Privacy Impact Assessment (PIA)

[AGENCY] webform/s

NSW Digital Channels Unit

Date Issued:

Version:



# About this PIA

The Digital Channels Unit (DCU) and the [Insert Agency] are undertaking a privacy impact assessment (PIA) to identify possible risks to an individual’s privacy by collecting personal information to [state purpose for collection]. The [Insert Agency] will collect personal information using web forms published on nsw.gov.au including:

* **[Webform Title]** - [state purpose for collection]. ([See [add](https://www.nsw.gov.au/departments-and-agencies/cabinet-office/access-application-form) link to form – CTRL+K]).
* **Add more forms as required**

This PIA was developed in consultation with [Insert Agency], OneCX Program [delete if not involved], and Digital Channels Unit (DCU) teams.

## Scope & Approach

This PIA assesses the ‘GIPA Request’ webform against the requirements defined in NSW:

* Privacy and Personal Information Protection Act 1998 (PPIPA)
* Information Protection Principles (IPPs) (PPIPA Part 2, Division 1)
* Government Information (Public Access) Act 2009 [Delete if not applicable- GIPA ONLY]
* Data Sharing (Government Sector) Act 2015
* State Records Act (1998)

This PIA is subject to review on an annual basis or to reflect any material changes to the contents of this document. Please note, significant change may be subject to change control procedures and necessitate a new Privacy Impact Assessment (PIA).

# Privacy Assessment

This section explains the collection, storage, use, access, and disclosure of personal information by the [Insert Agency].

## Business Context & Objectives

Add business context – what is being done, why this is being done and what value does it have for a NSW citizen. Remember it is important to keep a user-centric focus.

## Collection of Personal Information (PI)

Table 1 shows the PI data collected by the [Insert Agency] using the **[Webform Title], [Webform Title]** , **[Webform Title]** webform/s published on nsw.gov.au.

Table 1. Data collected for [Insert Agency] using nsw.gov.au web forms.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Data Collected** | **Data Type** | **Webform** | | |
| **[Webform Title]** | **[Webform Title]** | **[Webform Title]** |
| Title | List | \* | \* |  |
| First name | Text | \* | \* |  |
| Last name | Text | \* | \* |  |
| Email | Text | \* | \* | \* |
| Street address | Text |  |  |  |
| Suburb | Text |  |  |  |
| State | List | \* | \* |  |
| Postcode | Numerical | \* | \* |  |
| Message | Free Text | \* | \* |  |
| Add attachment | Varied file types |  |  |  |
| Collected From | | Individual | Media Representative | Individual |
| Privacy Collection Notice | | Notice D | Notice D | Notice B |

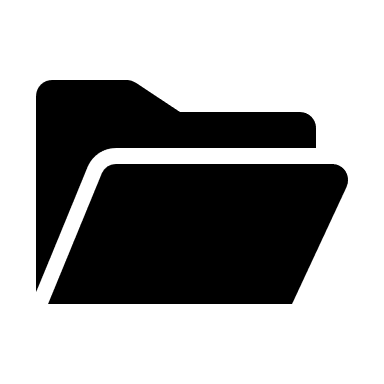
## PI Data Flow

Data submitted through the [Webform Title] webform is sent to the Content Management System (CMS) encrypted, then automatically transferred via API to a secure SharePoint folder in the [Insert Agency] (Figure 1).

