



## City of Seattle Privacy Program

October 2015

As we strive to create a safe, affordable, vibrant, innovative, and connected city, we must also explore ways to build trust about the ways we collect and manage the public's personal information. The City of Seattle Privacy Program establishes leading practices to protect privacy and increase City staff awareness.





## City of Seattle

From the Office of Edward B. Murray, Mayor



Data is a critical component to helping become a safe, affordable, vibrant, connected, and innovative city. It can help us measure the effectiveness of government services, identify communities in need of assistances, and make better decisions. Modern technology increases our ability to collect data from individuals and the built environment, and initiatives like our open data program aim to proactively make City data available for public benefit.

Yet the public is increasingly wary of how government entities collect and use their personal information. The City has not consistently communicated why we collect data or had. The City of Seattle has an obligation to earn the public's trust in how we the collection – and we can do better. Last year members of the City Council and I asked the City's Department of Information Technology (DoIT) and Seattle Police Department (SPD) to develop a City-wide Privacy Program, and I am pleased to share with you the results of their effort.

Based on an ethical policy and governance framework for addressing current and future issues as technologies and capabilities as they continue to evolve across all lines of the City's business, this program includes a broad, consistent set of principles to address the collection and management of personal information throughout its lifecycle to help protect the public's privacy. It also includes a review process for privacy impacting technologies and programs and a toolkit of resources to provide guidance and direction for City employees to incorporate privacy considerations into everyday operations.

This program will provide the structure and guidance required for City departments to incorporate the appropriate privacy practices into daily operations and to build public trust and confidence in how we collect and manage the public's personal information. My 2016 budget proposal to Council includes several resources to enable the program's implementation, including funding for all City employees who handle personal data to complete privacy awareness training and a new Chief Privacy Officer role.

We look forward to working with our employees, partners, and the community to drive awareness of and participation in our Privacy Program, and sharing the results of our work.

Sincerely,

Edward B. Murray

## Table of Contents

I. HISTORY OF THE PRIVACY PROGRAM.....	4
II. PROGRAM DEVELOPMENT APPROACH.....	5
III. WHAT IS PRIVACY? .....	6
IV. PRIVACY PRINCIPLES.....	7
V. PRIVACY REVIEW PROCESS .....	8
VI. ROLES AND RESPONSIBILITIES .....	9
VII. RESOURCES.....	10
APPENDIX 1: PRIVACY WORKGROUPS.....	11
APPENDIX 2: SUMMARY PRIVACY STATEMENT .....	12
APPENDIX 3: FULL PRIVACY STATEMENT .....	13
APPENDIX 4: PRIVACY INTAKE AND REVIEW FORM.....	23
APPENDIX 5: PRIVACY IMPACT ASSESSMENT.....	28
APPENDIX 6: PRIVACY PROGRAM FACTS AND QUESTIONS.....	34

# I. History of the Privacy Program

The City of Seattle increasingly interacts with the public by collecting and exchanging data. The collection of data occurs in every day City processes, such as paying a utility bill, renewing a pet license, browsing a web page, or signing up for an email list. Police, fire and emergency services to collect different forms of video and electronic data. We have recognized that the increasing complexity of emerging technologies, business systems and the laws pertaining them means the City must take appropriate steps to facilitate the collection, use, and disposal of data in a manner that balances the needs of the City to conduct its business and individual privacy, and in a manner that builds public trust.

## Technology's impact on privacy

Technologies including unmanned aircraft (drones), wireless communications networks and various forms of image capture such as surveillance and body-worn cameras while useful to aspects of our mission to protect people and property can conflict with privacy. Programs outside of public safety such as advanced metering for utilities, traffic monitoring tools and cloud-based applications also represent advances in the use of technology to provide services, but evaluated against the potential impacts on the public's privacy.

### Privacy Program

**Mission**

Build public trust about the use and management of personal information.

**Our Vision**

Work to find a fair balance between gathering information to provide needed services and protecting the public's privacy.

## Executive request and outcome

The outcome of this yearlong effort, instigated at the request of both the Mayor and City Council, is the program outlined in this document. The Privacy Program is based on an ethical policy and governance framework for addressing current and future issues as these technologies and capabilities continue to evolve across all lines of the City's business. This includes a broad, consistent set of principles to address the collection and management of personal information throughout its lifecycle to help ensure the public's privacy. It also includes a review process for privacy impacting technologies and programs and a toolkit of resources to provide guidance and direction for City employees to incorporate privacy in to everyday operations.

## II. Program Development Approach

To inform this process, we convened an external advisory group and an internal working group.

The Privacy Advisory Committee, comprised of Seattle-based academic and community privacy thought leaders served as best-practice advisors during this time. Starting in September 2014, a group of internal stakeholders from across City departments including Police, Fire, City Light, Transportation, Information Technology, Law, and Seattle Public Library worked over the next year to create a set of Privacy Principles and an

expanded privacy statement to communicate the City's privacy practices to the public. They also created an operational toolkit for driving awareness and compliance across City departments, determined an approach to educating City departments about privacy practices, and instituted a formal privacy review process.

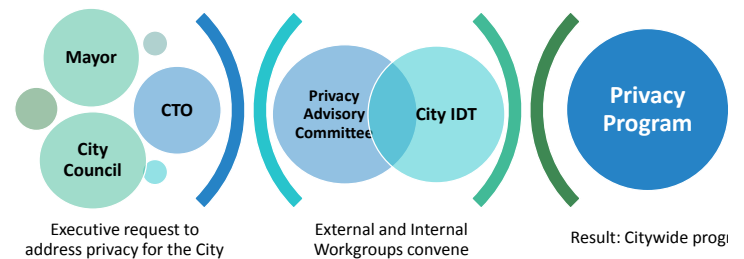
### Community engagement

To advise these efforts, we also convened an external Privacy Advisory Committee. The Committee included recognized thought leaders from academia, companies, law firms, community advocacy groups, and other arenas from the private and public sectors who focus on privacy concerns. Details about membership may be found in Appendix 1. This group's role, meeting three times over the life of the project, was to review the work of the IDT and provide best practice ideas and recommendations for the development of the citywide program.

### Outcome

The outcome of this yearlong effort is the program outlined in this document. The Privacy Program is based on an ethical policy and governance framework for addressing current and future issues as these technologies and capabilities continue to evolve across all lines of the City's business. This includes a broad, consistent set of principles to address the collection and management of personal information throughout its lifecycle to help ensure the public's privacy. It also includes a review process for privacy impacting technologies and programs and a toolkit of resources to provide guidance and direction for City employees to incorporate privacy in to everyday operations.

### *Privacy Initiative Approach*



### III. What is privacy?

Privacy may be defined as “The rights and obligations of individuals and organizations with respect to the collection, use, retention, disclosure and disposal of personal information.”

This is information that is about, or can be related to, an identifiable individual and is sometimes referred to as Personally Identifiable Information, or PII. Most information collected by an organization about an individual is likely to be considered personal information if it can be attributed to an identified individual.

Some personal information requires an extra level of protection and a higher duty of care. For example, some jurisdictions may require explicit consent rather than implicit consent for the collection and use of some types of personal information. Examples of personal information are:

Name	Religious or philosophical beliefs
Home or email address	Trade union membership
Identification number (Social Security #)	Sexual preferences
Physical characteristics	Information related to offenses or criminal convictions
Consumer purchase or billing history	Image, audio or video recording
Household information	Driver’s license information
Information on medical or health conditions	Biometric data
Financial information	Birthdate
Racial or ethnic origin	Location information
Political opinions	GPS

#### The importance of privacy

Gaining and maintaining the public's trust about information management is our responsibility as a local government and critical to our successful operations. While privacy laws protect some personal information, most of what we collect becomes a government record that others can ask to see through public records requests. It is therefore important that we manage this information appropriately and lawfully.

