

Privacy initiative and procurement form (v2)

Fill out the form below when seeking approval for an initiative or procurement solution (referred to generally as “solutions”) that involves the collection, storage, processing, analysis, sharing, or other use of data or information (referred to generally as “usage of data”).

If any questions while filling out form, contact the Digital Privacy Officer. Once completed, email this form to the Digital Privacy Officer at digitalprivacy@sanjoseca.gov

Privacy review: Filled out by Digital Privacy Office

The Youth Intervention Services (YIS) under the Parks, Recreation and Neighborhood Services (PRNS) Department collects data on youth and shares with its partners to deliver case management, incident prevention and suppression, and other youth services to support the educational, health, and life outcomes of San José youth and their families.

Type of information collected can include

1. Individual demographic data, such as name, gender, age, parents names, family address and contact information, and any other relevant public safety information regarding the behavior of the person or people involved in a recorded incident;
2. Case Management Intervention services related data such as: Program enrollment and consent information, presenting problem, individual service plans and goals, services performed, units of service data, case notes, case closure information, and other relevant health and human service information from other service providers, etc.
3. Additional information provided to YIS by the youth, their families and/or legal guardian, their school, case management partners, and the City

Notice and express consent are required in all collection except during a safety incident in which YIS has been called by a school or other partner program to prevent or de-escalate a violent incident among youth.

This project is approved given the following:

1. Data is used to improve targeted City services for vulnerable youth and their families
2. Usage defined in a Data Usage Policy available to the public for ongoing comment.
3. Except in emergencies, data is only collected following explicit consent
4. Personal information is stored confidentially and only for as long needed to comply with youth needs and partner government requirements.

X *Albert Gehami*

Albert Gehami
Digital Privacy Officer

Section 1

Main point of contact for solution

Name (first and last): [REDACTED]

Department: Parks, Recreation and Neighborhood Services

Title: Community Services Supervisor

Email: [REDACTED]

Phone: [REDACTED]

Summarize the project below and how it uses data:

This should be a 1-3 sentence summary of the project. Further detail can be provided in Section 2 if required.

The Safe School Campus Initiative (SSCI) funded technology enhancement project will expand the scale of the SSCI program by adding and strengthening the incident alert and documentation technology capacity of the SSCI program.

Where is the data used originating? Mark all that apply by highlighting the in red

Public data sources (e.g., US Census, CDC, any data readily accessible online) – **list all public data sources used below**. For data accessed on the internet, provide a URL through which the data can be accessed. Do not provide a direct download link, but to the page that provides a download/export link.

Private data (not public) collected exclusively on City employees or programs (e.g., outcome metrics of a department or program); this includes publishing data for public viewing – fill out Section 2

Private data shared **from** a non-City entity (e.g., vendor) – fill out Sections 2 and 3

Private data shared **to** another non-City entity – fill out Sections 2 and 3

Collecting new data on non-City employees (either directly, via another department, or through a non-City entity) – fill out Sections 2 and 4

Section 2

If any data used is Private (i.e., not readily accessible to the public at this time), answer the following:

Will the solution involve the sharing of **Personally Identifiable Information (PII)** to a party (e.g., vendor, public)? PII includes any information that can directly or indirectly identify an individual, such as one's name or address. **Refer to the table on the following page for types of PII.**

Yes (mark the relevant PII categories and sub-categories on the following page)

No

Who will be able to access the personal information collected? Mark all that apply by highlighting the in red.

City staff

Third parties (list below): Members of School Safety Team (Police Officers, Probation Offices, School staff, District Attorney, Designated Service Provider(s))

General public (excluding via a Public Records Act Request)

If sharing data publicly, is there an underlying dataset which includes PII that is directly linked to the data shared?

For example, this [public map shows crimes in the 95113 zip code](#). However, the underlying data is anonymized before it is uploaded (names removed, location is connected to a City block, etc.) and if a hacker were to access the back-end of the website, they would only find the anonymized data.

Yes (mark the relevant PII categories and sub-categories below)

No

N/A – data is not shared publicly

Uncertain (contact the Digital Privacy Officer to discuss)

Detail which of the following Personally Identifiable Information (PII) this solution uses, mark all categories and subcategories that apply by highlighting the in red:

