2019 Privacy Impact Assessment

CHIPS

Seattle IT

Seattle
Information Technology

Privacy Impact Assessment overview

What is a Privacy Impact Assessment?

A Privacy Impact Assessment ("PIA") is a method for collecting and documenting detailed information collected in order to conduct an in-depth privacy review of a program or project. It asks questions about the collection, use, sharing, security and access controls for data that is gathered using a technology or program. It also requests information about policies, training and documentation that govern use of the technology. The PIA responses are used to determine privacy risks associated with a project and mitigations that may reduce some or all of those risks. In the interests of transparency about data collection and management, the City of Seattle has committed to publishing all PIAs on an outward facing website for public access.

When is a PIA required?

A PIA may be required in two circumstances.

- When a project, technology, or other review has been flagged as having a high privacy risk.
- When a technology is required to complete the Surveillance Impact Report process. This is one deliverable that comprises the report.

How to complete this document?

As department staff complete the document, they should keep the following in mind.

- Responses to questions should be in the text or check boxes only, all other information (questions, descriptions, etc.) should **NOT** be edited by the department staff completing this document.
- All content in this report will be available externally to the public. With this in mind, avoid using acronyms, slang, or other terms which may not be well-known to external audiences. Additionally, responses should be written using principally non-technical language to ensure they are accessible to audiences unfamiliar with the topic.

1.0 Abstract

1.1 Please provide a brief description (one paragraph) of the purpose and proposed use of the project/technology.

This application supports administration of the Seattle Preschool Program by staff in the Department of Education and Early Learning with a Dynamics 365 application. The project also includes a public-facing Web portal for parents and providers who participate in the program.

1.2 Explain the reason the project/technology is being created or updated and why the PIA is required.

This project is to enhance the existing Microsoft Dynamics-based application and its associated public facing portal to add functionality and improve the experience for City staff and program parents and providers.

A PIA is required for this project due to the sensitive nature of the data involved. The CHIPS application involves the following types of data: name, address, children's data, birthdate, phone number, email address, email correspondence, income information, sex/gender, race/ethnicity, household information, language, enrolled preschool, preschool attendance, and homeless, and foster status.

This PIA provides public transparency around data management practices for CHIPS data and the project overall.

2.0 Project / Technology Overview

Provide an overview of the project or technology. The overview gives the context and background necessary to understand the purpose, mission and justification for the project / technology proposed

2.1 Describe the benefits of the project/technology.

The application will streamline administrative tasks for Department of Education and Early Learning staff and improve their ability to manage the program efficiently. The web-based portal will allow preschool providers to maintain their own information and parents to apply for and enroll their children in the program online.

2.2 Provide any data or research demonstrating anticipated benefits.

The web-based portal for parents of preschool children has supported the submission of nearly 2000 applications for the 2018-2019 school year and nearly 900, so far, for the 2019-2020 school year (compared to approximately 500 applications total before the web-based portal.) Allowing parents to apply for City programs online has increased the accessibility of the programs to the public.
For the 2018-2019 school year, DEEL managed enrollment paperwork for over 750 children on paper, collecting documents via mail and confidential fax. Over 450 more were managed through the web-based provider portal for preschool providers. The management of enrollments through the web-based portal allowed staff to focus on serving families, rather than data entry. For the 2019-2020

school year, so far, nearly 1200 enrollments are already being processed in the web-based portals, allowing stronger customer service for families and a quicker turn-around in enrollment.

2.3 Describe the technology involved.

The application is built on the Microsoft Dynamics 365 platform. The public-facing portal is built using Microsoft Dynamics Portals.

The Portals are accessible by DEEL service providers and families, differentiated by permission levels. The Provider portal allows preschool and summer learning providers to enter child enrollment, child attendance, agency, site, and staff data. The Parent portal allows parents to learn about the preschool programs, submit an application and submit enrollment information/documents.

2.4 Describe how the project or use of technology relates to the department's mission.

This application allows Department staff to manage the Seattle Preschool Program which is one of the Department's strategic investments in education. The public-facing portal allows families and providers to more easily engage with the program.

2.5 Who will be involved with the deployment and use of the project / technology?

The Seattle IT Dynamics team will develop, deploy, and maintain the application. Department of Education and Early Learning staff will use the internal application. Program providers and families will access the public-facing portal.

3.0 Use Governance

Provide an outline of any rules that will govern the use of the project / technology. Please note: non-City entities are bound by restrictions specified in the Surveillance Ordinance and Privacy Principles and must provide written procedures for how the entity will comply with any restrictions identified.

3.1 Describe the processes that are required prior to each use, or access to/ of the project / technology, such as a notification, or check-in, check-out of equipment.

No equipment is required to access this application other than a Web browser for both the internal application and the public-facing portal.