#### Our obligations

The Privacy Program will provide guidance about incorporating the following actions into our operations that involve personal information:

- *Minimizing Data Collection.* Minimizing data by only collecting what is necessary to get done the job at hand.
- *Providing Notice.* Clearly communicate about our data collection and use and provide access to our Privacy Statement.
- *Reviewing Obligations.* Understand and follow legal, contractual, and other obligations.
- *Reviewing Data and Systems Security.* Taking steps to secure adequately stored data.
- *Deleting or De-identifying Data.* Follow City data retentions schedules and dispose of data as required.

## IV. Privacy Principles

The City of Seattle collects personal information from the public so that we can provide many important services including community and critical infrastructure protection, 911 call response, waste management, electricity delivery and other services. We work to find a fair balance between gathering information to provide these needed services and protecting the public's privacy.

While privacy laws protect some personal information, the information we collect becomes a government record that others can ask to see through public records requests. Therefore, it is important for you to know when and how your personal information is collected, how we use it, how we disclose it and how long we keep it.

The following Privacy Principles guide the actions we take when collecting and using your personal information:

### 1. We value your privacy...

Keeping your personal information private is very important. We consider potential risks to the well-being of you and the public before collecting, using and disclosing your personal information.

### 2. We collect and keep only what we need...

We only collect information that we need to deliver City services and keep it as long as we are legally required or there is a valid business purpose. When it is practical, we tell you when we are collecting this information.

### 3. Using your information...

When appropriate, we make available information about the ways we use your personal information at the time we collect it. If possible, we will give you a choice about how we use your information.

### 4. We are accountable...

We manage personal information in a manner that is consistent with our commitments and as required by law. We protect your personal information by restricting improper access and by securing our computing resources from threats.

### 5. Sharing information...

We follow federal and state laws about information disclosure whenever we work with outside governmental agencies to protect our community and in answering Public Disclosure Requests (PDRs). Business partners and contracted vendors who receive or collect personal information from us or for us to deliver City services must agree to our privacy requirements.

### 6. Accuracy is important...

We work to maintain and use accurate personal information for City business. When practical, we will work to correct inaccurate personal information. We also instruct our partners and contracted vendors to follow the same guidelines.

## V. Privacy Review Process

The three-step privacy review process is designed to accommodate a wide-variety of projects and levels of privacy review. It begins with a self-assessment questionnaire that asks a series of questions to determine the level of privacy risk associated with the nature of the information that is collected and how it is used and managed throughout the information lifecycle. The steps outlined below:

### Self-service assessment

The first step in the privacy review process is to complete an assessment questionnaire. If the answers indicate a low privacy risk, project owners will be able to use the Toolkit resources to meet our privacy commitments.

### Privacy threshold analysis

If the project is determined to have a higher privacy risk, project owners will be asked to answer additional questions in a Privacy Threshold Analysis. The departmental Privacy Champion will review the answers to determine if project owners can use the Toolkit resources to mitigate any privacy risks or if a more in depth privacy review is required.

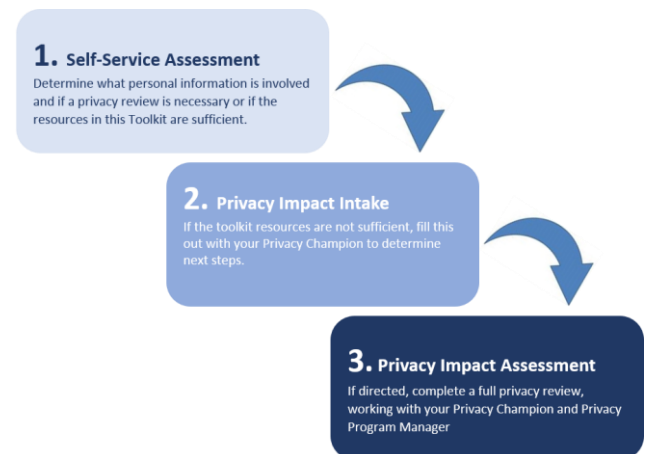
### Privacy Impact Assessment

If a project or program is determined to represent a significant privacy risk, then the owners will be asked to complete a Privacy Impact Assessment (PIA). This document takes a more detailed look at projects or programs to determine all potential privacy impacts and mitigation options.

### Transparency

Privacy review information will be saved to document its completion. Abstracts and findings of some PIAs may be made available on the Privacy website for public review.

### Privacy Review Process





## VI. Roles and Responsibilities

Facilitating decisions and operational practices consistent with the City's Privacy Principles require awareness to be driven across the organization. We will facilitate this through the implementation of a departmental Privacy Champion program, providing a network of departmental focal points to promote the Privacy Program and assist the Privacy Program Manager.

### Privacy Champion

The Privacy Champion will provide department support for incorporating the Privacy Program objectives into business systems and processes. This responsibility is designed to be a part-time supportive function that is in addition to an employee's regular job responsibilities. Privacy Champions will provide support for privacy related issues that may be resolved at the departmental level. This support includes:

- Handling basic inquiries, escalating as needed to Privacy Program Manager
- Conducting and signing off low-risk reviews
- Facilitating effective review of higher risk issues by validating response appropriateness in privacy assessments, participating in the actual review with the Privacy Lead/Manager as needed, and ensuring all remediation items are addressed and approved
- Actively participating in privacy meetings and building awareness about privacy

### Privacy Program Manager

The Privacy Program Manager role is a full-time position in the Department of Information Technology responsible for coordinating the Privacy Champions in a community of practice, completing privacy impact assessments for projects that present higher privacy risk, and helping drive the privacy training and awareness efforts. The Privacy Program Manager's responsibilities includes:

- Conducting Privacy Impact Assessments
- Managing the Privacy Champions, and cultivating a community of practice to share knowledge and best practices
- Working with the DoIT compliance and security teams to develop, implement, and enforce policies
- Helping develop a privacy training and awareness program

### Chief Privacy Officer

Mayor Murray's 2016 budget proposed the creation of a Chief Privacy Officer. This role would provide overall leadership and direction to the Privacy Program, including the creation of annual Privacy Program plans, communicating with City and department leaders about the Program, working with the City Auditor to assess compliance with our Privacy Principles, and developing new strategies for further protecting the public's privacy.

## VII. Resources

The Privacy Program provides policies, expertise, training, review processes, governance structure and direction required for City departments to be aware of and compliant with our privacy commitments. Given the variety of programs and missions throughout the City, these resources are presented in an online and self-guiding manner to enable employees to access and use them as appropriate for both the level of potential privacy impact and departmental resources available.

### Privacy Toolkit

The Privacy Toolkit is an online collection of electronic documents, online forms and links that provide guidance for incorporating our privacy obligations into daily operations. City departments with applications, processes or programs that collect the public's personal information need to be familiar with and use the resources in the Privacy Toolkit.

The toolkit contains the following:

- Privacy Principles and Privacy Statement
- Review forms and process documents
- Training and awareness links
- Standards and policies
- Contract language
- Legal and regulatory information
- Translations of our privacy documents
- Privacy program information including synopses of Privacy Impact Assessments

The screenshot shows the 'Welcome to the Privacy Toolkit' page. At the top, a blue banner reads 'Welcome to the Privacy Toolkit' with the mission: 'Build public trust about the use and management of personal information'. Below this, several sections provide information:

- What is privacy?**: Defines privacy as 'the rights and obligations of individuals and organizations with respect to the collection, use, retention, disclosure and disposal of personal information.' It references the 'Generally Accepted Privacy Principles'.
- Why is it important?**: States that gaining and maintaining public trust is a responsibility of local government and that privacy laws protect personal information.
- How do we meet these obligations?**: Lists actions like 'Minimizing Data Collection, Providing Notice, Reviewing Legal Obligations, Reviewing Data and Systems Security and Deleting or De-identifying Data'.
- Who needs this Toolkit?**: Identifies city departments that collect public personal information.
- How do you use the Toolkit?**: Mentions 'Step 1: Understand our Privacy Policies' and the role of the Privacy Principles, Statement, and Policy.

