**PRIVACY IMPACT ASSESSMENT FOR [INSERT PROJECT NAME]:**

**COMPLIANCE WITH THE REQUIREMENTS OF THE PRIVACY ACT 2020**

A Privacy Impact Assessment **must** be completed if your project involves personal information. Personal information is any information about an identifiable individual – such as their name, address, photo, opinion or viewpoint. The information does not need to name someone specifically, as long as they are identifiable in other ways.

A Privacy Impact Assessment is not required for projects making only minor changes to an existing system. However, if an existing system is being changed, and a Privacy Impact Assessment has not been completed previously for the system concerned, a Privacy Impact Assessment is recommended.

**Summary of the requirements of the Privacy Act 2020**

1. Only collect personal information you need
2. Get it directly from the individual when possible, unless an exception under the Privacy Act 2020 applies
3. Be open about what you are going to do with it
4. Be fair about how you get it
5. Keep it secure
6. Let people see their own information
7. Correct it if it is wrong
8. Make sure it is accurate before you use it
9. Dispose of it when you no longer need it
10. Only use it for the reason it was collected, unless an exception applies
11. Only share it if you have a good reason
12. Only send it overseas if it will be adequately protected
13. Only use unique identifiers when it is clearly allowed and minimise the risk of their misuse

**Please contact the Registrar’s office if you have any questions or wish to discuss (**[**generalcounsel@otago.ac.nz**](mailto:generalcounsel@otago.ac.nz)**).**

**QUESTIONS FOR PRIVACY IMPACT ASSESSMENT**

**General**

1. Please give a brief description of how the Project will utilise personal information.
2. How will the Project change existing University systems/infrastructure?

**Collection of personal information (IPP 1 to 4)**

1. What personal information will be collected, used or disclosed?

|  |  |  |  |
| --- | --- | --- | --- |
| Type of personal  Information | Source of  Information\* | Purpose of information  for the system or service | Is any of the information sensitive \*\*?  (Tick) |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

*\*For example, are you collecting the data directly from the individuals concerned; from other University systems/data source; publicly available sources; and/or other non-public sources (e.g. where individual authorised such collection, the individual will not be identified, or where collecting the information from individual concerned will undermine purposes of the collection)?*

*\*\* Sensitive information might include information about an Individual’s racial or ethnic origin, political opinions religious or philosophical beliefs, trade union membership, genetics, biometrics, health, sex life, sexual orientation and criminal convictions. It may also include student health information, employee performance or remuneration details, financial information (such as bank account and credit card details), or sensitive research data involving human participants.*

**Collection of personal information (IPP 1 to 4)**

1. Approximately how many people’s information will be held?

* Less than 10
* Between 10 to 50
* More than 50

1. Will information that is already held be used for a new purpose? Why and how?
2. How will individuals be informed about what is happening to their personal information?

* It is covered by an existing University privacy statement (please identify the statement(s) in question and how it applies – e.g., [Student Privacy Statement](https://www.otago.ac.nz/administration/privacy/otago034437.html))
* It is partially covered by an existing University privacy statement, and it is proposed that the statement will be updated (please identify the statement(s) in question and what the proposed changes are)
* A privacy statement or policy is going to be drafted
* It is not necessary for one of the following reasons (please explain):
  + The collection of information is from a public source
  + The information is already held by the University and is not being directly sourced from the individuals concerned
  + The information will not be used in a form where the individual concerned is identified (e.g. information will be used for statistical or research purposes and will not be published in a form that could reasonably be expected to identify the individual concerned)

1. Are you proposing to collect information from individuals under the age of 18? If so, please explain what information you propose to collect and the measures you will put in place to ensure that the collection of such information is fair and not unreasonably intrusive (e.g., obtaining parental consent).

* Yes (please explain)
* No

**Storage and security of personal information (IPP 5)**

1. How will the personal information be stored? Will there be a change in the way the personal information is stored or secured? For example, storing information in the cloud.
2. What safeguards will be put in place to protect the security of the personal information – tick all that apply:

* Policies – please specify
* physical and technical controls (e.g. security and access control)
* staff training – please specify
* confidentiality clauses – please specify
* other – please specify

1. Do contracts with third parties include privacy clauses and safeguards?
2. Are third parties required to notify the University in the event of a privacy breach?
3. Please confirm whether the Project has received approval from Cyber Security?
4. **Individuals’ Access to their Information (IPP 6 and 7)**
5. The Privacy Act requires that individuals be able to access and request copies of their information. Please confirm which of the following applies and provide any comments below:

* Individuals will have direct access to all information held about them so will not need to make requests
* Requests for all or any information about an individual or individuals will be easy to facilitate (searching and provision of information is well supported)
* Requests for all or any information about an individual or individuals will be able to be met, but this will take significant work or time (searching and provision of information is not well supported)
* Individuals will not be able to access information about them (this is not normally an acceptable option – please explain).

