City of San José, California

COUNCIL POLICY

TITLE Digital Privacy Policy	PAGE 1 of 5	POLICY NUMBER
EFFECTIVE DATE 12/08/2020	REVISED DATE	
APPROVED BY COUNCIL ACTION		

PURPOSE

The purpose of this Policy is to safeguard the public's trust in the City's use of new and emerging technologies and to protect their digital privacy rights. It sets forth the framework for City departments to observe when information systems or other applications and forms collect the public's Personally Identifiable Information (PII), as defined in Appendix A. This Policy strives, to the extent practicable, to enable residents to determine for themselves when, how and to what extent information about them is communicated to others.

As new and emerging technologies have a greater capacity for collecting information and drawing insights about people and communities, a Digital Privacy Policy will enable the City to harness the power of those insights to provide better services to the community while ensuring that personal and sensitive information is properly protected.

POLICY

It is the Policy of the City to protect the privacy of individuals and the digital form of any Personally Identifiable Information that is collected, used, shared, or stored by the City. In addition to this Policy, the City is also subject to laws and regulations that govern the collection, storage, and retention of information.

To the extent permissible by law, City departments will adhere to the Privacy Principles, and this Policy based on those Privacy Principles including the following elements to protect individual privacy:

- **Notice**: Providing notice about the collection, use, and sharing of personal information at the time such information is collected. The City will make every reasonable effort to provide a privacy notice when basic municipal services are requested or delivered.
- **Retention**: Developing, maintaining, and following the City data retention schedule. Departments must ensure that identifying information is deleted or deidentified after the retention period expires. In the event of a conflict between this Policy and the Public Records Act, Sunshine Act, or other law governing the disclosure of records, the

applicable law will determine our obligation in support of open and transparent government. *See* California Public Records Act.

- **Minimization**: Minimizing the collection and processing of identifying information and limiting collection to only what is necessary to provide services and to conduct business. When personally identifiable data is required to deliver or improve a service, departments must anonymize, de-identify, pseudonymize, or otherwise mask this information.
- **Accountability**: Maintaining documentation, available for public review and third-party monitoring, to demonstrate compliance with our privacy principles and Policy. If any information under our control is compromised or if residents are impacted due to a breach of security or negligent maintenance of information systems, the City will take reasonable steps to investigate the situation and notify those individuals whose information may have been impacted.
- **Accuracy**: Making every reasonable effort to provide the public with information on how predictive or automated systems are used and will institute processes to correct inaccurate information or methodologies in those systems. City Departments may use predictive or automated systems and technologies to support decision making, but some degree of human input and oversight into decision making is also required.
- **Sharing:** Following clear data governance procedures and instituting information sharing agreements when sharing information with outside entities, which shall strive to enable effective information sharing while following the City's Privacy Principles and this Policy. Nothing in this policy shall preclude data sharing with research or other institutions as long as clear data sharing agreements are in place which govern the use of data pursuant to the standards of this Policy.
- **Equity**: The City is mindful of the populations it serves and how data about members of the public, including vulnerable populations, can and should be used. The City will strive to advance equity in a data-driven way while ensuring that PII is used only in accordance with this policy. The City will work to mitigate the impact of algorithmic and data bias.

Application

This Policy is effective 180 days after approval by the City Council or July 1, 2021 ("effective date") whichever is later, and it applies to all departments and employees of the City.

The Smart Cities and Service Improvements Committee of the City Council shall be responsible for ensuring accountability for digital privacy by reviewing progress and monitoring the City's digital privacy efforts.

The City Manager will designate a Chief Privacy Officer position to lead the citywide implementation, maintenance, and adherence to the Digital Privacy Policy in coordination with

the Chief Information Security Officer and City departments. The Chief Privacy Officer and Chief Information Security Officer shall adjudicate technologies and projects according to this Policy.

Implementation of the Policy shall include at least the following:

(i) Development of procedures for prioritizing and executing the evaluation of privacy risks for new projects and vendor contracts according to this Policy, the City's Privacy Principles, and the interests expressed by the City Council and community members; and

(ii) Privacy review and assessment processes to aid departments and information system owners in ensuring that digital privacy standards in this Policy are integrated into technologies, projects, processes, and vendor contracts.

At the recommendation of the Chief Privacy Officer and Chief Information Security Officer and in accordance with the standards in this Policy, the City Manager may require departments or offices to effect modifications to technologies or projects to comply with this Policy.

Exceptions

Due to the individualized and serious nature of emergency response efforts, a variety of personally identifying information may be collected by first responders and other personnel, as needed, and such data collection, use and disclosure practices may fall outside of the scope of this Privacy Policy. Emergency call centers may also follow different protocols during responding to emergency calls. Whenever possible, our emergency responders will attempt to honor the City's Privacy Principles, and all activities by first responders or other personnel shall be in accordance with the applicable provisions of relevant law, including the 4th, 5th, 6th, and 14th amendments to the United States Constitution.

This Policy does not apply to personal/personnel information obtained in the City's capacity as an employer. Employment information is covered under separate Human Resources policies.

The Notice section of the Policy does not apply to Police and Fire Departments, as they are covered by separate policies. This Policy specifically does not preempt policies already in existence at the departmental level. This Policy is intended to implement and enhance local, state, and federal laws and regulations that apply to the City.

Confidentiality, Anonymity, and Open Government Standards

New information systems acquired after the effective date of this Policy should, to the extent practicable, have the ability to anonymize, de-identify, or pseudonymize personally identifying information in such a way that it no longer can be related back to a given individual. When

updating existing legacy systems, the City shall make a reasonable effort to ensure that such systems have the ability anonymize, de-identify, or pseudonymize this information.

This Policy follows the City Council's Open Data Policy (0-43). For the purposes of government transparency, and consistent with the intent of the California Public Records Act and the City's Sunshine Ordinance, the City posts some data sets to our Open Data portal, data.sanjoseca.gov.

Authorities and Responsibilities

The City is supportive of the California Consumer Privacy Act (CCPA), and this Policy does not substitute nor alter the obligations of all vendors working with the City who fall under the eligibility criteria of the CCPA.

The Chief Privacy Officer and Chief Information Security Officer will review this Policy annually for updates and bring forward updates for review by the Smart Cities and Service Improvements Committee and City Council as necessary.

APPENDIX A: DEFINITIONS

Personally Identifiable Information (PII): Information collected by the City that can directly or indirectly identify individuals can be classified into five primary categories of data:

1. **Personal data:** information relating to an individual, such as full name, street address, email address, and personal computer or mobile device IP address.
2. **Sensitive or demographic data:** subsets of personal data that require extra security and care, such as biometric or genetic data, racial or ethnic origin, and religious or political affiliations.
3. **Image data:** digital pictures or photographs that can identify an individual by their face or other contextual information.
4. **Recording data:** audio or video information that can identify an individual by their face, voice, or other contextual information.
5. **Geolocation data:** information affiliated with a computer, device, or vehicle that can be used to identify an individual based on physical location or on aggregate location patterns.

Tracking Technology: Any technology that collects, stores, or transmits personally identifiable information, location or spatial data, images, or recordings that can be used to identify, monitor, surveil, make inferences about, or predict the behavior of individuals.