Category of PII	Sub-categories
<input checked="" type="checkbox"/> Personal Data	<p>General: <input checked="" type="checkbox"/> Full name; <input checked="" type="checkbox"/> Home address; <input checked="" type="checkbox"/> Date of birth; <input checked="" type="checkbox"/> Place of birth</p> <p>Technology: <input type="checkbox"/> Email address; <input checked="" type="checkbox"/> Phone number; <input type="checkbox"/> laptop, or other device IP¹ address; <input type="checkbox"/> Vehicle make, model and year</p> <p>Government-issued ID: <input type="checkbox"/> Driver’s License; <input type="checkbox"/> Passport; <input type="checkbox"/> Social Security Number; <input type="checkbox"/> Federal Employer ID or Tax ID; <input type="checkbox"/> Employee ID number; <input type="checkbox"/> License Plate</p> <p>Financial data: <input type="checkbox"/> Credit or debit card information; <input type="checkbox"/> Bank account, brokerage account or other financial information</p> <p><input type="checkbox"/> Other written or scanned information that can directly tie to an individual or household – detail below:</p>
<input checked="" type="checkbox"/> Sensitive PII or demographic-related PII	<p>Health data: <input type="checkbox"/> Biometric data; <input type="checkbox"/> Genetic data; <input type="checkbox"/> Physical identifiable characteristics; <input type="checkbox"/> Other health records</p> <p>Race/Ethnicity: <input checked="" type="checkbox"/> Race or ethnic origin; <input type="checkbox"/> Nationality; <input checked="" type="checkbox"/> Immigration status</p> <p>Religion/Politics: <input type="checkbox"/> Religious affiliation; <input type="checkbox"/> Political affiliation; <input type="checkbox"/> Voter status</p> <p>Sensitive personal records: <input checked="" type="checkbox"/> Education records; <input checked="" type="checkbox"/> Criminal records</p> <p><input type="checkbox"/> Other sensitive written or scanned information traditionally kept confidential – detail below:</p> <p>NOTE: Do not mark if data is only shared/collected/used in aggregate of a population larger than 1,000² (e.g., # of registered voters in San José)</p>
<input checked="" type="checkbox"/> Image data	<p><input checked="" type="checkbox"/> Picture that can identify an individual by their face or other physical and contextual information³ - detail below: student picture may be included as part of the education records</p>
<input type="checkbox"/> Recording data	<p><input type="checkbox"/> Video that can identify an individual by their face or other physical and contextual information – detail below:</p> <p><input type="checkbox"/> Audio that can identify an individual by their voice or other contextual information – detail below:</p>
<input type="checkbox"/> Geolocation data	<p><input type="checkbox"/> Data affiliated with a vehicle, computer, or other device that can be used to identify an individual’s physical location – detail below:</p>

¹ Internet Protocol - An IP address is a unique address that identifies a device on the internet or a local network

² Based on reporting requirements used for anonymity by the US Department of Health and Human Services [AFCARS Foster Care Dataset](#); refer to the [2021 codebook, element #6](#)

³ An example of “contextual information” being used to identify someone could include a picture of a license plate, car make model and year, or a picture of someone’s backside next to a house with a visible address.

Category of PII	Sub-categories
<input type="checkbox"/> Other private or personal information	<i>Detail other data that could directly or indirectly identify an individual:</i>

Project context and purpose:

What is the issue this project is looking to address? What is the question this project is trying to answer? What is the opportunity or new benefit this project is meant to create?

The SSCI technology enhancement project would expand the scale of the Youth Intervention Unit (YUI) safety and case management intervention programs by adding and strengthening safety incident and case management intervention documentation technology capacity of the YIU programs. The *technology enhancement project* would replace a manually maintained labor intense database system (Excel), with a customized and automated comprehensive database that would automatically document safety activation incident, and case management intervention data and information, allowing the YUI to more efficiently analyze and report service delivery data, and other related data requirements such as, population profiles, service and community geographic trends. Currently, the school/community and case management intervention documentation and report generation steps are manually conducted, requiring data be entered and tabulated several times by different people for different purposes and reports. The incident automated database system proposed would reduce manual time of handing data (labor intensive), as well, reduce the potential for error.

Data collected/shared:

Summarize what data is being collected. This should include the Personally Identifiable Information categories that you marked in the table above.

Type of information collected can include: 1) Individual demographic data, such as name, gender, age, parents names, family address and contact information, any other relevant public safety information regarding the behavior of the person or person’s involved; 2) Case Management Intervention services related data such as; Program enrollment and consent information, presenting problem, individual service plans and goals, services performed, units of service data, case notes, case closure information, and other relevant health and human service information from other service providers, etc.

Disciplinary information, school info, services delivered

Data Usage:

How will the data be used? What are the usage limitations? Will this data regularly be used for law enforcement purposes, or will it only be used for law enforcement purposes when required by law?

The data and information in the database and case management system would be used primarily for service delivery and reporting purposes. The system would not be made available to other parties without proper legal consents documented, and/or court ordered documents required by law. The only exception, is the YIU School/Community safety program, where only Safety Team members (so designated) are allowed share among themselves only confidential intelligence and information regarding an active violent incident case in real time. The program operates under the authority of

California 830.1 Welfare and Institutions Code which guides the structure and operation of a School Safety Multi-Disciplinary Team, and abides to strict confidentiality standards.