1. The Privacy Act allows people to request correction to information about them. Will the system have facility for updating information, or attaching a note to an individual’s record to indicate a correction request was made?

* Yes
* No (please explain)

**Using or disclosing the personal information (IPP 8 to 13)**

***Accuracy (IPP 8)***

1. What processes are used to check that the information is correct, up to date, complete, relevant and not misleading? Tick all that apply

* Individuals provide their own information so are responsible for ensuring its accuracy
* Checking occurs prior to information being provided
* Individuals have access to their own information and can report any errors
* Other – please explain
* No specific checks in place – please explain (this is not normally an acceptable option – please explain)

***Retention and disposal (IPP 9)***

1. The Act requires that we must not keep personal information for longer than is required for the purposes for which the information may lawfully be used. Please confirm whether the Project has received approval from Corporate Records Services?
2. If the Project is sharing the information with a third party, how long will they hold the information for and what steps are in place to ensure that they dispose of it when the business requirement is completed?

***Limits on Use (IPP 10)***

1. Please confirm: the Project will only use the information for a purpose for which it was collected, and any future use outside of those purposes will be discussed with the University Privacy Officer before proceeding.

* Yes

***Limits on Disclosure (IPP 11)***

1. Who will have access to this information within the University?
2. How will access be managed? Tick all that apply

* Only relevant staff will have access to the parts of the system or records relevant to them (e.g., via passwords or physical access restrictions)
* Access to relevant parts of the system or records will be controlled by policy, staff training etc (i.e., staff may access records or parts of the system not relevant to them, but will be instructed not to).
* Staff other than relevant staff will have access (not normally acceptable, please explain).

1. Who will have access to this information outside the University? Explain on what grounds this information is provided outside the University.
2. Will personal information already held be used or disclosed in a new way?For example, will existing personal information be disclosed to parties who did not previously have access to it?

***Disclosure outside of New Zealand (IPP 12)***

1. Does the project involve personal information being sent outside of New Zealand?
2. If yes, in which countries are the intended recipients based?
3. How will this be managed to ensure compliance with the Privacy Act? Tick all that apply

* The recipients are subject to New Zealand law
* The recipients are located in a country with privacy laws which provide the same level of safeguard as New Zealand privacy laws (e.g., a country in the European Union, UK, Japan, Australia (except where this relates to employee data), Israel, Argentina, Canada (commercial organisations), Andorra, Faroe Islands, Guernsey, Isle of Man, Jersey, Switzerland, Uruguay).
* the affected individuals have provided written consent for the information to be sent outside of New Zealand after been informed that the country to which their information is being sent may not provide the same privacy safeguards as exist under New Zealand law
* the recipient has signed an agreement to protect the personal information in a way that, overall, provides comparable safeguards to those in the New Zealand Privacy Act.

***Unique identifiers (IPP 13)***

1. Please confirm: The Project
2. will only use unique identifiers when necessary;
3. will not assign a unique identifier to a person if that unique identifier has already been given to that person by another organisation; and
4. will take reasonable steps to protect unique identifiers from misuse (please specify).

