City of San José Digital Privacy Precedent

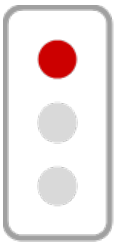
Whenever a City department wishes to adopt a new technology, that technology must be reviewed by the Digital Privacy Officer to ensure it follows the City's Digital Privacy Policy.

Below is a non-exhaustive list of technologies that have been reviewed by the Digital Privacy Officer. Some technologies are outright rejected because they do not align with the City's Digital Privacy Policy. Some technologies are approved with a brief review because they do not present any significant privacy risks. Other technologies are approved after an additional review process to ensure that the technology is used to support residents and adheres to the Digital Privacy Policy.

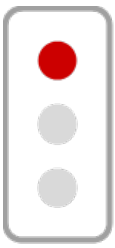
Definitions and abbreviations:

- Personally Identifiable Information (PII): Information that can identify someone and provide personal information, such as someone's name, home address, and phone number
- SSN: Social Security Number
- Artificial Intelligence (AI): Automated identification made by a computer. For example, an AI-based traffic camera might be able to automatically count the number of cars that pass an intersection.
- City: The City of San José

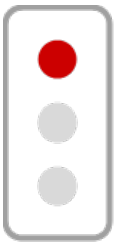
Not approved



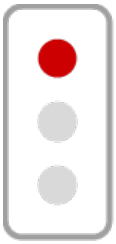
City installs smart light poles to capture video footage
Rejected due to poor set-up and questionable security protocol
A vendor offered a smart light pole pilot complete with cameras and sensors for 10 light poles, with plans to expand to the rest of the City. During privacy review, the system security was found to be insecure in its handling of sensitive video information and consequently rejected.



Private vendor offers tracking bands to schoolchildren to monitor child activity
Rejected given sensitivity of tracking child data
A vendor offered to pay the City $10,000 to offer light bands to children to track their health information, location, and other information while the child is at school. This proposal was rejected given the high sensitivity of children's information and unclear value to the school, the students, and their families in exchange for the data.



Private vendor offers cameras to identify and track homeless individuals
Rejected due to highly invasive monitoring without necessity
A vendor would use cameras in public areas to identify and track individuals experiencing chronic homelessness. This proposal was rejected given the highly invasive nature of ongoing monitoring of targeted individuals that did not pose an immediate threat to life, serious injury, nor serious property damage.

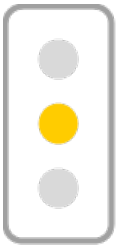


Private vendor sharing of data from the City in Automated License Plate Reader vendor's shared database

Rejected given the potential for other jurisdictions to use City data for prohibited uses

A vendor would share the City's Automated License Plate Reader (ALPR) pictures and data with the vendor's shared cloud database accessible to all law enforcement agencies using the system. This proposal was rejected because it would have enabled other police agencies to access the City's ALPR reads without City approval, and it may be used for prohibited activities, such as to investigate an individual's immigration status. Only the City may agree to share its ALPR data with other law enforcement agencies within the State of California on an agency-by-agency basis.

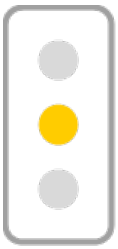
Approved with further review



Fire Department collection of name, address, and basic contact info to provide Fire inspection services

Approved after review because all information is necessary and usage is defined

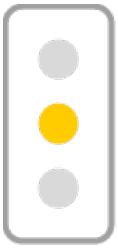
This project stores resident names, address, and basic contact information to provide Fire inspection services. Address is needed to assign the location of the inspection, and name and contact information are needed to contact the owner of the property. Information is used internally and not made public. This proposal was approved since all personal information is necessary for the service, used in the interests of the communities inspected, and kept confidential unless required by law.



Department of Public Works collection of Social Security Number and other PII to ensure compliance with labor laws and monitor work performance

Approved after review given usage, informed consent, and confidential storage

The Office of Equality Assurance (OEA) receives employment data on contractors to enforce local labor requirements (e.g., living wage), track work outcomes and performance, and analyze worker demographic trends. The data collected in this project includes payroll data, employment information including Social Security Number, and basic information including name and contact information. The project was approved given that the data is used to improve City services and comply with local requirements, the data is acquired with explicit consent, and PII is stored confidentially for a defined retention period of 5 years.

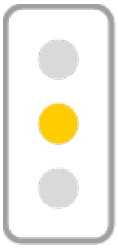


Department of Transportation use of AI-recorded metrics for traffic monitoring

Approved after review given limited video stored, no audio, and long-term metrics are anonymous.

The Department of Transportation would use AI-enabled cameras to assess safety metrics and conditions of an intersection before and after safety counter measures are implemented collect traffic data to improve traffic management.

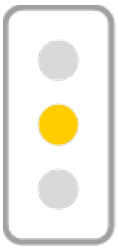
No audio is recorded, and only clips of video are stored to verify if a safety incident, such as a near-miss crash, occurred. This is approved so long as only small clips of video are kept, no audio is collected, and all other data containing images is deleted. The full data practices are provided in the Data Usage Protocol.