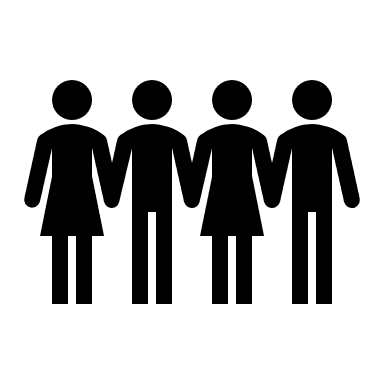
Web Form

CMS

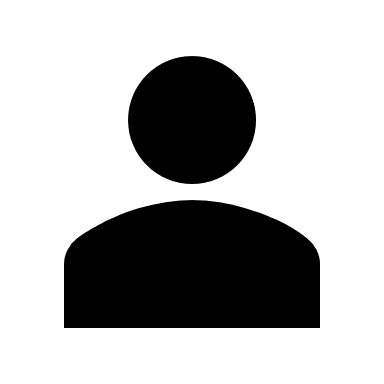
**[Agency]**



SharePoint



Agency Actors

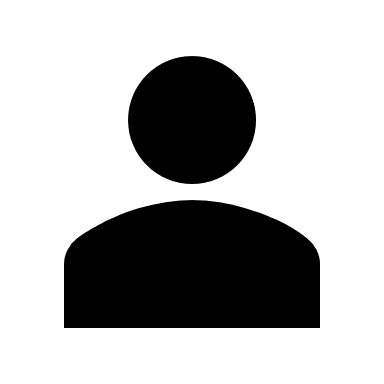
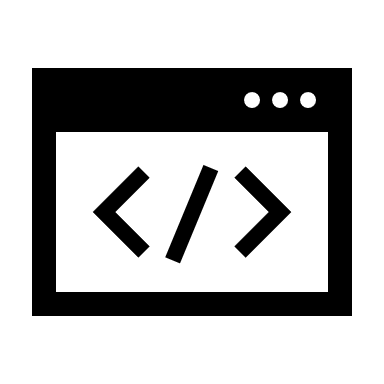


USER

API

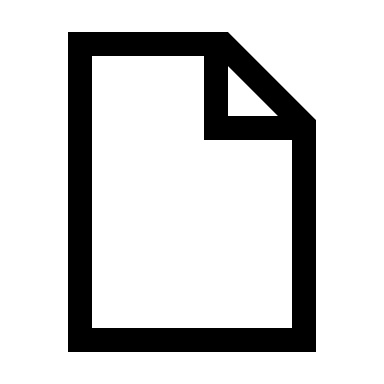
**nsw.gov.au**

Figure1. PI Data Flow



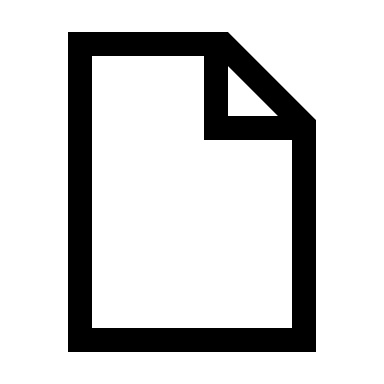
USER

**Media Enquiry**



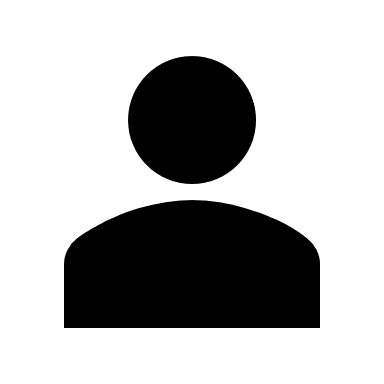
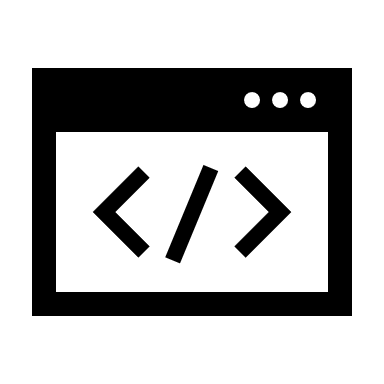
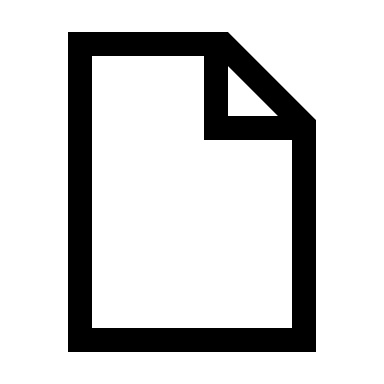
**CMS**