* Yes
* No

**PRIVACY IMPACT ASSESSMENT – COMPLIANCE WITH REQUIREMENTS OF PRIVACY ACT 2020**

**To be completed by the Privacy Officer or Deputy Privacy Officer**

| # | Description of the  privacy principle | Assessment and measures to mitigate risk  (*Note for each principle whether the project complies or risks being non-compliant and how any risks will be mitigated)* | Assessment of compliance |
| --- | --- | --- | --- |
| 1 | Principle 1 - Purpose of the collection of personal information Confirm information will be collected for a lawful purpose connected with a function or activity of the University, and be minimised so that only the personal information required for that purpose is collected.  What is the purpose of collecting the personal information involved here? How will that enable the organisation to do what it needs to do? Are you only collecting what you actually need? |  |  |
| 2 | Principle 2 – Source of personal information Is information collected directly from individual, unless an exception under IPP 2 applies? |  |  |
| 3 | Principle 3 – Collection of information from subject How will you tell people everything in this checklist? Or will it be so obvious to them that you don’t need to spell it out? If you’re not going to be open with them about what you’re doing, which of the exceptions allows you to keep it from them? |  |  |
| 4 | Principle 4 – Manner of collection of personal information Will the Project involve a new way of collecting personal information? E.g. collecting information online rather than on paper forms?  Is the method of collection lawful, fair and not unreasonably intrusive upon the personal affairs of any individual? Particularly where the individual is a young person or child? |  |  |
| 5 | Principle 5 – Storage and security of personal information Has the Project obtained approval from Cyber Security? List applicable policies / agreements. |  |  |
| 6 | Principle 6 – Access to personal information Are people easily able to see their personal information if they want to? |  |  |
| 7 | Principle 7 – Correction of personal information  Can individuals correct their information if it is wrong, or have a statement of correction attached to their information? Are there limitations? (for instance character limits in data fields; or lack of ability to add a flag indicating there is relevant information held on a physical file) |  |  |
| 8 | Principle 8 – Accuracy etc. of personal information to be checked before use Are there reasonable steps in place to ensure information is correct, relevant and up to date before it is used?  How damaging will it be to the individual if information is wrong or misleading?(The more damaging it will be, the more extensive should the steps be for checking accuracy) |  |  |
| 9 | Principle 9 – Not to keep personal information for longer than necessary Has the Project received approval from Corporate Records Services? |  |  |
| 10 | Principle 10 – Limits on use of personal information Is the personal information used for the purposes for which it was collected? Or a related purpose?  Are you using it for a different purpose from the one for which you collected it? If so, is there an exception justifying this use? |  |  |
| 11 | Principle 11 – Limits on disclosure of personal information Identify everyone who will receive it. Is disclosure one of the purposes for which you collected the information? If so, was the individual told that at the time? (This links to principle 3.)  If you’re disclosing for a different purpose, is there an exception justifying the disclosure? Or another law that applies allowing you to disclose? |  |  |
| 12 | Principle 12 – Disclosure outside of New Zealand Will the Project be sharing the information overseas? If so, are the recipients subject to New Zealand law; located in a country with privacy laws which provide the same level of safeguards as New Zealand; the recipient has signed an agreement to protect the personal information in a way that compares overall to the safeguards provided in New Zealand; or the affected individual has provided written consent for the information to be shared to a recipient in a country that does not provide the same privacy safeguards as New Zealand. |  |  |
| 13 | Principle 13 – Unique identifiers Is it necessary to use unique identifiers? Have adequate steps been taken to protect unique identifiers from misuse? |  |  |
|  | Other privacy interests Would the Project be contrary to the expectations of, or could come as a surprise to, those individuals about whom the University collects and holds personal information? For example, the use of new or intrusive technology, altering the storage or security of the personal information, or bodily searches?  Does the Project involve changes to any of the University’s premises that will involve private spaces where students or staff or visitors may disclose their personal information? For example: Changing the location of the reception areas, where people may discuss personal details, or intrusions into physical spaces.  Consider what other relevant laws may be applicable. |  |  |

| The privacy impact for this project has been assessed as: | | Tick |
| --- | --- | --- |
| **Low** | There is little or no personal information involved; or the use of personal information is uncontroversial; or the risk of harm eventuating is negligible; or the change is minor and something that the individuals concerned would expect; or risks are fully mitigated |  |
| **Medium** | Some personal information is involved, but any risks can be mitigated satisfactorily |  |
| **High** | Sensitive personal information is involved, and several medium to high risks have been identified |  |
| **Reduced risk** | The project will lessen existing privacy risks |  |
| **Inadequate information** | More information and analysis is needed to fully assess the privacy impact of the project. |  |
| Reasons for privacy impact rating | | |
|  | | |

**Additional Comments:**

|  |  |  |  |
| --- | --- | --- | --- |
| **ACTIONS REQUIRED** | | | |
| **Action** | **Person Responsible** | **Timeframe** | **Date Action Completed** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

|  |  |
| --- | --- |
| Sign Off | |
| Name position (Project Manager) | Name position (Manager) |
| Signature | Signature |
| Date: | Date: |

|  |
| --- |
| Sign Off |
| Name position (Privacy Officer) |
| Signature |
| Date: |