MACQUARIE University

Privacy Impact Assessment Guidance Note

Governance and Compliance Services

What is a Privacy Impact Assessment?

A Privacy Impact Assessment (PIA) is a process for analysing a program's impact on individuals' information and privacy. The process of conducting a PIA can help to identify potential privacy risks and develop risk mitigation strategies to address these privacy impacts before a project or initiative commences.

Why perform a PIA?

PIAs are recommended to assist with ensuring that projects are compliant with privacy laws. PIAs also demonstrate a 'privacy by design' approach, ensuring that privacy risks and potential issues are considered early.

When to conduct the PIA

It is recommended that a PIA is conducted as early as possible. It should be undertaken early enough in the development of the project that it is still possible to influence the project design and ensure that privacy is considered throughout the planning process.

A PIA should be treated as a living document, which is updated throughout the course of the program to reflect any risks that may emerge as the project evolves. This is particularly important if the program is long running, has different phases, there is new or changing legislation or there are material changes to the project. Material changes can include changes to the nature or volume of personal information elements or implementation of a new system.

Who should conduct the PIA?

A PIA should be completed by the individual who is best placed to assess the risk for a particular program. Generally, whoever is managing the project will be responsible for ensuring the PIA is conducted. It is recommended that you consult with the Privacy Officer who can assist with identifying privacy risks and provide guidance on privacy legislation.

Is a PIA necessary?

It is advised that a threshold assessment is conducted to determine whether a PIA is necessary.

The simplest threshold assessment is: Does the program or initiative involve the handling of personal information?

If yes, consider conducting a PIA.

Other factors to consider when conducting a threshold assessment:

- the nature, size and complexity of the program;
- large scale use of sensitive data or personal information;
- the integrating of multiple databases;
- engaging third parties to handle the personal information held by the University;
- disclosing personal information overseas; and/or
- use of innovative technology, including Artificial Intelligence (AI).

Document the outcome of your threshold assessment. This record could include:

- a brief project description;
- whether the project involves personal/health information;

- a brief description of the personal and/or health information involved, including the nature and sensitivity of the information and the general purposes for which information will be collected, used and/or disclosed;
- why this information is needed;
- storage and security of the information;
- access to and amendment of the information;
- the views of relevant stakeholders about the potential impacts of the project on privacy;
- whether a PIA is recommended or not; and
- details of the person or team responsible for the threshold assessment.

Liaise with the Privacy Officer regarding the conclusion of the threshold assessment.

If a PIA has been recommended, perform the PIA in line with the following.

Plan the PIA

Planning should consider:

- how detailed the PIA needs to be, based on scope;
- who will conduct the PIA and assign responsibilities and actions;
- the timeframe for the PIA;
- planning for implementation of recommendations from the PIA and ongoing monitoring; and
- whether internal consultation is required. Other areas that may be impacted, such as records management, human resources, information technology, legal and policy.

Conduct the PIA

Complete the template to conduct the PIA. Relevant sections include:

- mapping information flows;
- identifying privacy risks and possible remedial actions;
- details of stakeholder consultation;
- formulating recommendations, including actions required, timeframes and responsible persons; and
- establishing how often the PIA will be reviewed.

Internal PIA Register

Completed PIAs should be provided to the Privacy Officer who maintains an internal PIA register.

MACQUARIE
University

[Insert organisations name]

Privacy Impact Assessment

[Insert program name]

Executive Summary

Describe in brief:

- The purpose of the PIA
- Brief project description and key information flows
- A summary of findings
- A summary of recommended actions

PIA methodology

Outline the approach taken, that is:

- who was responsible for the PIA
- who conducted the PIA (their skills and expertise)
- key steps taken to complete the PIA

Program			
Organisation			
PIA Drafter		Email	
Program Manager		Email	
Privacy Officer		Email	
Date Completed			

Part 1 – Program background and details

Description of the program and parties

This section should include:

- any relevant background and what it will achieve;
- why the project is needed;
- any links with existing projects;
- who is responsible for the project;
- timeframes;
- whether the project will use innovative technology, such as AI; and
- how personal and health information will be handled in the project, from beginning to end, explaining:
    - what information will be collected
      Does the project involve personal information? Does the program involve other information that has the potential to identify individuals? Does the program involve sensitive or health information? Is all the personal information collected necessary for the project?
    - how it will be collected
      Describe the means by which the information is collected.
      Is the personal information collected directly from the individual? Will the individual be notified about the collection of their personal information? Will any personal information be collected indirectly from another source? Will the individual be notified that their personal information has been collected from another source? Will any personal information be de-identified as part of the project? What will be done to ensure the ongoing accuracy, completeness and currency of the personal information?
    - how it will be stored
      List the policies, procedures or controls that the University implements to protect personal information. Explain how these measures will be implemented for this project.
      Describe the format in which the personal information will be stored (e.g. electronic, hard copy etc.) and where it will be stored (e.g. internally, external provider, cloud, third party platform etc.)
      How long will the personal information be kept for? (any relevant retention and disposal policies)
      How will personal information be destroyed once it is no longer required? Or as an alternative, will any personal information be de-identified once it is no longer required?
    - who will have access to it
      Describe the positions that will have access, how access is gained or controlled, and whether it is logged.
    - what it will be used for
      Describe what personal information will be used or disclosed, and for what purposes.

- any third parties to whom it will be routinely or otherwise disclosed
  Describe what information will be shared, with whom the information will be shared, the frequency of the disclosure, how the information will be shared and how the disclosure is authorised by the PPIP/HRIPA or other relevant legislation. Describe what information will be transferred outside of NSW, the jurisdiction the information will be stored, and how the information will be transferred.

- Other considerations
  Identify the avenues available for individuals to request access to or correction of their personal information, and who is responsible for handling such requests.
  Who can individuals complain to if they have concerns about the handling of their personal information?
  At a high level, describe the steps that the University will take in the event of a data breach.

Information flow diagram

Delete this text and the text below and insert an information flow diagram.

Insert here or attach as an appendix a diagram or table that shows the flow of information involved in the program. This should indicate the systems used, the parties involved (if applicable), and the methods of transfer. Where possible, indicate the types of information that flow, between the various stages or parts of the program, and between different parties.

Stakeholder consultation

This section should include:

- an outline of any internal and external stakeholder consultation that has been undertaken in relation to the program; and
- where relevant, a summary of the outcomes of any consultation.

Part 2 – Analysis of privacy issues

Some examples of privacy risks:

- *Consider the risk of unauthorised/unlawful collection of personal information.*
- *Consider whether there is a risk of overcollection of personal information.*
- *Consider whether the method of collection is fair and not unreasonably intrusive.*
- *If personal information is indirectly collected, consider whether there is a risk of the information being inaccurate, out of date or incomplete. Consider the impact on individuals if they are not made aware that their information is being collected from another source.*
- *If there are inadequate or no security measures in place, consider whether there is a risk that the information will not be properly protected, leading to loss, misuse, or unauthorised access, modification or disclosure.*
- *If personal information is de-identified, consider whether there is a risk that the information can be re-identified. For example, de-identified information may be re-identifiable when matched to other information, or because of the way the de-identified information is used in the context of this program.*
- *If de-identifying personal information once it is no longer required, consider whether there is a risk that the information can be re-identified.*
- *Consider the risk of the information being held or retained longer than necessary or required.*

	Description of risk	*Consequence rating*	*Likelihood rating*	*Inherent risk rating**	*Accept*	*Risk management strategy*	*Residual consequence rating*	*Residual likelihood rating*	*Residual risk rating*	*Owner*
1	'The risk of… event … caused by … how … resulting in … impact(s) …'	What is the impact of the risk?	What is the likelihood of the risk occurring?	What is the overall risk rating on?	Is the risk accepted or not?	Detail the measures taken (or to be taken) to mitigate and manage the risk. Where relevant, include the timeframe for implementing the strategy and identify who is responsible for it.	What is the impact of the risk after security measures have been applied?	What is the likelihood of the risk occurring after security measures have been applied?	What is the overall risk rating after security measures have been applied?	Who is responsible for monitoring and reviewing the risk?

**Add more rows by clicking in the bottom right cell and pressing 'tab'

*Use Attachment A to determine inherent and residual risk rating.

