed	<ul style="list-style-type: none">• Shred documents that contain data when the retention period ends.• Sealed records: instruct vendors to remove all identifiers from the data, if applicable.

Other Notes

- Standard Procurement
 - *Tech Marketplace* (TMP): CRA, DT CIO, 19B reviews
- Privacy is Protected
 - Technology only captures the destination websites: no user data, no keystrokes, no PII/PHI.

PSAB Meeting Dates

- PSAB Meetings Attended:
 - 01/25/2024
 - 02/22/2024
 - PSAB Recommended Approval on 02/22/2024
- COIT Meetings Attended:
 - 03/21/2024
 - COIT Recommended Approval on 03/21/2024

Questions



Committee on Information Technology

Office of the City Administrator

To: Members of the Board of Supervisors
From: Carmen Chu, City Administrator
Katharine Petrucione, Deputy City Administrator

Date: April 24, 2024

Subject: Legislation introduced to approve Surveillance Technology Policy for the Juvenile Probation Department's Web Filtering Software

In compliance with Section 19B of the City and County of San Francisco's Administrative Code, the City Administrator's Office is pleased to submit the Surveillance Technology Policy for the Juvenile Probation Department's Web Filtering Software.

To engage the public in discussion on the role of government surveillance, the Committee on Information Technology (COIT) and its subcommittee the Privacy and Surveillance Advisory Board (PSAB) held 3 public meetings for Web Filtering Software between January and March 2023 to review and approve the policy. All details of these discussions are available at sf.gov/coit.

The following page provides greater detail on the review process for the Surveillance Technology Policy, and COIT's recommended course of action.

If you have questions on the review process please direct them to Katherine Millier, Chief Probation Officer or Shane Thomas, Director of Juvenile Facilities.

Web Filtering Software

Department	Authorized Uses
Juvenile Probation Department	<ol style="list-style-type: none"> 1. Protect the safety of young people residing at the Juvenile Justice Center, who are under JUV’s care, by preventing access to content that may be harmful in the interest of public safety and the residents' well-being. 2. Configure and apply web filters across devices used by young people residing at the Juvenile Justice Center to enforce safe web searches so that only content that is appropriate to their academic, vocational, or training coursework is viewed. 3. Ensure that firewalls are not bypassed or hacked for unintended use of the SFJPD network

Web Filtering Software Public Meeting Dates

Date	Meeting
January 25, 2024, and February 22, 2024	Privacy and Surveillance Advisory Board (PSAB)
March 21, 2024	Committee on Information Technology (COIT)

COIT recommends the following action be taken on the policy:

- Approve the Web Filtering Software Surveillance Technology Policy for the Juvenile Probation Department.



Katherine Weinstein Miller
Chief Probation Officer

September 10, 2024

To: BOS.Legislation@sfgov.org

From: Juvenile Probation Department – Ordinance approving Surveillance Technology Policy for Juvenile Probation Department use of Web Filtering Software

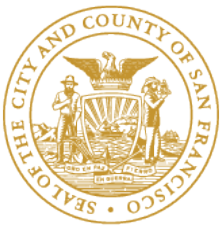
Attached is proposed legislation concerning and ordinance approving Surveillance Technology Policy for the Juvenile Probation Department's use of web filtering software.

Under Administrative Code Section 19B.2(b), the Juvenile Probation Department must seek Board of Supervisors approval of a Surveillance Technology Policy to use web filtering software.

The electronic attachments are listed below:

- 1_Cover Letter (this document)
- 2_Legislative Digest_JUV_9.10.24 (Legislative Digest)
- 3_Legislation_JUV_9.10.24 (Ordinance): includes /s/ signature from Deputy City Attorney (DCA)
- 4_COIT Recommendation
- 5_DCA approval as to form_9.10.24
- Surveillance Technology Policy
- Surveillance Impact Report

Staff Contact(s): Katherine W. Miller, Chief Probation Officer, (415) 753-7556
Verónica Martínez, Deputy Director of Administrative Services, (415) 680-8451
Shane Thomas, Director of Juvenile Facilities, (415) 417-4941
Elisa Baeza, Senior Contracts & Policy Analyst, (415) 753-7595



City and County of San Francisco
Juvenile Probation Department

Web Filtering Software

Rules Committee Meeting

October 28, 2024

Technology Description

- The tool allows us to uniformly filter out certain websites across an entire group to only allow web searches relating to the young persons academic/training/vocational studies (e.g., during time of use of computer for online course/online training).
- The tool enables the Department to protect the safety of young people residing in the Juvenile Justice Center, 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.

Authorized Use Cases

Web filtering software shall be used to:

- monitor internet usage of young people residing at Juvenile Justice Center so that only content that is appropriate is viewed;
- configure and apply web filters across devices to enforce safe web searches;
- ensure that firewalls are not bypassed or hacked for unintended use of Department 's network.

Data Lifecycle Summarized

Type of Data Collected	<ul style="list-style-type: none">• Destination websites (no PHI, PII).
Who Has Access to That Data	<ul style="list-style-type: none">• Authorized Staff at the Juvenile Justice Center.
Who is the Data Shared with Outside of Dept	<ul style="list-style-type: none">• Shared with justice partners pursuant to an ongoing investigation and/or court proceeding including Police Department, District Attorney, Public Defender.
How Long Data is Retained by Dept	<ul style="list-style-type: none">• Retention of juvenile records guided by state law.• Records retention period varies depending on circumstances of young person's case.
How is Data Disposed	<ul style="list-style-type: none">• Shred documents that contain data when the retention period ends.• Sealed records: instruct vendors to remove all identifiers from the data, if applicable.

Other Notes

- Standard Procurement
 - *Tech Marketplace* (TMP): CRA, DT CIO, 19B reviews
- Privacy is Protected
 - Technology only captures the destination websites: no user data, no keystrokes, no PII/PHI.

PSAB Meeting Dates

- PSAB Meetings Attended:
 - 01/25/2024
 - 02/22/2024
 - PSAB Recommended Approval on 02/22/2024
- COIT Meetings Attended:
 - 03/21/2024
 - COIT Recommended Approval on 03/21/2024

Questions