Privacy Recommendations

Data Collection for Design Review Early Community Outreach

Contents

[Purpose 1](#_Toc513645399)

[Scope 1](#_Toc513645400)

[Four Steps to Privacy 1](#_Toc513645401)

[1. Provide notice 1](#_Toc513645402)

[2. Limit Data Collection 2](#_Toc513645404)

[3. Plan for records retention 2](#_Toc513645406)

[4. Keep Information Secure 2](#_Toc513645408)

[Appendix A: Data Collection Notification Language 4](#_Toc513645410)

[Appendix B: SUrvey Guidance 6](#_Toc513645411)

# Purpose

This guideline provides recommendations to protect personal information collected from the public. The potential of sensitive information, should it fall into the wrong hands, to compromise the safety or security of families and their data warrants taking care when collecting and managing their data. This guide will assist developers/applicants conducting Early Community Outreach as part of the Design Review Program by providing best practices for managing the data collected during community outreach.

# Scope

These recommendations apply to developer-led public outreach communication and events in service of SDCI’s Design Review process.

# Four Steps to Privacy

* Provide notice that data is being collected and may be made public. See Appendix A notice language provided for various data collection methods.
* Limit data collection to only what is required for the specific purpose.
* Put records retention and deletion processes in place in case of a public records request.
* Keep information secure and private

## 1. Provide notice

It is important to inform members of the public when their personal data is being collected and that because it is being collected on behalf of the City of Seattle, it may be subject to public records requests. The purpose of the Public Records Act is to provide transparency about government operations and the information we collect about the public. This means that names, addresses, personal details and comments collected and submitted through the permitting process must be sent to anyone who submits a formal record request to the City for this information. For details, see the State of Washington Public Records Act ([RCW 42.56](http://apps.leg.wa.gov/rcw/default.aspx?cite=42.56)).

### ReCommended Actions

Developers/applicants must provide notice about the collection of information and the public records act for all occasions where public information is gathered that is linked to an identifiable individual or member of the public. This means written notice language must be posted and provided in invitations to events, at meetings that are audio-recorded or photos are taken, wherever sign-in sheets are collected, on portals or webpages where electronic or written comments or other means of collecting information, or through email exchanges. Please see Appendix A for notice language that the City of Seattle uses for these purposes and that may be adapted for use by applicants.

## 2. Limit Data Collection

When asking for personal information, it is important to limit the data being requested to only what is required and to tailor questions to collect the minimum amount of information about an identifiable person. Only ask questions and share information that directly relate to the design of new development.

### Recommended Actions

Some examples of limiting data collection to protect privacy are:

* When posting sign-in sheets, request only first name and last initial.
* If demographic information must be collected, provide a separate, anonymous form or link to a survey that does not collect personally identifying information.
* Instead of a street address, ask for the individual’s zip code or email address.
* Use age ranges instead of requesting birthdate (1-20, 21-40, 41-60, 61-80, 81-older).
* If race or ethnicity information is required, consider providing options that avoid the inclusion of countries of origin.
* Do not take photos or videos of audiences at in-person events, particularly those that show identifiable facial features.

For more guidelines about protecting privacy when designing surveys see Appendix B.

## 3. Plan for records retention

The potential for a public records request means that the applicant/developer needs to maintain all records of public interactions and engagements required as part of their Early Community Outreach for Design Review . The current City requirement for permit record retention is 6 years. Please check with SDCI for the latest records retention requirements.

### Recommended Actions

* Locate and store all records associated with the required Early Community Outreach in a safe and secure location or electronic file and be prepared to provide it to the City if requested to fulfill a records request.
* Delete or shred records that are no longer required.

4. Keep Information Secure

Anyone handling personal information must accept responsibility and use good judgement for keeping it secure and private. Paperwork containing personal information should be secured and locked, and computer systems should have passwords and the latest software versions and virus protection running.