On the right side, there is a 'Privacy Review Process' section with a 'Self-Service Assessment' button and a 'Toolkit Resources' section with a grid of icons for 'Privacy Policy', 'Privacy Review Process', 'Contract Language', and 'Regulatory and Legal Information'.

## Appendix 1: Privacy Workgroups

The internal and external privacy workgroups convened for the Privacy Initiative were instrumental in drafting the privacy commitment documents, toolkit requirements and deliverables. These groups were comprised of the following individuals:

### PRIVACY INTERDEPARTMENTAL TEAM (IDT)

Department	Representative(s)
Mayor's Office	Ryan Biava
DoIT	Bryant Bradbury
DoIT	Ginger Armbruster
SPD	Capt. Dick Reed, Asst. Chief Washburn
SCL	Hina Arai
SFD	Lenny Roberts, Chief Gregory Dean
Law	Mary Perry
SPL	Andra Addison
SDOT	Angela Steel
Records	Jennifer Winkler
Councilmember O'Brien's Office	Josh Fogt
Councilmember Harrell's Office	Vinh Tang

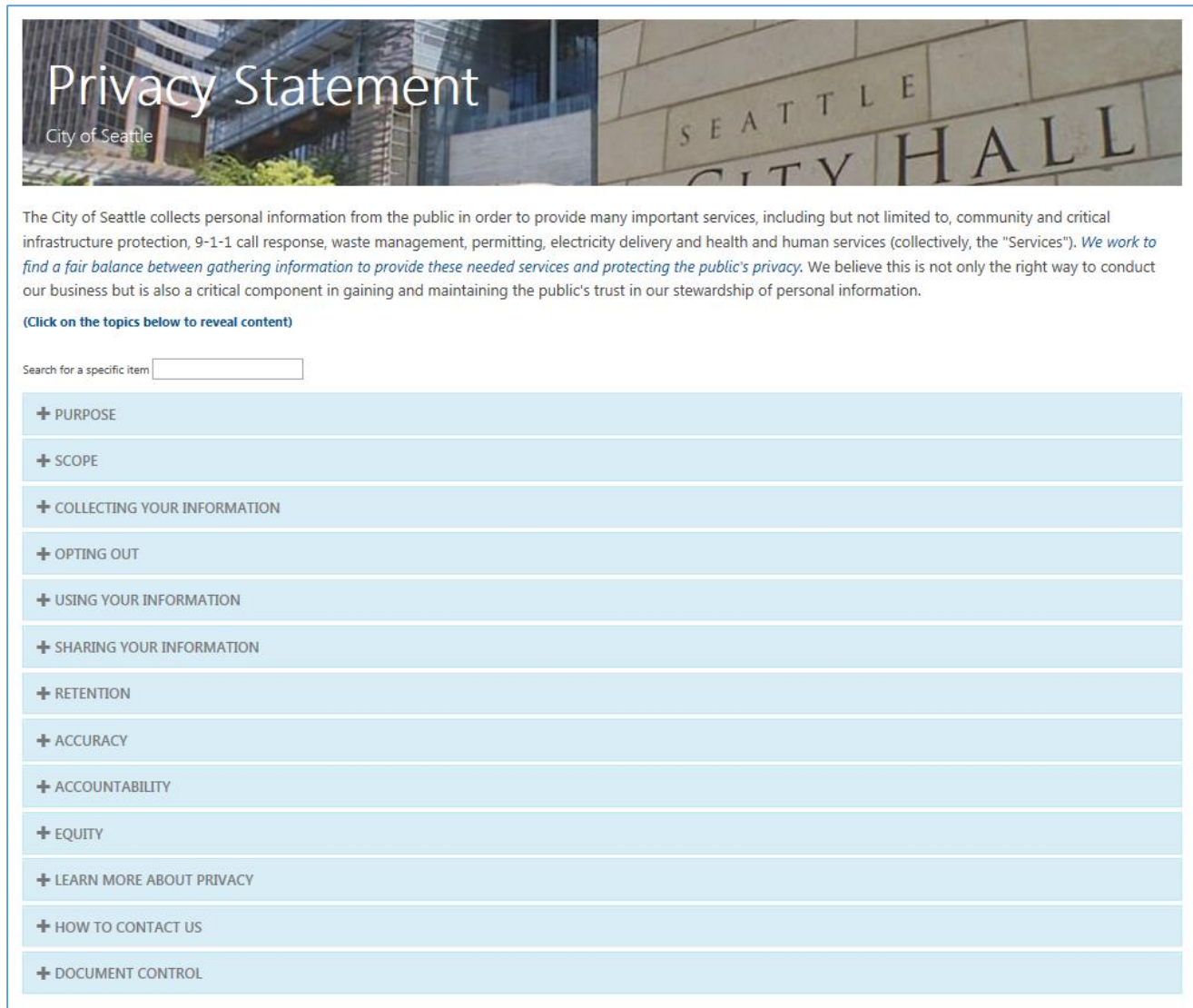
### PRIVACY ADVISORY COMMITTEE

Name	Title	Special Interests
Tracy Ann Kosa	Seattle Privacy Coalition	Privacy; political science, privacy policy efficacy metrics
Ben Krokower	Chair, CTTAB	Government, civil rights
Susan Lyon-Hintze	Partner, Hintze Law	Tech and e-commerce law
Aravind Swaminathan	Partner, Privacy and Security, Orrick	Cybersecurity, data breach management, privacy
Ryan Calo	Assistant Professor of Law, University of Washington	Cyber Law, Privacy, Robotics, Torts
Michael Hamilton	Partner, MKH & Associates	Cyber Security
Jim Neff	Investigative Editor, Seattle Times	Open Data
Jared Friend	Director of Technology, ACLU of Washington	Privacy rights
Aileen Cronin	Associate General Counsel, Alaska Airlines	Privacy policy and practice

# Appendix 2: Summary Privacy Statement

## Summary Version

The Privacy Statement will be presented on the website as shown below. The Statement is organized into sections, allowing users to drill-down into sections of interest. The full statement follows this summarized list.



The screenshot shows the top of the City of Seattle Privacy Statement website. At the top left, there is a header image with the text "Privacy Statement" and "City of Seattle" overlaid. To the right of the image, the words "SEATTLE CITY HALL" are visible on a stone wall. Below the header, there is a paragraph of introductory text explaining the City's commitment to privacy. Underneath the text is a search bar with the placeholder "Search for a specific item". Below the search bar is a vertical list of 13 menu items, each with a plus sign icon and a light blue background:

- + PURPOSE
- + SCOPE
- + COLLECTING YOUR INFORMATION
- + OPTING OUT
- + USING YOUR INFORMATION
- + SHARING YOUR INFORMATION
- + RETENTION
- + ACCURACY
- + ACCOUNTABILITY
- + EQUITY
- + LEARN MORE ABOUT PRIVACY
- + HOW TO CONTACT US
- + DOCUMENT CONTROL

## Appendix 3: Full Privacy Statement

### Introduction

The City of Seattle collects personal information from the public in order to provide many important services, including but not limited to, community and critical infrastructure protection, 9-1-1 call response, waste management, permitting, electricity delivery and health and human services (collectively, the “Services”). *We work to find a fair balance between gathering information to provide these needed services and protecting the public’s privacy.* We believe this is not only the right way to conduct our business but is also a critical component in gaining and maintaining the public’s trust in our stewardship of personal information.

### Purpose

We understand the value of personal information and work to protect the personal information we collect from the public. We are committed to providing greater transparency into our data privacy practices. As part of our deeper commitment to good data practices and data stewardship, the City has created the City of Seattle Privacy Principles to serve as a guide for all City departments that collect and use personal information. Please note that the City will be updating and improving our privacy and security posture over the next several months and that it will take time to implement certain changes throughout the City system. We appreciate your patience while we enhance and unify our privacy practices. Please contact us at [Privacy@seattle.gov](mailto:Privacy@seattle.gov) if you have any questions, or if you believe you see or experience policies or practices that are not yet in line with the principles set forth in this document.