Portal users can log in to the Web portal either by registering a new account (if they're a parent) or by being invited to use the portal (if they're a provider). When a portal user registers a new account, they are provided with the City's standard notification language that personal information is being collected. The notification language is as follows:

"The City of Seattle collects the public's data delivering everyday City services, such as paying a utility bill, renewing a pet license, browsing a web page, signing up for an email list, and the City's delivery of public safety services. As technology is increasingly used to improve how we deliver City services, our collection and management of information will also continue to grow. We understand how important this information is and have a privacy program in place to review how and when we collect, manage, use, and protect it. For more information, click on the buttons below." (With links to our Privacy Statement at the bottom of the page.)

3.2 List the legal standards or conditions, if any, that must be met before the project / technology is used.

There are no legal standards or conditions that must be met prior to use of the technology.

3.3 Describe the policies and training required of all personnel operating the project / technology, and who has access to ensure compliance with use and management policies.

DEEL staff and external agency users will be required to review and sign a User Agreement stipulating proper procedures for handling sensitive information. The User Agreement addresses proper protocol for accessing, storing, and destroying data. DEEL staff will receive additional training in line with City of Seattle expectations to ensure adherence to governing security regulations. Program managers will monitor staff's completion of required training. Copies of training sign-in sheets and User Agreements will be retained to verify training completion.

4.0 Data Collection and Use

Provide information about the policies and practices around the collection and use of the data collected.

4.1 Provide details about what information is being collected from sources other than an individual, including other IT systems, systems of record, commercial data aggregators, publicly available data and/or other city departments.

Most data is collected by and stored within the CHIPS system. The data not collected directly by the CHIPS system is additional address information (such as latitude, longitude, school zones, Council districts.) This information is pulled from the Seattle IT's GIS address service for specific addresses.

4.2 What measures are in place to minimize inadvertent or improper collection of data?

Data collection is minimized to absolute bare requirements needed to enroll a child in a preschool program and determine their eligibility. Careful review is done with the Privacy Team at the City of Seattle to ensure only the basic requirements are collected and stored for program eligibility.

Providers and families have access to the information collected about them through the portal. In some cases, they can correct the data through the portal themselves. In cases where data is not editable through the portal, users can contact the Department via email or phone (contact information is prominently displayed on the portal).

4.3 How and when will the project / technology be deployed or used? By whom? Who will determine when the project / technology is deployed and used?

The project and any updates will be deployed after approval from the business owners in the Department of Education and Early Learning. Deployments will be conducted by the Seattle IT

Dynamics team. The business owners have the ultimate approval for whether the project and updates are deployed.

4.4 How often will the technology be in operation?

Both the internal application and public-facing portal are available 24 hours a day, every day.

4.5 What is the permanence of the installation? Is it installed permanently or temporarily?

CHIPS is a permanent installation.

4.6 Is a physical object collecting data or images, visible to the public? What are the markings to indicate that it is in use? What signage is used to determine department ownership and contact information?

There is no physical object that has in use indicators. However, on the public facing portal site there is notification language indicating that personal information is being collected and may be subject to public disclosure. This language has been identified in 3.1 of this document.

4.7 How will data that is collected be accessed and by whom?

Authorized staff in the Department of Education and Early Learning have access to information about provider information and program applications and enrollments in the system. Access to data is granted or restricted based on security roles.

Parents will have access to their household's information through the portal.

Providers will have access to information about their program and staff and to some information about the children who are enrolled with them

The Seattle IT Dynamics team may also have incidental access to the data by way of providing operational support.

4.8 If operated or used by another entity on behalf of the City, provide details about access, and applicable protocols. Please link memorandums of agreement, contracts, etc. that are applicable.

This question is not applicable, as CHIPS is not operated or used by an outside entity.

4.9 What are acceptable reasons for access to the equipment and/or data collected?

Parents and guardians may access their children's data for the purposes of ensuring accuracy and completeness of the information they provide, including updating it as appropriate. Providers may access the data of the children they are responsible for in order to fulfill their job duties and provide services. DEEL staff will have access to the data in order to administer services and fulfill job requirements related to CHIPs implementation. Seattle IT staff may have incidental access to the data in providing operational support.

4.10 What safeguards are in place, for protecting data from unauthorized access (encryption, access control mechanisms, etc.) and to provide an audit trail (viewer logging, modification logging, etc.)?

Department staff must have a City Active Directory account with access to the application controlled by security groups and Dynamics security roles. License and access requests must be approved by the business owner.

Providers can only access the portal after receiving a registration invitation by Department staff. Provider users are granted specific roles to control what data they have access to.

Parents are able to register a new account on their own or can be invited by Department staff and are granted a role that limits access to only their own data.

Dynamics logs any changes made in the system, including what change was made, who made it, and when it was made.

5.0 Data Storage, Retention and Deletion

5.1 How will data be securely stored?

Data is stored in Dynamics, which requires a City account, a Dynamics license, and membership in the specific group that allows access to the Dynamics application, and security roles within Dynamics to be set.

5.2 How will the owner allow for departmental and other entities, to audit for compliance with legal deletion requirements?

Department of Education and Early Learning is responsible for ensuring compliance with data retention requirements.