### Recommended Actions

Below are some privacy best practices to consider for securing sensitive information:

#### files and papers

* Install a lock on a file cabinet that currently is without one.
* Keep completed paperwork and documents locked up when not in use.
* Shred paper with personal information when no longer needed. Do not throw it away or recycle it.
* Don’t leave documents, faxes, or lists with personal information on desks or counters when not in active use. Put them in folder, lock them away in a file or box with a closed or secure lid or turn them over so they cannot be read. Provide a covered file box for immediate form storage needs.
* Use good judgement on how much access to information to allow individual employees.

#### Working Space

* Install door locks that open with a combination code instead of a key. This facilitates rekeying when an employee leaves.
* Secure an area for document storage staff to use by changing the file room door knob without a lock, to a door knob with a lock.
* Post a sign that says, “Authorized Personnel Only” to limit access to a protected area.

#### Computers

* Consider creating a project-specific email address to be de-activated at the end of the Design Review Early Outreach process.
* Give all computer users their own computer password. Sharing passwords is an issue for both security and accountability if someone uses the computer for non-business reasons.
* Set up software to limit access to personal information to those who need it to do their jobs.
* Keep computer backup copies secured or locked up.
* Position computer screens so people passing by cannot read any personal information.
* Set up screen savers that blank out the screen when not in use for a few minutes and require passwords to open again.
* All emails sent or received that contain personal information must be encrypted. For example, Encryption is available with Outlook, and SharePoint is another secure method of sharing files. Similar services are available on Google and other email systems.
* When an employee leaves, cancel their computer password.

|  |
| --- |
| Appendix A: Data Collection Notification Language |

This language is for private developers to use when completing the early community outreach activities required by the Seattle Department of Construction & Inspections (SDCI) as part of the Design Review program. This language should be prominently displayed before the public fill out a form, enters an event or responds to a phone call.

|  |  |  |
| --- | --- | --- |
| Use Case | Description | Notification |
| Telephone call recording | For use in all instances of recorded telephone sessions, including call centers. | For customer services purposes, this call may be recorded. |
| Electronic forms | For use on all electronic forms, applications, surveys, sign-in sheets, petitions, or other modes of information collection. | This information is being collected by [NAME OF COMPANY OR DEVELOPER], but may be submitted to the City of Seattle. To learn more about how this information is managed please see the City’s [Privacy Statement](http://www.seattle.gov/tech/initiatives/privacy). |
| Paper forms | For use on all paper forms, online surveys, sign-in sheets, or other modes of information collection. | This information is being collected by [NAME OF COMPANY OR DEVELOPER], but may be submitted to the City of Seattle. Therefore, personal information entered on this form may be subject to disclosure to a third-party requestor pursuant to the Washington Public Records Act.  |
| Email communications | For use on applicant email signature lines for communication with the public. | This information is being collected by [NAME OF COMPANY OR DEVELOPER], but may be submitted to the City of Seattle. All emails and attachments, including personal information, sent and received as part of the required Early Outreach for Design Review are public records subject to the Washington Public Records Act, and may be subject to disclosure by the City of Seattle to a third-party requestor. To learn more about how this information is managed please see the City’s [Privacy Statement](http://www.seattle.gov/tech/initiatives/privacy). |
| Public events image and audio recording | For use at public events where digital images or recordings are made. (This is not encouraged). | Cameras and audio recording devices are in use for this event. |

# Appendix B: SUrvey Guidance

The City provides the following as guidelines for the creation of surveys:

* Only ask questions that directly relate to the new development or to better understand the neighborhood context.
* Do not include the City or Department logos or anything else that would give the impression that the survey was designed by City staff.
* Display prominent notice of data collection and the Public Records Act on the first page of the survey.
* Indicate required versus optional data entry fields with an asterisk.
* Secure the information collected via survey by not sending it over email unless it is encrypted; and once collected, download and store in a secure system.
* Do not collect IP address or other system information linkable to an individual (this is an option with SurveyMonkey and other survey services).
* Limit use of open text fields. This limits the possibility of users mistakenly providing sensitive information like family names, addresses, health and income information, or other data points. Instead of open data fields, use radio buttons, multiple choice, or yes/no options.