*More information about the Privacy Principles and our Privacy Initiative may be found [here](#).*

### Scope

This Privacy Statement applies to the collection, use, disclosure, sharing and retention of personal information we obtain from individuals interacting with City departments, whether in person, on a website (<http://www.seattle.gov/>), or by mail in the course of providing City services. Each City department will strive to abide by and use this Privacy Statement to direct the handling of personal information, though from time to time it may be necessary for a City department to develop a practice that differs from this Privacy Statement. When that happens, we will do our best to provide you with notice of the practice and to let you know about your choices.

### City of Seattle Employees

This Statement does not apply to personal information we obtain in our capacity as an employer. Employment information is covered under separate policies which may be found on our Human Resources website, [here](#).

### Collecting your information

The City collects different kinds of information from the public in order to conduct City operations and provide the public with important services. Some of this information you provide directly to us. Some of it we collect in the course of your interactions with various City departments. To learn more about what we collect and how it is collected, click on the links below:

## What information we collect

We collect information necessary for City departments to provide services to the public, protect the public's health and safety, and to improve the efficiency and effectiveness of our operations. Our goal is to collect only enough information as is reasonable to perform our Services and to let you know when providing personal information is optional. We also seek to aggregate or otherwise de-identify personal data, when possible, whenever it is not necessary to store or share personally identifiable data elements. The table below provides some examples of the information we collect:

DESCRIPTION	EXAMPLES
PERSONALLY IDENTIFIABLE INFORMATION	Name, address, age, birthdate, social security number, driver's license number
WEBSITE INFORMATION	Information passively gathered from visitors on our website and from mobile devices
FINANCIAL INFORMATION AND PAYMENT CARD INFORMATION	Bank account number, credit or debit card numbers, or other billing information, such as when you pay your utilities, pay taxes, or sign up program membership or classes
HEALTH RECORDS	Medical information collected during emergency response, vaccination records, health program participation
DIGITAL IMAGES	Facility security cameras, City sponsored event photos, traffic camera video
UTILITY USE	Consumption data about electricity, water and waste management services
PERMITTING INFORMATION	New construction, reconstruction and remodeling, land use, events, utilities
PUBLIC SAFETY	Violations, court records, emergency calls
TRAFFIC MOVEMENT	Traffic flows, event monitoring
DEMOGRAPHIC INFORMATION	Income bracket, gender, race or ethnicity, vocation

## How we collect information through our website

Click on the links below for details about information we collect when you use our websites.

### *[Providing personal information on our website.](#)*

You may choose whether to provide personal information online. "Personal information" is information about a natural person that is readily identifiable to that specific individual. Personal information includes such things as an individual's name, address, and phone number.

We collect no personal information about you unless you voluntarily provide it to us by sending us e-mail, participating in a survey, completing an online form, or engaging in an online transaction. You may choose not to contact us by e-mail, participate in a survey, provide personal information using an online form, or engage in an electronic transaction. However, you may not be able to access certain user-specific features of the web site without providing personal information.

### *Information collected from visitors to our website.*

If you do nothing during your visit to our web site but browse, read pages, or download information, we will automatically gather and store certain information about your visit through the use of cookies and other similar tracking technologies. This information does not identify you personally. The information we collect through these technologies can include:

- The Internet Protocol Address and domain name used to access our web site. The Internet Protocol address is a numerical identifier assigned either to your Internet service provider or directly to your computer. We use the Internet Protocol Address to direct Internet traffic to you. This address can be translated to determine the domain name of your service provider (e.g. xcompany.com or yourschool.edu). Generally, the City only determines visitor domain names if a security issue is suspected;
- The type of browser and operating system you used;
- The date and time you visited this site;
- The web pages or services you accessed at this site; and
- The web site you visited prior to coming to this web site.

We may use this data automatically collected through cookies and other technologies to: (a) remember information so that you will not have to re-enter it during your visit or the next time you visit the site; (b) provide custom, personalized content; (c) provide and monitor the effectiveness of our website; (d) monitor aggregate metrics such as total number of visitors, traffic, usage, and demographic patterns on our website and our Service; (e) diagnose or fix technology problems; (f) enhance network security; and (g) otherwise to plan for and enhance our Service or website. For example, the City's web site uses software programs to create summary statistics, which are used for such purposes as assessing what information is of most and least interest, determining technical design specifications, and identifying system performance or problem areas.

We may also use analytic and security tools hosted by third parties or managed within the City as part of maintaining our web presence. These tools help us measure traffic and usage trends for our web site and help ensure that this service remains available to all users. These tools can also be used to monitor network traffic to identify unauthorized attempts to upload or change information, or otherwise cause damage. Except for authorized law enforcement investigations and the security purposes mentioned elsewhere in this notice, no other attempts are made to identify individual users or their usage habits. Raw data logs are used for no other purposes and are scheduled for regular destruction in accordance with public records retention schedules.

The City does not generally use cookies or other tracking technology to track its users across websites or over time, nor does it currently permit third party ad networks or other companies to track users on our web site. Because we do not track users over time and across websites, your use of the Do Not Track feature on your browser will have no effect on this web site.

### *Information collected from website visitors who chose to provide personal information online.*

If during your visit to our web site you participate in a survey, send an e-mail, participate in a City hosted mailing list or web-based discussion, register an account, participate in online commerce, or perform some other transaction online, we may collect personal information from you, including:

- The e-mail address, and contents of the e-mail, for those who communicate with us via e-mail or who participate in a City hosted mailing list or web-based discussion.

- Information volunteered in response to a survey.
- Information provided through an online form for any other purpose.
- Information submitted when participating in an online transaction with the City.
- Information provided when you register an account.

The information collected is not limited to text characters and may include audio, video, and graphic information formats you send us.

We use your e-mail address to respond to you. We do not send you unsolicited e-mail unless you specifically elect to receive it or unless it is part of a transactional communication that is part of receiving a City service. Online discussion lists or "threads" are maintained and controlled in accordance with the [City's Electronic Conferencing and List Services Policy](#). Survey information is used for the purpose identified by the survey. Information from other online forms is used only for conducting City business related to the online form.

#### *Information collected from your mobile device*

If you access our website and online services or use an application on a mobile device, we may collect certain information about that device. Messages sent from certain mobile devices contain unique identifiers about the physical location of such devices. Mobile devices also typically transmit caller ID data when used to transmit a telephone call or text message. Depending on the device and its settings, this information includes but is not limited to geolocation data, unique device identifiers and other information about your type of device, wireless provider, date and time of transaction, browser type, browser language and other transactional information.

We may use this information to contact you and to respond to requests. We will not to use your phone number to initiate a call or SMS text message to you without your express prior consent. Your wireless carrier and other service providers also collect data about your SMS Service usage, and their practices are governed by their own privacy policies.

*Additional Resources:* To find out more about the information that your mobile device collects and transmits, and the options available to you to change factory defaults that may affect those transmissions, please consult with your wireless or mobile device provider. For general information about wireless industry laws and regulations, please go to the Cellular Telecommunications and Internet Association website at [http://ctia.org/consumer\\_info/service/](http://ctia.org/consumer_info/service/).

#### *Avoiding Internet Fraud*

Fraudulent scams called "phishing" have been increasing in frequency. "Phishing" involves a victim receiving an e-mail appearing to be from a legitimate business. The "from" line is often forged and the e-mail usually contains authentic looking graphics making it appear to be legitimate. The e-mail may also contain what appears to be a legitimate link to that organization, e.g., <http://www.seattle.gov/>. When the victim clicks on this link, they are then taken to what appears to be a legitimate looking website. Criminals can even make your browser's address bar contain the address of the legitimate organization despite the fact that the website is a forgery. Victims are then encouraged to enter personal information including credit card numbers and expiration dates.

We will not request confidential personal or financial information from our customers via an unsolicited e-mail. The City will also never send you an unsolicited e-mail containing a link to a City website where confidential personal or financial information is requested. If you receive such an e-mail, purportedly from the City, you are encouraged to immediately contact the City's Citizen Service Bureau at: (206) 684-CITY.