**Memo Subscription**

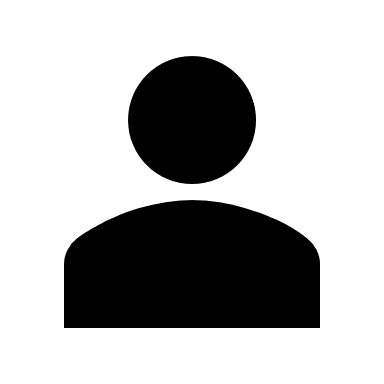


Unsubscribe & Manage Preferences

**Contact Us**



USER



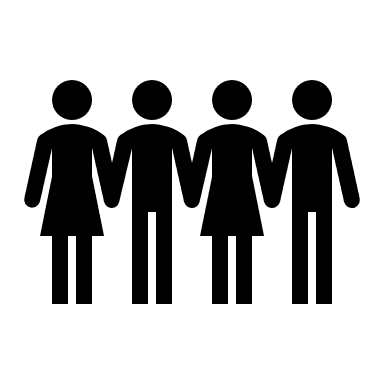
USER

**arp.nsw.gov.au**

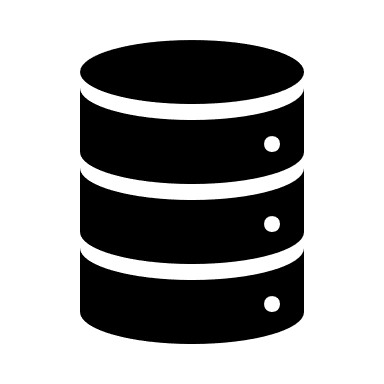
**nsw.gov.au**

**Premier’s Dept**

**arp.nsw.gov.au**



Agency Staff



## Information Rights

Persons who submitted a data using the [Webform Title], [Webform Title] may access, amend, or correct this information by [insert action]. Individuals will not have access to amend or update their data beyond the retention period. For issues or concerns relating to privacy, the individual may contact the [Insert Agency] [Team/Role] using the contact details provided in the PCN.

## Storage, Security and Retention

Collected web form data is stored in Australia by the OneCX program and [Insert Agency] as described below.

#### Nsw.gov.au

OneCX secures webform data within CMS in accordance with the NSW Cybersecurity Policy and Essential 8 Level 3 Maturity. OneCX retains data for 10 days to provide [Insert Agency] support and hyper care before automatically purging data. Access to the CMS is restricted by Multi-Factor Authentication (MFA) to DCU development staff for the sole purpose of providing [Insert Agency] support and services, and select [Insert Agency] staff for system management. All [Insert Agency] staff that require access to the CMS must complete privacy and CMS training before gaining authority to access the system.

#### [Insert Agency]

The SharePoint governance, classifications, permissions, and retention will be managed by [Insert Agency] in accordance with applicable legislation and OneCX terms and conditions (see 1.1). [Insert Agency] will restrict staff access to authenticated team members as outlined in Table 2. GIPA requests must be actioned by [Insert Agency] Staff within 5 working days of application receipt. Once finalised, GIPA requests are stored in [insert action] and retained for a period of [insert retention period]. Thereafter the data will be archived/deleted in accordance with the NSW State Records Act to the [Insert Agency] electronic document management system, that complies with the State Records Act means to lawfully dispose of State records. Individuals will not have access to amend or update their data beyond the retention period.

