# HOW TO COMPLETE A PRIVACY IMPACT ASSESSMENT (PIA)

This document supports the University's Privacy Impact Assessment (PIA) Procedures.

## Step 1 - Plan the PIA

### Assign Responsibilities and Describe the Proposed Undertaking

You must determine who is responsible for the PIA, the expertise and inputs required, important milestones, key decision-making points and how consultations will be carried out.

You should outline:

1. The context or setting of the proposed undertaking, including relevant legal, social, economic and technological considerations
2. The reason for the proposed undertaking
3. The proposed undertaking's overall aims and objectives and how these fit with the University's broader objectives
4. Any links with existing projects, technology and digital systems, products, services, programs and/or initiatives
5. The target market of the proposed undertaking, and
6. What personal and health information will be collected, how it will be used, accessed, disclosed or shared, stored and destroyed and how security and data accuracy will be addressed

Depending on the nature, size and complexity of the proposed undertaking, you should consider whether:

1. Expertise in a range of areas is required, including information privacy and data protection, technology and systems, risk management, law and ethics, and
2. The PIA should be conducted by an external assessor or expert who can help identify privacy impacts that have not been recognised and which may help develop community trust in the PIA findings and the proposed undertaking's intent.

If the proposed undertaking involves the use of a new form of technology or data processing, the undertaking's developer may have completed their own PIA, which you could use to inform your analysis

### Scope of the PIA

In preparing the PIA, you must consider the key attributes of the proposed undertaking's privacy scope and answer the following questions:

1. What is the quantity and type of personal information which will be collected, used, accessed, disclosed or shared, stored and destroyed?
2. Who will provide the personal information, or how will the personal information be provided (for example, collected directly from the person, or via an integration)?
3. Can the proposed undertaking's objectives be achieved without collecting some, or all, of the personal information?
4. Is health or sensitive information involved?
5. What is the size or complexity of the proposed undertaking?
6. Will the proposed undertaking involve cross-organisation/agency or cross-sector information sharing?
7. What is the likely community and/or media interest in the privacy aspects of the proposed undertaking?

8. Can any other PIA's and/or risk assessments relevant to the proposed undertaking be leveraged, or updated, to consider privacy risks associated with the current proposal?

## Step 2 - Stakeholder Consultation

Whether internal or external, stakeholders can offer valuable insights into what privacy risks might arise. In particular, approaching representatives of the people who will be the subjects of the personal information – whether students, staff or others – can be a powerful way to find out early if there are any privacy concerns about the project, what might be considered 'reasonable', or if there are any misconceptions that you need to address.

You must provide:

7. A list of internal and external stakeholders who are, or might be, interested in or affected by the proposed undertaking
8. An outline of any internal and external stakeholder consultation that will be, or has already been, conducted in relation to the proposed undertaking
9. Where relevant, a summary of the outcomes of any consultation
10. Where relevant, the reasons why stakeholders, or certain stakeholders, were not consulted, and
11. Whether the PIA development process can be used as part of a consultation strategy

## Step 3 - Map Information Flows

Describe and map the proposed undertaking's personal information flows. The analysis should be sufficiently detailed to provide a sense of what information is and how it will be managed throughout its lifecycle. This includes how it will be collected, used, accessed, disclosed or shared, transferred, stored or destroyed, the integration methods and who will have access to it.

You may wish to insert a diagram or table, either in this section or attached as reference information, that shows the flow of the information involved.

The mapping must describe:

1. Who will collect what information, and who it will be collected from
2. How the information will be collected, and for what purpose
3. How the information will be used or handled
4. The processes for ensuring information confidentiality and integrity
5. Whether the information will be disclosed to another business unit or School within the University, or third party agency or organisation, to whom and for what purpose
6. If the information is to be disclosed to and used by secondary users, how will those secondary users protect that information and what restrictions are in place to prevent them from passing it on to others
7. If the information is to be transferred between digital services, what is the integration method and encryption mechanism, and which data points will be transferred
8. Whether personal information will be transferred to a third party organisation either interstate in Australia or overseas
9. Whether individuals will be able to access and correct their personal information, and if the corrected information is adjusted to downstream applications, and
10. How long the information will be retained and when and how the information will be destroyed

If the proposed undertaking involves data linkage or matching, the mapping must also consider:

1. planned or potential data-matching or linking to other information held in different databases (by the University or third parties)
2. how any data-matching or linking will be done, and

3. any decisions affecting the individual or the information that might be made on the basis of data matching or linking

Mapping information flows is particularly important where artificial intelligence or other innovative processing systems are used, given that data can be moved around in multiple ways, making it difficult to maintain records and to control access. By understanding and documenting how personal information is being handled, you will be helping the University to improve its data governance, comply with its privacy obligations, and allow it to efficiently handle requests from individuals for access to their information

## Step 4 - Identify the Nature of the Process or Digital Service

Is the collection of data a mandatory requirement, or can it be established as an opt-in service?
Provide justification for your response

## Step 5 - Identify Privacy Risks and Possible Remedial Actions

Identify and assess the potential privacy impacts of the undertaking. As a first step, check how personal and health information will be handled in relation the privacy obligations set out in:

1. The PPIP Act and HRIP Act and regulations
2. The University's Privacy Policy and Privacy Management Plan, and any applicable Public Interest Directions
3. Where applicable, the Privacy Act 1988 (Cth)
4. If applicable, other extraterritorial laws such as the GDPR, and the extent to which this applies to the proposed undertaken and
5. Other legislation that applies to the University relating to the collection and use of personal and health information.