Parks, Recreation and Neighborhood Services and Youth Intervention Services use of a tool that processes PII to provide essential youth services

Approved after review given usage and secure storage of PII

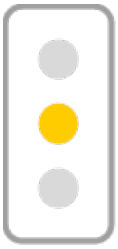
The Parks, Recreation and Neighborhood Services Department (PRNS), its Youth Intervention Services (YIS), and its partner programs deliver case management, incident prevention and suppression, and other youth services to support the educational, health, and life outcomes of San José youth and their families. A data management system would be used to provide the services and connect youth with partner programs. Since the data is necessary to provide critical youth services, safeguards would be established to ensure that the data is stored in a secure cloud environment, the data will only be shared with partner service providers, among other protocols. The proposal was approved since the department and Digital Privacy Officer crafted acceptable usage conditions under the Data Usage Protocol.



Police Bomb Squad use of X-Ray detector kit for bomb detection

Approved after review because X-Ray tool focuses only on devices that do not present PII risks

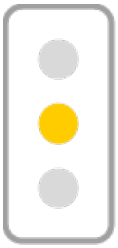
This proposal would allow the Police Bomb Squad to use a device that records and processes X-Ray video. Since the device would be directed at physical objects (i.e. potential bombs) and not directed at locations that would receive significant amounts of PII, such as towards people, the proposal was approved.



Community Energy Department purchases data on energy prices

Approved after review given no PII involved, vendor collected data separately from work with the City

The vendor provides the Community Energy Department (CED) with "price forward curve" data, which informs CED how much it costs to buy energy (such as oil, wind, or natural gas) that will be delivered in the future (e.g., in a month, year, or two years). The data involved is purchased from a vendor and does not include any data collected by the City or on behalf of the City. The data does not include personally identifiable information and serves a necessary purpose for CED to purchase energy for San José residents, so it is approved by the Digital Privacy Officer. Since the vendor creates the forward curves data separate from any working relationship with the City, the data is considered to be owned by the vendor rather than the City.

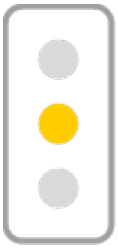


Police Department use of Automated License Plate Readers at traffic intersections

Approved after review given Privacy Impact Assessment, public comment, and Council approval

To reduce traffic accidents and support investigations, the City would install Automated License Plate Reader (ALPR) cameras around intersections and on roads. The City would use recorded data to prosecute major crimes like hit and runs, car theft, and to monitor the intersection to improve safety. The City would not use the data to monitor individuals, or automatically enforce crimes without human oversight. Signage is required in the area where ALPR cameras are installed to provide notice to residents.

Following a Privacy Impact Assessment that defined the data usage and protocol for ALPR, generally positive response from the public via online comment and in-person outreach to ~100 community organizations, 5 neighborhoods identified as areas to install cameras, and over 200 families, the project has been approved. The final Data Usage Protocol is set to be reviewed by Council on Sept 13th.



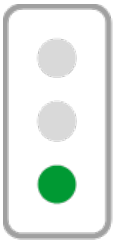
Police Department use of fingerprint and evidence management system

Approved after review given security measures and conditional usage protocol

The Police Department would utilize a fingerprint and evidence management system primarily containing fingerprints and pictures of fingerprints. Data stored in the management system would only be accessed by authorized individuals and stored in an environment approved by the City's cybersecurity team.

The database would serve to store and maintain evidence for ongoing investigations and in the event of criminal action. Data from the management system would only be made available as required by law. Given the limited usage of the data, confidential security, and ongoing need for criminal investigations, the fingerprint management system was approved.

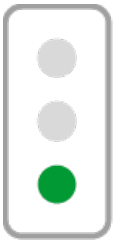
Approved with a brief review



City Department purchase of scanner for office use

Approved with a brief review because no PII implicitly collected

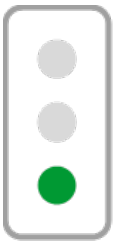
A scanner, photocopier, fax machine, computer, etc. on its own is not a Privacy Risk since the device does not automatically collect Personally Identifiable Information (PII), nor is it heavily implied that the device will be used to collect PII. The scanner serves to make a copy of existing information to be stored in an existing approved space with its own role-based access controls.



City Library purchase of laptops for public use

Approved with a brief review because no data is actively collected by or on behalf of the City

Minimal or no personally identifiable information is being stored, processed, or otherwise used for this initiative. While the technology can collect personal information, only personal information that the user actively and willingly provides to the technology will be collected.



Airport renewal of software used to generate reports on existing data

Approved with a brief review because data continues to be used for intended purpose

No additional privacy risks are presented by the reporting analytics from data already collected, processed, or otherwise generated in the approved course of City business, assuming the data is used in accordance with the original purpose outlined during collection.