For more general information about "phishing" [visit the Federal Trade Commission web site](#). For specific information about a suspected phishing attempt, you may have received contact the organization represented in the suspect e-mail.

## How we collect information through other means

Click on the links below for details about others ways we collect personal information.

### *Paper forms*

City departments may collect information on paper forms as part of providing a government service or community engagement. These forms may request personal information, such as name, birthdate, address, telephone number, and email address. Forms may also request additional information necessary to determine eligibility for a service, such as income. When possible, forms will note what information is required to obtain a government service or participate in a government function and what information is optional. In addition, the form will note if there are any options for "opting out" of certain data uses, such as follow-up communications not directly related to the service being requested. Please note that we will be updating our forms over time to contain these disclosures.

### *Telephone calls*

Individuals may contact the City via phone such as when calling our Customer Service Bureau (CSB), Seattle City Light/Seattle Public Utilities Call Center, or when calling a City department or staff member directly. Our phone system automatically logs the phone number and other characteristics of calls to and from City numbers, such as call duration and the extension in the City that received or made a call. It is not possible to opt-out of this collection. During the course of your call to a call center, we may ask for additional information. This information will be used to help provide the requested service. The call taker will inform you about what information may be optionally provided. We will also provide notice if and when a call center records calls for training purposes or to improve the services.

We may also collect personal information when we call you or notify you of an event via phone or text message, including by creating a record of when a call was made and whether it was received by a live person.

### *Email communication*

When sending an email to a City email address, such as [user@seattle.gov](#), or [user@startupseattle.com](#), we collect personal information that may be contained in the email message and automatically log certain information about message, including the sender information, the IP address, routing information, and email address. It is not possible to opt-out of this collection.

In some cases, when the City sends an email to a user, it may contain beacons, which help the City track which emails have been opened and which links are clicked by our recipients.

### *Video cameras*

Some City-owned facilities use video cameras to monitor activity and protect those working in or visiting the facility, or to protect the public. These include the following:

### *Image recording*

Some City facilities use video cameras to monitor activity in common areas to protect the health and safety of those working in or visiting the facility. Notices will be posted in the area where these video cameras are in use. Depending on public policy, the needs of the facility, and applicable laws and regulations, these recordings may record video, audio, or both.

### Traffic cameras

Main arterials and other roads, sidewalks and waterways have cameras posted to monitor traffic flow and major traffic events. The City also deploys red light cameras at some intersections to enforce the traffic laws.

### Public Safety

There are a variety of video and audio capture technologies used for public safety purposes. For example, please see the following for more details governing some image recording technologies:

TECHNOLOGY	GOVERNANCE
IN CAR VIDEO SYSTEM	Seattle Police Department (SPD) Manual Chapter 16.090
BODY-WORN VIDEO PILOT PROGRAM	SPD Manual Chapter 16.091
AUTOMATIC LICENSE PLATE READERS	SPD Manual Chapter 16.170
COLLECTION OF INFORMATION FOR LAW ENFORCEMENT PURPOSES	Seattle Municipal Code (SMC) Chapter 14.12
HOLDING CELL CAMERA SYSTEM	SPD Manual Chapter 10.060
ACQUISITION AND USE OF SURVEILLANCE EQUIPMENT	SMC Chapter 14.18
AUTOMATED TRAFFIC SAFETY CAMERAS	SMC 11.50.570

### Emergency response

In certain public safety and emergency response situations, we collect biometric data, including fingerprints and health related measurements such as heart rate or blood pressure. In some cases, we also employ facial recognition technology to assist in public safety response. Due to the individualized and serious nature of emergency response efforts, a variety of personal 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 Statement. Emergency call centers may also follow different protocols in the course of responding to emergency calls. Whenever possible, our emergency responders will attempt to honor the Privacy Principles and this Privacy Statement when collecting, using, storing or sharing personal information.

### Opting out

While it may limit the services we are able provide, where it is possible we will present information about what we are collecting and provide an opportunity to accept or decline to provide it to us, such as follow-up communications not directly related to the service being requested. Please understand that in some circumstances, we may not be able to provide the desired services if you decline to provide necessary information.

### Using your information

We recognize that the public expects government both to protect individual privacy and to operate effectively. Toward that end, the City of Seattle uses personal information in the course of providing services, protecting the public's safety, meeting our mission obligations, and determining the best use of our resources. We endeavor to collect only as much information as is necessary to perform these functions and to limit information use to the purpose stated at the time of collection and to protect and improve our services. To learn more about how we use information to improve services, click on the links below:

## Research and Audit

We may use information we collect to help the City better understand community needs and improve the efficiency, effectiveness, and equity of our service delivery. When performing research, attempts will be made to de-identify data, either performing analysis at an aggregate level or removing data elements containing personal information that are not necessary for analysis.

## Systems Security

We may collect or use collected information for systems security purposes, and to ensure that our online website services remain available to all users. The City's online services may use software or services to detect fraudulent transactions, identify unauthorized attempts to upload or change information, or otherwise interference with service delivery.

## Sharing your information

We share information to coordinate delivery of services to the public, improve customer service, maintain data consistency, assess program performance, identify opportunities to improve our operations and because we are required to by law. We may also share information that has been aggregated or de-identified. To learn about how we share personally identifiable information, please click on the links below:

## Third-parties

We also share information with third parties who provide services on behalf of the City. For example, the City contracts with third parties to process financial transactions, technology companies that provide cloud and managed services, and analytics companies that measure traffic visiting the City's websites. In doing so we comply with state and federal laws and follow information security practices to protect both physically and electronically stored and transmitted data. We do not sell personal information to third parties for marketing purposes or for their own commercial use.

## Government Agencies

We may share information with other government agencies, external service providers, researchers, contracted vendors, and others to perform city functions and comply with applicable laws. We ask third parties to abide by our privacy principles when handling data provided by the City. In many cases, we require compliance through contractual obligations that include:

- Providing notice when information is collected and used on our behalf by contracted third parties.
- Directing that contracted third parties agree to and follow our contractual privacy requirements.

## Public Records Act

In the State Of Washington, Public Disclosure laws exist to ensure that government is open and that the public has a right to access records and information possessed by City government, as appropriate (The Public Records Act or "PRA" [RCW 42.56](#)).

The PRA requires the disclosure of public records unless a particular record (or particular information contained in a record) is specifically exempt from public access under the PRA or other applicable law. For example, there is no categorical exemption for residential telephone numbers, residential addresses, or personal e-mail addresses and therefore these data elements may be made public under the PRA. However, the PRA does not require the disclosure of "credit card numbers, debit card numbers, electronic check numbers, card expiration dates, or bank or other financial account numbers supplied to [the City] for the purpose of electronic transfer of funds, except when disclosure is expressly required by law."

In the event of a conflict between this Privacy Statement and the Public Records Act or other law governing the disclosure of records, the Public Records Act or other applicable law will determine our obligation. This means the City may be required to disclose your information in the event of a Public Disclosure Request; however, we will consider what information may be exempted before responding to a request.

## Open Data Program

For the purpose of government transparency, and consistent with the intent of the Public Records Act, the City posts some data sets to our Open Data portal, [data.seattle.gov](http://data.seattle.gov). This allows the public to view, access and use information gathered by the City for a variety of purposes, from research to technology innovation.

## Links to Third Party Websites

The City's web site has many links to other websites. These include links to web sites operated by other government agencies, nonprofit organizations and private businesses. When you link to another site, you are no longer on the City's website and this Privacy Statement will not apply. When you link to another website, you are subject to the privacy policy of that new site. Visitors linking to another site are encouraged to examine the privacy policy of that site.