Consider whether there are other privacy risks that need to be addressed. For example:

1. Will individuals lose control over their personal information?
2. How valuable would the information be to unauthorised users? For example, is it information that others would pay money for or try to access by unethical means?
3. Is there a visible, comprehensive and effective complaint handling mechanism? (Refer to the University's Privacy Policy and Privacy Management Plan)
4. What auditing and oversight mechanisms are in place, especially if a system or digital service fails?

Does the proposed undertaking collect more information than is necessary? Consider the following:

1. If the person is already known to the University, is it necessary to establish identification points to prove who they are?
2. Are all data points collected necessary, or are they just "nice to have"?
3. Does the University hold the information in another digital service that can be referenced instead of re-collecting it?
4. Is it possible to de-identify personal data or assign a pseudonym so that it can no longer be attributed to a specific person?

Consider specific risks to individuals, such as the potential re-identification of pseudonymised data, identity theft or fraud, reputational damage, loss of confidentiality or financial loss.

Based on the nature of the project and the University's handling of personal information, consider the likelihood and severity of the risks identified.

Consider the following actions or options to resolve privacy risks:

1. Is it possible to not collect certain types of data?
2. Can you reduce the retention periods for some personal information?
3. Can data be anonymised or pseudonymised?
4. Can additional security measures (both technical, such as access control mechanisms and encryption, as well as physical, such as lockable storage and limited access to certain areas) be adopted?
5. Are clear data sharing arrangements in place?
6. Can you offer individuals the chance to opt in or opt out, where appropriate?
7. Have you trained staff on the project team to ensure risks are anticipated and managed?
8. Have you prepared internal guidance and processes to avoid risks?

Note that the above list is not exhaustive. The measures which can be taken to mitigate privacy risks will depend on the undertaking. Where there are multiple options to address a privacy risk, you should evaluate the likely costs, risks and benefits of each option to identify which is the most appropriate.

## Step 6 - Formulate and Consult on Draft Recommendations

You must prepare draft recommendations that include an action plan and timeline. These recommendations must identify how privacy protection measures can be enhanced and how negative privacy impacts or risks can be avoided or reduced. The recommendations may address, for example:

1. changes to the project or process that would achieve a more appropriate balance between the proposed undertaking's goals and the protection of personal and/or health information
2. privacy management strategies that will reduce or mitigate privacy risks
3. the need for further stakeholder consultation
4. whether the privacy impacts are so significant that the proposed undertaking needs considerable re-design or even its feasibility examined
5. the creation of privacy documentation or amendment of existing agency privacy management plans, and
6. issues beyond project or process specific matters to overall privacy risk management for the University.

Before the proposed recommendations are finalised, discuss them with affected stakeholders to ensure their views are incorporated and to secure their commitment to the recommended actions.

## Step 7 - Prepare Report

The PIA report should set out all the information gathered throughout the PIA process. An example template PIA report is available from the Privacy website.

Key elements of the PIA report include:

1. Introduction and background information, including the context of the proposed undertaking
2. Description of the proposed undertaking
3. Who was responsible for the PIA and the approach taken
4. A description of the information flows
5. Results of stakeholder consultation
6. Outcome of risk assessment and compliance check, including privacy risks that have been identified, options considered to mitigate risk, why particular options or alternatives were rejected or discounted and why a particular course of action has been recommended, and
7. Description of privacy risks that cannot be mitigated, the likely response to these risks, and whether they are outweighed by the proposed undertakings' benefits to the University, staff and students

Consider and adopt a position on the recommendations in the PIA report, identifying whether you will adopt, partially adopt or not adopt any of the recommendations made. You must provide reasons for not adopting recommendations.

The Final PIA must be approved by the Executive Sponsor of the proposed undertaking.

## Step 8 - Access to PIA Reports

The University may release a summarised or edited version of a PIA report in limited circumstances upon request, but on the condition that this does not prejudice confidentiality of personal information including security measures. You must consult with the Privacy Officer in the first instance if you receive a request to access a PIA.

## Step 9 - Review and Update the PIA

Consider whether an external review of a PIA by an independent third party should be undertaken as this can ensure that the PIA has been carried out properly and that the recommendations have been implemented.

Many projects and processes undergo changes before their completion. If the changes are substantial and result in significant new privacy impacts that were not considered in the original PIA, it may be necessary to undertake a new PIA.

privacy@westernsydney.edu.au
May 2023