Table 2. Data storage, access, and retention.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Web Form** | **Data Location** | **Managed By** | **Accessed By** | **Retention** |
| [Webform Title] | SharePoint folder | [[Insert Agency] ROLE] | [[Insert Agency] TEAM] | [time] |
| Add more as required |  |  |  |  |

## Use

The [Insert Agency] will restrict access and use of the data to the primary purpose outlined in 2.1. above. The [Insert Agency] will not create user profiles for enquires, nor cross-reference the collected PI with any other sources of personal information. The purpose and administration of this data collection does not require technical support or assistance by a third-party vendor.

## Disclosure

[Insert Agency] will not share webform data with any [Insert Agency] unless the enquiry falls outside [Insert Agency] purpose, functions, or activities. In this case, the [Insert Agency] will make enquiries to find the lawful collection authority and seek consent, if required, before passing the form details to the rightful [Insert Agency] (as per IPP3, IPP4 and s18(1a)).

# Findings

Table 2 summarises privacy risks associated with the collection of personal information as outlined in Section 2. Each risk is rated using the NSW Department of Customer Service Risk Matrix reported likelihood, consequence, and overall risk rating (see Appendix A). Recommendations to mitigate the privacy risks are categorised as Compliance (C) actions required to comply with legislative requirements and Best Practice (BP) actions designed to ensure we meet community expectations and avoid reputational risk.

Table 2. Privacy Analysis Findings

| **Privacy Requirements** | **Findings** | | **Recommendations** | |
| --- | --- | --- | --- | --- |
| **Identified Risk** | **Rating** | **Ref** | **Description** |
| **IPP 1: Lawful**  Only collect personal information for a lawful purpose, which is directly related to the [Insert Agency] ’s function or activities and necessary for that purpose. | **NO FINDING**  Data collected for a lawful purpose (2.1, GIPA s41). |  |  |  |
| **IPP 2: Direct**  Only collect personal information directly from the person concerned, unless they have authorised collection from someone else, or if the person is under the age of 16 and the information has been provided by a parent or guardian. | **NO FINDING**  Data collected directly from individual (Figure 1). |  |  |  |
| **IPP 3: Open**  Inform the person you are collecting the information from why you are collecting it, what you will do with it and who else might see it. Tell the person how they can view and correct their personal information, if the information is required by law or voluntary, and any consequences that may apply if they decide not to provide their information. | **NO FINDING**  PCN provided (2.1). |  |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **IPP 4: Relevant**  An [Insert Agency] must ensure that your personal information is relevant, accurate, complete, up-to-date and not excessive. The collection should not unreasonably intrude into your personal affairs. |  |  |  |  |
|  |
|  |
|  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **IPP 5: Secure**  Store personal information securely, keep it no longer than necessary and dispose of it appropriately. It should also be protected from unauthorised access, use, modification, or disclosure. | **NO FINDING**  Data secure (2.5) |  |  |  |
| **IPP 6: Transparent - Access and Accuracy**  Explain to the person what personal information about them is being stored, why it is being used and any rights they have to access it. | **To be determined**  Complete section 2.4 and 2.5 to assess gaps and identify risks |  |  |  |
| **IPP 7: Accessible**  Allow people to access their personal information without excessive delay or expense. | **To be determined**  Complete section 2.4 and 2.5 to assess gaps and identify risks |  |  |  |
| **IPP 8: Correct**  Allow people to update, correct or amend their personal information where necessary. | **To be determined**  Complete section 2.4 and 2.5 to assess gaps and identify risks |  |  |  |
| **IPP 9: Accurate**  Make sure that the personal information is relevant, accurate, up to date and complete before using it. | **NO FINDING**  Data accurate and current (2.5) |  |  |  |
| **IPP 10: Limited**  Only use personal information for the purpose it was collected unless the person has given their consent, or the purpose of use is directly related to the purpose for which it was collected, or to prevent or lessen a serious or imminent threat to any person’s health or safety. | **NO FINDING**  Data use limited (2.5) the stated purpose (2.1) |  |  |  |
| **IPP 11 - Restricted**  An [Insert Agency] can only disclose your information in limited circumstances if you have consented or were informed at time collection. An [Insert Agency] can also disclose your information if it is for a directly related purpose and it can be reasonably assumed that you would not object, if you have been made aware that information of that kind is usually disclosed, or if disclosure is necessary to prevent a serious and imminent threat to any person’s health or safety. | **NO FINDING**  Data use limited (2.5) the stated purpose (2.1) |  |  |  |
| **IPP 12 – Safeguarded**  An [Insert Agency] cannot disclose sensitive personal information without consent, for example, information about ethnic or racial origin, political opinions, religious or philosophical beliefs, sexual activities, or trade union membership. It can only disclose sensitive information without consent if disclosure is necessary to avert a serious and urgent threat to health or safety. | **NO FINDING**  Data safeguarded. |  |  |  |