Data Retention:

How long will the data be kept? What relevant policies (e.g., laws, statutes, our City Retention Schedule) inform retention?

Personal information will be retained for at least 2 years in accordance with California Government Code 34090, but may be retained for longer if required by a government agency or grant provider, or if the youth and/or their family remains involved YIS and its partner programs. Personal information will be deleted from all City systems no later than 2 years after a youth and/or their family have stopped receiving services from YIS and its partner programs, and the data is no longer required by a court order, government agency, or other grant provider.

Access to the data:

Who will have access to the data? Is it just City departments, or will vendors or other partners have access? Who can access the data to edit or correct information?

The City Department of Parks, Recreation and Neighborhood Service (and in particular; Youth Intervention Services Superintendent), control the access levels (direct service levels, management levels data) to the data system.

Notice:

How will individuals be notified that their data is being collected and how it will be used?

The YIU Case Management Intervention program services maintain a program intake and enrollment process that require parent/guardian consent for minors' involvement in the programs. Young adults are also required to consent prior to receiving program services. The consent forms include a description of what the program service entitle, and that client information will be kept of the client. The consent form also states that approval will be secured from client or parent prior to release of information (unless prevention of harm to self or other is involved.) When the Safe School program incident protocol is activated and the program is contacted by a school site personnel, staff are sent to the school to evaluate and if required intervene in the situation. The school personnel are the lead in making appropriate student and or parent notifications of incident under their authority granted schools. This notification may also include the involvement of SSCI staff role in intervening and follow-up student or family support service. If SSCI program is involved in follow-up support services, they secure written parental approval.

Selling data:

Will any of the information be sold by the City or a third-party? Tip: This should be no, otherwise project is likely to be rejected.

Yes

No

Section 3

If using private data shared from or to another department or non-City entity, answer the following:

Does this solution involve the sharing of any PII as defined in Section 2?

Yes – answer additional questions below

No

If yes, answer the questions below:

Does this solution’s new usage of data stay consistent with the existing purpose of the data shared?

Yes No Unclear

For example, if full name and email address were initially collected to sign up for a Parks mailing list, a solution that sends the emails for this mailing list may be consistent with the existing purpose. However, using the data for a different mailing list would be inconsistent and require an updated privacy notice to the data subjects (data subjects would be the individuals who provided their full name and email address).

Attach the Privacy Notice which details the existing purpose and usage of the data shared.

Attached Could not locate notice or notice does not exist

If Notice is not attached, please provide detail (if available) about the existing purpose, data usage and Privacy Notice below:

Privacy Notice has been developed as part of this review, and is now included as part of the release form when registering new youth.

Attach the additional or updated Privacy Notice which details the new purpose of the data used in this solution

Attached Could not locate notice or notice does not exist

If Notice is not attached, please provide detail (if available) about the new purpose, data usage and Privacy Notice below:

No additional usage beyond stated purpose

Section 4

If collecting new information, either directly or through another department or non-City entity, answer the following:

Will the data subject (individual which is the focus of the data collected) be provided a Privacy Notice upon collection?

Yes No

Note: The notice should inform the individual what is being collected, how it will be used, who can access it, how long it will be stored, and who they can contact for further information or for requesting edits to their data. Often this is covered in the terms and conditions.

Will the data subject be required to give “express consent” for the data collected?

Yes No

Note: “Express consent” differs from a Notice in that for consent a data subject must explicitly agree (usually in writing) to the data usage outlined in the Notice. This can be done via a signature, a check box online, or other explicit method. Providing Notice only requires that the Notice be easily accessible to the data subject, and the data subject is made aware of the Notice and given the opportunity to read the Notice before data collection

If the data subject is not provided a Notice before data collection, explain why below. For example, is the data being collected as part of an arrest, or an emergency response?

The SSCI response to a school call requires that they conduct a Threat Assessment of the situation to determine if violence may occur or to de-escalate a violent occurrence. The school may or may not notify a subject unstill after an assessment is completed. The SSCI operates under the authority of California 830.1 Welfare and Institutions Code which guides the structure and operation of a School Safety Multi-Disciplinary Team, and abides to strict confidentiality standards.

Attach the Privacy Notice (a digital copy or a scan of a physical copy) that will be provided to the individual upon collection.

Attached Could not locate notice or notice does not exist

If Notice is not attached but still provided, please provide detail (if available) about the purpose, data usage and Privacy Notice below:

Privacy Notice has been developed as part of this review, and is now included as part of the release form when registering new youth.