Neither the City, or any department, officer, or employee of the City warrants the accuracy, reliability or timeliness of any information published by this system, nor endorses any content, viewpoints, products, or services linked from this system, and shall not be held liable for any losses caused by reliance on the accuracy, reliability or timeliness of such information. Portions of such information may be incorrect or not current. Any person or entity that relies on any information obtained from this system does so at his or her own risk.

## Retention

Public records created or received by the City must be retained for legal or operational purposes according to applicable laws. As a government entity, much of the information that the City collects is considered a public record regardless of format or where it is stored. More information about the Preservation and Destruction of Public Records may be found [here](#). When possible, the City may provide the right for an individual to request that information collected from the individual be deleted, unless the City is required to retain such information.

## Accuracy

We take reasonable steps to ensure that personal information we have is up-to-date. Where possible, we implement processes for updating inaccurate information that is used in the course of doing business. If you believe that your personal information needs to be updated, please complete the "[Request a City Service](#)" form and select the service type "Personal Information Change". We will take reasonable steps to verify your identity before granting access or making corrections.

## Accountability

We comply with laws, statutes and regulations that govern the information we collect. We also follow best practices and internal policies to reduce or eliminate the potential impact of new technologies and practices on the public's privacy. Should we become aware of programs or applications that are contrary to this privacy statement we will take steps to educate staff and remediate the issue. To learn more, click on the links below:

## Privacy Tools

To meet our departmental mission objectives and uphold our commitments to privacy, the City is implementing several new tools to help evaluate the effectiveness of our privacy protections. For example, the City is in the process of

developing a Privacy Toolkit to assist City employees evaluate a new program or initiative, or when planning to purchase or develop a new technology. Staff consider the privacy implications of the new service or technology by applying our “Privacy Principles.” The City is also creating procedures to require employees to conduct a Privacy Impact Assessment (PIA) before new technologies are employed to identify privacy risk and implement appropriate measures to reduce the risk of violating personal privacy. The PIA process is overseen by the City’s Privacy Program Manager. For information about that process, please see the Privacy Program webpage, [here](#). We will update this section as these tools are put in place across the City organization.

## Security

The City has taken steps to safeguard the integrity of its data and to prevent unauthorized access to information it maintains. Depending on the type of information, we may use physical, administrative and technological techniques to protect data including but not limited to access control, monitoring, auditing, and encryption to secure data. Security measures have been integrated into the design, implementation and day-to-day practices of the entire operating environment as part of the City’s continuing commitment to protecting our environment.

This information should not be construed in any way as giving business, legal, or other advice, or warranting as fail proof, the security of information provided via the City's web site. Please remember that no security system is impenetrable and we cannot guarantee the security of our systems 100%. In the event that any information under our control is compromised as a result of a breach of security, the City will take reasonable steps to investigate the situation and where appropriate, notify those individuals whose information may have been compromised and take other steps, in accordance with any applicable laws and regulations.

## Equity

We are mindful of the populations we serve and how data about members of the public, including vulnerable populations, can and should be used. Our Privacy Principles are consistent with our Race and Social Justice Initiative. Details about RSJI may be found, [here](#).

## Learn more about Privacy

- [Washington State Public Records Act](#)

City of Seattle Resources:

- [Privacy Program](#)
- [Privacy Principles](#)
- [Public Records Request](#)
- [Surveillance Ordinance](#)
- [Declaration of Privacy as Human Right](#)

## How to Contact Us

If you have a general privacy question please contact our Privacy Program Manager:

- By email at [privacy@seattle.gov](mailto:privacy@seattle.gov).
- By Phone: 206-684-2489 (CITY)

## Document Control

This document will be reviewed annually and updated as necessary by the Privacy Program Manager, and reviewed and approved by the City's Chief Technology Officer.

Version	Changes	Approval	Date
1.0 Original	N/A	Michael Mattmiller	9/30/2015

# Appendix 4: Privacy Intake and Review form

## City of Seattle Privacy Review Process

### Part 1: Self-Assessment

#### Purpose

The purpose of this form is to determine:

1. Whether a proposed program or program update affects public privacy.
2. The extent of privacy impact in order to consider possible ways to limit or remediate issues.
3. If the program should undergo a more comprehensive Privacy Impact Assessment.

#### Instructions

1. Please fill out this form completely.
2. If a more in-depth review is required, your Privacy Champion or the Privacy Program Manager will review the information contained in this form to determine your next steps.

#### Summary Information

1. **DATE submitted for review:** Click here to enter a date.
2. **NAME of Program:** Click here to enter text.
3. **Name of Program Manager:** Click here to enter text.

### Are you collecting Personal Information?

Please see our [Personal Information Definition](#) to determine if your project or program involves personal information:

- Yes  
 No

**NO?** If you answered NO, your project will not require a Privacy Review. If your project's data collection requirements change, please submit a revised Privacy analysis form.  
Thank you!

**YES?** If you answered YES, please continue to the next set of questions:

**What are you collecting?**  
Some technologies will require a more in-depth privacy review

Is the Information being collected under regulatory control?

- Yes
- No

**Does the technology involve surveillance cameras or unmanned aircraft technologies?**

- Yes.
- No.

Please describe the nature of the information captured by camera:

[Click here to enter text.](#)

**Could the data collection practice be perceived as controversial or is a negative public perception possible?**

- Yes
- No

**YES?**

If you answered YES to one or more of the questions above, you project will need to undergo a Privacy Impact Assessment (PIA). Please click here to access the PIA form.

**NO?**

If you answered NO to ALL of the questions above, please continue to the next set of questions:

**What personal information about individuals could be collected, generated or retained?**

<input type="checkbox"/> Social Security Numbers (SSNs)? (This includes truncated SSNs)	<input type="checkbox"/> Sex and/or Gender
<input type="checkbox"/> Names	<input type="checkbox"/> Race
<input type="checkbox"/> Addresses	<input type="checkbox"/> Household information
<input type="checkbox"/> Driver's license number	<input type="checkbox"/> Credit card info
<input type="checkbox"/> Birthdate	<input type="checkbox"/> Financial info
<input type="checkbox"/> Audio recording	<input type="checkbox"/> Health info
<input type="checkbox"/> Email or electronic communications	<input type="checkbox"/> Emails
<input type="checkbox"/> Biometric data	<input type="checkbox"/> Location

Other? Please describe the information that is collected:



Click here to enter text.

**Are you minimizing data collection?**

- Are you collecting only information that is necessary to meet a specific need?
- Will it be effective in meeting the need?
- Are you choosing the least privacy intrusive way of achieving the same goal?
- Is the benefit of using the information worth the privacy impact?
- Are you providing clear notice of collection and uses of information?
- If you are engaging a third party, have you included privacy language in your vendor contract?
- Have you reviewed data security requirements with CISO or other security professionals?
- Have you reviewed data retention schedule and planned for data disposal?

**YES?**

If you answered YES to ALL of the questions above, your project will not need further review. Please disregard the rest of the questions in this form and save this with your project documentation.

**NO?**

If you answered NO to ANY of the questions above, you will need to continue to the next set of questions in the Privacy Threshold Analysis, below.

**Part 2: Privacy Threshold Analysis**

**Program Description and Details**

**Describe the program and its purpose and the purpose of the information captured or collected. Please provide a general description of the program and its purpose in a way a non-technical person could understand.**

Click here to enter text.

**Status of Program**

Click on the appropriate box below:

- This is a new development effort.
- This an existing program.
  - **Date first developed:** Click here to enter a date.