5.3 What measures will be used to destroy improperly collected data?

Data can be permanently deleted from the system. Either full records or data from individual fields. If necessary, the fields can be removed from the application so no future data will be collected. Data can be deleted by DEEL staff or by IT staff as requested by DEEL.

5.4 Which specific departmental unit or individual is responsible for ensuring compliance with data retention requirements?

The Finance and Administration Division within DEEL is responsible for ensuring compliance with data retention requirements, working with the Performance and Evaluation and Operations units to apply the rules to the data stored within Dynamics 365. The City Clerk’s Office provides DEEL with a “Retention Schedule” based on program participants/applicants and funding structures. These business rules will determine the schedule data is deleted/archived.

6.0 Data Sharing and Accuracy

6.1 Which entity or entities inside and external to the City will be data sharing partners?

The data sharing partners associated with this project, external to the City, include:
1) Child-care providers who have access only to the data of the children they are responsible for serving
2) King County Public Health
3) Seattle Public Schools
4) Evaluators conducting classroom assessments

Data sharing agreements exist between DEEL and the external partners above.

Note: None of these groups have direct access to the data; rather DEEL simply shares specific sets of appropriate data with them, after getting consent from participants.
The only data sharing partners associated with this project, who are external to the City, are child-care providers who have access only to the data of the children they are responsible for serving.

6.2 Why is data sharing necessary?

Data sharing is necessary in order to give those listed in 6.1 access to the data of the children in their care, and to fulfill all business requirements related to full implementation of the CHIPS project.

6.3 Are there any restrictions on non-City data use?

Yes ☒ No ☐

6.3.1 If you answered Yes, provide a copy of the department's procedures and policies for ensuring compliance with these restrictions.

The entire database is only viewable by City staff. Providers and parents can see their own data from the portal after they log in. Parents can only see information related to their household. Providers can only see information related to the enrolled families they serve.

All restrictions around data use are provisioned in separate data sharing agreements with the groups identified in 6.1.

6.4 How does the project/technology review and approve information sharing agreements, memorandums of understanding, new uses of the information, new access to the system by organizations within City of Seattle and outside agencies?

Data sharing agreements are reviewed and approved by the Performance and Evaluation Team in the Department of Education and Early Learning.

6.5 Explain how the project/technology checks the accuracy of the information collected. If accuracy is not checked, please explain why.

Data entry forms utilize lists and required fields where appropriate to ensure data accuracy during data entry. Department of Education and Early Learning staff make use of prepared and ad-hoc views of the data to look for data discrepancies.

6.6 Describe any procedures that allow individuals to access their information and correct inaccurate or erroneous information.

Providers and families have access to the information collected about them through the portal. In some cases, they can correct the data through the portal themselves. In cases where data is not editable through the portal, users can contact the Department via email or phone (contact information is prominently displayed on the portal).

7.0 Legal Obligations, Risks and Compliance

7.1 What specific legal authorities and/or agreements permit and define the collection of information by the project/technology?

The Seattle preschool program levy was approved by Seattle voters in 2014; the Seattle City Council approved the implementation plan, which includes development of the CHIPS program.

7.2 Describe what privacy training is provided to users either generally or specifically relevant to the project/technology.

DEEL and Seattle IT staff are required to take an annual Privacy and Security Awareness Training. Any additional training is provided by the business unit.

7.3 Given the specific data elements collected, describe 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.

Because this is a SAAS solution, there is no physical access to the servers. The system is backed up on a regular basis to ensure the City of Seattle has access to its core information.

7.4 Is there any aspect of the project/technology that might cause concern by giving the appearance to the public of privacy intrusion or misuse of personal information?

CHIPS will contain data provided by parents or guardians about the children participating in Early Learning programs, as well as assessments for the participants. This information is currently collected in and shared from multiple databases and paper forms, and that same collection and sharing will take place with the Solution, though from a centralized source.

For data shared with other organizations, such as Seattle Public Schools, there is a concern regarding the recipient organization’s use of the data. In such cases, risk will be mitigated through a data sharing agreement.

The addition of providing access to their respective information to parents or guardians registered to use the web portal adds a level of risk. The risk will be controlled by requiring encryption and multi-factor authentication of the users.

8.0 Monitoring and Enforcement

8.1 Describe how the project/technology maintains a record of any disclosures outside of the department.

The Solution will capture date, time, and user ID of the logged-in person. This information will be logged for updated records, collaboration with notes and notifications within the solution, and for communication from within the solution to any external recipients of information via email. Audit reports will be available to review these logs, and can include the specific record, note or comments shared.

Data can be exported from CHIPS and shared with appropriate entities. Various data sharing agreements, maintained and monitored separately from this particular instance, establish structures for data sharing. The individual data sharing agreements dictate what information is required for each agreement and how it is to be shared, by and with whom.

8.2 What auditing measures are in place to safeguard the information, and policies that pertain to them, as well as who has access to the audit data? Explain whether the project/technology conducts self-audits, third party audits or reviews.

The City Auditor’s office may audit for compliance at any time.