# Recommendation Response Plan

This section presents the best practice recommendations, the leadership approach and approved planned actions to address recommendations. Table 3 presents the Leadership Teams commitment to and rationale for addressing the recommendations, with agreed actions and responsibilities outlined in Table 4.

Table 3. Recommendation Approval and Action Rationale

| **Ref** | **Description** | **Approval** |
| --- | --- | --- |
| C.1 | [Insert Agency] requires a procedure to remove or redact personal, sensitive and health information collected from the free text field that is not required to respond to the enquiry. | [Insert Agency] [Decision]  If approved – add actions to Table 4  If rejected – provide reason or planning for future work. |
| C.2 |  |  |
| C.3 |  |  |
| C.4 |  |  |
| BP.1 | Create a reminder on the free text ‘Message’ form field to remind users not to add Personal, Health or Sensitive information. | APPROVED – See A.3 |
| BP.2 |  |  |

Table 4. Recommendation Implementation Plan

| **Action** | | **Ref** | **Status** | **Responsible** | **Date** |
| --- | --- | --- | --- | --- | --- |
| A.1 | Add the following reminder to the free text ‘Message’ field “Please do not provide detailed personal, health or sensitive information within your message” to the ‘Contact Us’ and ‘Media Enquiry’ web forms. | BP.2 | Identified | Web form owner? |  |

# Approvals and Endorsements

This PIA was prepared by [Author] ([Author role]) on [Day] [Month] [Year].

## Approvals

The following Department Customer Service employees **recommend** the project proceeds as proposed in this document.

|  |  |  |  |
| --- | --- | --- | --- |
| Name: |  | 1. Signature: | |
| Position: |  |
| Agency: | 1. Department of Customer Service | 1. Date: |  |

|  |  |  |  |
| --- | --- | --- | --- |
| Name: | Simon Hatty | 1. Signature: | |
| Position: | Senior Manager Platforms and Operations |
| Agency: | Department of Customer Service | 1. Date: |  |

The following [Insert Agency] employees **recommend** the project proceeds as proposed in this document.

|  |  |  |  |
| --- | --- | --- | --- |
| Name: |  | 1. Signature: | |
| Position: |  |
| Agency : |  | 1. Date: |  |

Add further names as required

## Endorsement

The following Department Customer Service employees have **endorsed** this document.

|  |  |  |  |
| --- | --- | --- | --- |
| Name: |  | 1. Signature: | |
| Position: |  |
| Agency: |  | 1. Date: |  |

|  |  |  |  |
| --- | --- | --- | --- |
| Name: |  | 1. Signature: | |
| Position: |  |
| Agency: |  | 1. Date: |  |

The following [Insert Agency] employees have **endorsed** this document.

|  |  |  |  |
| --- | --- | --- | --- |
| Name: |  | 1. Signature: | |
| Position: |  |
| Agency: | 1. [Insert Agency] | 1. Date: |  |

Add further names as required

**Appendix A – Risk Rating Matrix**

NSW Department of Customer Service Risk Matrix reported likelihood, consequence, and overall risk rating. For example, Risk rating 4.2.12 represents a Medium rated risk that is likely to happen with minor consequences.