- Date last updated: [Click here to enter a date.](#)
- Provide a general description of the update: [Click here to enter text.](#)

- 1. What is the hardware and software used for this program?**  
(Please provide product and company name(s) for software and/or hardware platforms.)  
[Click here to enter text.](#)
- 2. Was this program developed with or by an external third party?**  
 No, it was developed in-house. [Please continue to the next question.](#)  
 Yes. [If yes, please provide third-party company information](#)  
[Click here to enter text.](#)
- 3. What portion or the information captured will be made publicly available?**  
[Please describe the plans for making the information publicly available:](#)  
[Click here to enter text.](#)

### Privacy Policy Commitments

**4. How does the program adhere to our privacy policies? Please check the box if the statement is true for this program:**

- |                           |   |
|---------------------------|---|
| <b>Notification</b>       | <input type="checkbox"/> The program uses City of Seattle privacy notice and statement to inform users about the collection and use of the information that is collected.<br><input type="checkbox"/> There is an opt-out/in for providing the information or participating in the program.   |
| <b>Collection and Use</b> | <input type="checkbox"/> A third party is involved in collecting the information used in the program.<br><input type="checkbox"/> There is another use planned for the information collected, in addition to the primary purpose for which it was gathered.<br><input type="checkbox"/> The personal information is used to make an analysis or decision affecting the individual involved.   |
| <b>Sharing</b>            | <input type="checkbox"/> The collected information is shared inside the City.<br><input type="checkbox"/> The collected information is shared outside the City.   |
| <b>Accountability</b>     | <input type="checkbox"/> The program is in compliance with appropriate laws and regulations.<br><input type="checkbox"/> The program has been reviewed and approved for appropriate information security practices.<br><input type="checkbox"/> There is an audit process in place to ensure that data is used according to the plan and mission of the department and managed appropriately.<br><input type="checkbox"/> Members of the program team have gone through privacy training. |
| <b>Accuracy</b>           | <input type="checkbox"/> Individuals can both access and correct the information collected about them.  |
| <b>Retention</b>          | <input type="checkbox"/> The program follows the City retention schedule for the information that is gathered.<br>For details, go <a href="#">here</a> .  |

5. **Is there any aspect of this program that might cause public concern by giving the appearance of a privacy intrusion or misuse of personal information?** *An example might include an unexpected push of information out to individuals using email or mobile phones information that was collected for another purpose.*

Please describe any possible appearance of intrusion of privacy:

Click here to enter text.

Thank you for completing this questionnaire. Please save and send to the Privacy Program Manager for review at [privacy@seattle.gov](mailto:privacy@seattle.gov)

### Review Determination

To be completed by the City of Seattle Privacy Champion and Privacy Program Manager

**Review date:** Click here to enter a date.

**Determination:** Click here to enter text.

Privacy Threshold Analysis is sufficient at this time

Full PIA is required

**Privacy Program Manager Comments:**

Click here to enter text.

## Appendix 5: Privacy Impact Assessment



### City of Seattle Privacy Impact Assessment

#### Purpose of a PIA

A Privacy Impact Assessment is designed to outline the anticipated privacy impacts from a City project/program or project/program update that collects, manages, retains or shares personal information from the public. The PIA will provide project/program details that will be used to determine how privacy impacts may be mitigated or reduced in accordance with the City of Seattle Privacy Principles and Privacy Statement.

#### Abstract

**Please provide a brief abstract.** The abstract is the single paragraph that will be used to describe the project and **will be published on the Privacy Program website**. It should be a minimum of three sentences and a maximum of four, and use the following format:

- The first sentence should include the name of the project, technology, pilot, or project/program (hereinafter referred to as "project/program").
- The second sentence should be a brief description of the project/program and its function.
- The third sentence should explain the reason the project/program is being created or updated and why the PIA is required. This sentence should include the reasons that caused the project/program to be identified as a "privacy sensitive system" in the Privacy Intake Form, such as the project/program requiring personal information or the technology being considered privacy sensitive.

[<< Add Abstract Here >>](#)

#### Project/program Overview

**Please provide an overview of the project/program.** The overview provides the context and background necessary to understand the project/program's purpose and mission and the justification for operating a privacy sensitive project/program. Include the following:

- Describe the purpose of the system, technology, pilot or project/program; the name of the department that owns or is funding the project/program and how it the project/program relates to the department's mission;
- Describe how the project/program collects and uses personal information, including a typical transaction that details the life cycle from collection to disposal of the information;
- Describe any routine information sharing conducted by the project/program both within City of Seattle departments and with external partners. Describe how such external sharing is designed with the original collection of the information.
- Identify any major potential privacy risks identified and briefly discuss overall privacy impact of the project/program on individuals
- Identify the technology used and provide a brief description of how it collects information for the project/program.

<< Add Project/program Overview here >>

#### Notification

1. **How does the project/program provide notice about the information that is being collected?** Our Privacy Principles and Statement require that we provide notice to the public when we collect personal information, whenever possible.
  - Describe how notice will be provided to the individuals whose information is collected by this project/program and how it is adequate.
  - If notice is not provided, explain why not. (For certain law enforcement or other project/programs, notice may not be appropriate.)
  - Discuss how the notice provided corresponds to the purpose of the project/program and the stated uses of the information collected.

<<Add answer here>>

2. **What opportunities are available for individuals to consent to the use of their information, decline to provide information, or opt out of the project/program?** Describe how an individual may provide consent for specific uses or whether consent is given to cover all uses (current or potential) of his/her information. If specific consent is permitted or required, how does the individual consent to each use? If notice is provided explain how an individual may exercise the right to consent to particular uses or decline to provide information describe the process. If this is not an option, explain why not. *Note: An example of a reason to not provide an opt-out would be that the data is encrypted and therefore unlikely available to identify an individual in the event of a data breach.*

<< ADD Answer Here >>

#### Collection

3. **Identify the information, including personal information, that the project/program collects, uses, disseminates, or maintains.** Explain how the data collection ties with the purpose of the underlying mission of the department.

<< ADD Answer Here >>

4. **Is information being collected from sources other than an individual, including other IT systems, systems of records, commercial data aggregators, publicly available data and/or other departments?** State the source(s) and explain why information from sources other than the individual is required.

<< ADD Answer Here >>

#### Use

5. **Describe how and why the project/program uses the information that is collected.** List each use (internal and external to the department) of the information collected or maintained. Provide a detailed response that states how and why the different data elements will be used.

<< ADD Answer Here >>

6. Does the project/program use technology to:
- Conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly *or*
  - Create new information such as a score, analysis, or report?

If so, state how the City of Seattle plans to use such results. Some project/programs perform complex analytical tasks resulting in other types of data, matching, relational analysis, scoring, reporting, or pattern analysis. Explain what will be done with the newly derived information. Will the results be placed in the individual's existing record? Will a new record be created? Will any action be taken against or for the individual identified because of the newly derived data?

<< ADD Answer Here >>

7. How does the project/program ensure appropriate use of the information that is collected? Describe any types of controls that may be in place to ensure that information is handled in accordance with the uses described above.

<< ADD Answer Here >>

#### Retention

8. Does the project/program follow the City records retention standard for the information it collects? Departments are responsible for ensuring information collected is only retained for the period required by law. City departments are further responsible for reviewing and auditing their compliance with this process. For more information, please see the internal retention schedule, [here](#), and records retention ordinance, [here](#).

In addition, please provide answers to the following questions:

- How does it dispose of the information stored at the appropriate interval?
- What is your audit process for ensuring the timely and appropriate disposal of information?

<< ADD Answer Here >>

#### Sharing

9. Are there other departments or agencies with assigned roles and responsibilities regarding the information that is collected? Identify and list the name(s) of any departments or agencies with which the information is shared and how ownership and management of the data will be handled.

<< ADD Answer Here >>

10. Does the project/program place limitations on data sharing? Describe any limitations that may be placed on external agencies further sharing the information provided by the City of Seattle. In some instances, the external agency may have a duty to share the information, for example through the information sharing environment.

<< ADD Answer Here >>

- 11. What procedures are in place to determine which users may access the information and how does the project/program determine who has access?** Describe the process and authorization by which an individual receives access to the information held by the project/program, both electronic and paper based records. Identify users from other departments who may have access to the project/program information and under what roles these individuals have such access. Describe the different roles in general terms that have been created that permit access to such project/program information. Specifically, if remote access to the system is allowed or external storage or communication devices interact with the system, describe any measures in place to secure the transmission and storage of data (e.g., encryption and/or two-factor authentication).

<<ADD Answer Here >>

- 12. How does the project/program review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within City of Seattle and outside agencies?** Please describe the process for reviewing and updating data sharing agreements.

<<ADD Answer Here >>

#### Legal Obligations and Compliance

- 13. Are there any specific legal authorities and/or agreements that permit and define the collection of information by the project/program in question?**

- List all statutory and regulatory authority that pertains to or governs the information collected by the project/program, including the authority to collect the information listed in question.
- If you are relying on another department and/or agency to manage the legal or compliance authority of the information that is collected, please list those departments and authorities.

<<ADD Answer Here >>

- 14. How is data accuracy ensured?** Explain how the project/program checks the accuracy of the information. If a commercial data aggregator is involved describe the levels of accuracy required by the contract. If the project/program does not check for accuracy, please explain why. Describe any technical solutions, policies, or procedures focused on improving data accuracy and integrity of the project/program.

<<ADD Answer Here>>

- 15. What are the procedures that allow individuals to access their information?**

Describe any procedures or regulations the department has in place that allow access to information collected by the system or project/program and/or to an accounting of disclosures of that information.

<<ADD Answer Here >>

- 16. What procedures, if any, are in place to allow an individual to correct inaccurate or erroneous information?** Discuss the procedures for individuals to address possibly inaccurate or erroneous information. If none exist, please state why.

<<ADD Answer Here >>

- 17. Is the system compliant with all appropriate City of Seattle and other appropriate regulations and requirements?** Please provide details about reviews and other means of ensuring systems and project/program compliance.

<<ADD Answer Here>>

- 18. Has a system security plan been completed for the information system(s) supporting the project/program?** Please provide details about how the information and system are secured against unauthorized access.

<< ADD Answer Here >>

- 19. How is the project/program mitigating privacy risk?** Given the specific data elements collected, discuss the privacy risks identified and for each risk explain how it was mitigated. Specific risks may be inherent in the sources or methods of collection, or the quality or quantity of information included.

<< ADD Answer Here >>

#### Monitoring and Enforcement

- 20. Describe how the project/program maintains a record of any disclosures outside of the department.** A project/program may keep a paper or electronic record of the date, nature, and purpose of each disclosure, and name and address of the individual or agency to whom the disclosure is made. If the project/program keeps a record, list what information is retained as part of the accounting requirement. A separate system does not need to be created to meet the accounting requirement, but the project/program must be able to recreate the information noted above to demonstrate compliance. If the project/program does not, explain why not.

<<ADD Answer Here >>

- 21. Have access controls been implemented and are audit logs are regularly reviewed to ensure appropriate sharing outside of the department?** Is there a Memorandum of Understanding (MOU), contract, or agreement in place with outside agencies? Discuss how the sharing of information outside of the Department is compatible with the stated purpose and use of the original collection.

<<ADD Answer Here >>



**22. How does the project/program ensure that the information is used in accordance with stated practices of the project/program?** What auditing measures are in place to safeguard the information and policies that pertain to them? Explain whether the project/program conducts self-audits, third party audits or reviews.?

<<ADD Answer Here >>

**23. Describe what privacy training is provided to users either generally or specifically relevant to the project/program.** City of Seattle offers privacy and security training. Each project/program may offer training specific to the project/program, which touches on information handling procedures and sensitivity of information. Discuss how individuals who have access to personal information are trained to handle it appropriately. Explain what controls are in place to ensure that users of the system have completed training relevant to the project/program.

<<ADD Answer Here >>

**24. Is there any aspect of the project/program that might cause concern by giving the appearance to the public of privacy intrusion or misuse of personal information?** Examples might include a push of information out to individuals that is unexpected and appears to be intrusive, or an engagement with a third party to use information derived from the data collected that is not explained in the initial notification.

## Appendix 6: Privacy Program Facts and Questions

### What is the City of Seattle Privacy Program?

The Seattle Privacy Program provides policy direction, operational support, training and awareness, and guidance for City of Seattle employees concerning privacy impacts associated with collecting and managing the public's personal information. This includes information and resources about data collection, data retention, video capture technologies, mobile computing, social media and web-based interactions that are conducted in the course of doing City business.

### What is Personal Information?

*Personal information* is any information relating to an identified or identifiable individual. Examples of personal information include but are not limited to a person's name, home or email address, social security number, religion, political opinions, financial and health records, location and racial and ethnic origin.

### Why does the City collect personal information?

The City collects personal information to deliver services and to protect property and people. We collect information when a resident pays a utility bill, renews a pet license, a visitor browses a web page, or signs up for an email list. Police, fire and emergency services also collect different forms of video and electronic data when they respond to an emergency. Individuals provide some information voluntarily when they request services and some we collect to as part of our role in providing utilities, permits, transportation and public safety services.

### Why is privacy important?

While privacy laws protect some of the personal information we collect, most of it becomes a government record that others can ask to see through public records requests. Therefore, it is important the public know when and how personal information is collected, how we use it, how we disclose it and how long we keep it. To earn the public's trust we should communicate how we intent to use data at the time it is collected and honor this commitment throughout the time we possess it.

### What will undergo Privacy Reviews?

All projects that collect personal information will be subject to a privacy review. The Privacy Review process is comprised of three parts. The first is identifying whether a project or application involves the collection and management of personal information. The second part is determining the level of potential privacy risk and if using the privacy review process in our Privacy Toolkit may be sufficient to meet privacy obligations. The third part is a Privacy Impact Assessment that provides an in-depth analysis of the project to determine privacy impacts steps or strategies to decrease those impacts.

### Does the public have input into the process?

At the beginning of this program, we asked for ideas and best practices recommendations from community leaders, privacy advocates, academics, and corporate privacy leaders. Now that we are launching the program, we will start to post privacy review results on our public website so that the community can see what we are reviewing. Public members are welcome to contact us at [privacy@seattle.gov](mailto:privacy@seattle.gov) with any questions or comments.

### Who has been involved developing the Privacy Program?

In October 2014, the City's Chief Technology Officer and the Seattle Police Department's Chief Operating Officer brought together a group of City employees from across many departments including Police, Fire, City Light, Transportation, Information Technology, Law, and the Seattle Public Library to develop a privacy program. This team worked together to create policies and processes that govern how the City approaches privacy-impacting decisions. They worked to write a set of Privacy Principles and a Privacy Statement that communicates the City's privacy practices to the public. In addition, the group also educating City departments on privacy practices and assess compliance.

To advise these efforts, we assembled a Privacy Advisory Committee. The Committee included recognized thought - leaders from academia, companies, law firms, community advocacy groups, and other leaders who focus on privacy concerns. Committee member names can be found [here](#).

### Which departments and employees will be involved in the program?

All City of Seattle Departments and external agencies with which we share that information in the course of delivering City services or protecting public safety and critical infrastructure. See the [Seattle.gov website](#) for a complete list of City departments and agencies.

### What is not included in this program?

The commitments we make about privacy only pertain to the information we collect from the public. The information that is not covered includes the following:

- Personal information we obtain in our capacity as an employer. Employment information is covered under separate polices which may be found on our [Human Resources website](#).
- Actions taken or information collected by county, state or federal government agencies outside of City service delivery and function.
- Data collection or use of technologies governed by the City's Surveillance Ordinance (SMC 14.18)

### How does this work with state and federal laws?

We abide by all state and federal laws that pertain to the collection, management and disclosure of personal information. Our privacy policies are not in place of nor are they designed to conflict with those laws. For more on this, please see the regulations and laws that apply to us on our website, [here](#).

### How does this affect those companies and individuals doing business with the City?

Entities entering into contracts with the City will encounter clauses in our contracts that describe our expectations and third party obligations about handling personal information. Our contract specialists will discuss this with you in more detail.

### Where can I go if I have more questions?

Please visit our Privacy Program webpage to find more about our new privacy policies and privacy review process. You are also welcome e to contact our Privacy Program Manager at [privacy@seattle.gov](mailto:privacy@seattle.gov) with any questions or comments.