Part 3 – Action items, endorsement, document information

This part details any action items identified, endorsement of the PIA, and document information.

Action items

Action items identified in Part 2 are listed here, along with the owner of the action and any timeframe within which the action needs to be completed.

	Action	*Owner*	*Timeframe*	*Completed*
1				
2				

**Add more rows by clicking in the bottom right cell and pressing 'tab'

Endorsement

The required endorsements for this PIA are listed below. This may include the program manager, a privacy officer, executive business owner, or any other responsible person.

Name	*Position*	*Signature*	*Date*

**Add more rows by clicking in the bottom right cell and pressing 'tab'

Document information

Document title	
Document location	
Document owner	
Document distribution	
Related documents	
Next review	
Document version	

Attachment A

To remove as required

Risk Assessment Matrix Sep 2022		CONSEQUENCE RATING				
		Minimal	Minor	Moderate	Major	Severe
LIKELIHOOD RATING	**Almost certain** *Over 90% probability; or expected to occur in most circumstances; or expected to occur multiple times throughout a project*	(11) MEDIUM	(16) HIGH	(20) HIGH	(23) VERY HIGH	(25) VERY HIGH
	Likely *Between 51-90% probability; or probable to occur in most circumstances; or likely to occur in a project, has occurred in similar projects*	(7) MEDIUM	(12) MEDIUM	(17) HIGH	(21) HIGH	(24) VERY HIGH
	Possible *Between 21-50% probability; or might occur, has occurred before; or has occurred in a minority of similar projects*	(4) LOW	(8) MEDIUM	(13) MEDIUM	(18) HIGH	(22) VERY HIGH
	Unlikely *Between 1-20% probability; or could occur; has not occurred before in similar projects, but could*	(2) LOW	(5) MEDIUM	(9) MEDIUM	(14) MEDIUM	(19) HIGH
	Rare *Less than 1% probability; or very unlikely to occur, even in the longer term; or a '100 year event'*	(1) LOW	(3) LOW	(6) MEDIUM	(10) MEDIUM	(15) HIGH

Level of Risk Rating		
Rating	**Escalation and Action required**	**Escalation and Action required for Research specifically**
LOW (1-4)	Manage by routine procedures; Monitor trends	Consideration that the University can engage in the Activity or Arrangement without modifications and risk management strategies are undertaken.
MEDIUM (5-14)	Specify management accountability and responsibility; Monitor trends and plan for improvement	Consideration that the University may only engage in the Activity or Arrangement if certain modifications and risk management strategies are undertaken. List modifications and risk management strategies.
HIGH (15-21)	Escalate to senior management; Implement a detailed action plan to reduce risk rating	Consideration that the University should NOT engage in the Activity or Arrangement UNLESS significant modifications and risk management strategies are undertaken. List modifications and risk management strategies. Follow up that modifications and risk management strategies implemented.
VERY HIGH (22-25)	Escalate to Executive Group; Implement a detailed action plan to reduce risk rating	Consideration that University should NOT engage in the Activity or Arrangement due to the impact of the risk on the University. Cease associated activity.

MQ Risk Matrix – Consequence Criteria Sep 2022	CONSEQUENCE RATING				
	Minimal	Minor	Moderate	Major	Severe
Risk Category – Reputation	Student disaffected; Authority notes concern	Authorities formally seek clarification; Student Groups register separate concerns; MQ student body media traffic; Localised social media traffic	Authorities and Government register strong concerns and threaten investigation; State based media; Social media traffic (mainly spurious); Multiple Student Groups vocalise concerns; Prominent Academic resigns	Targeted enquiry and investigation by Authorities / Gov; Aust Wide press interest; Short term spike in adverse social media traffic; Widespread disaffected Student Community; Faculty Dean or DVC resign; Loss of standing within the Research Funding Community	Total loss of confidence by Government/Student Community/Authorities/Funding & Research Bodies; International media attention; Wide-spread prolonged adverse social media traffic; VC and Key Executives resign
Risk Category – Academic Matters	Minor course development or introduced postponed	Course development or introduced delayed	Loss of external accreditation of course; Load sharing to support signature courses and or research; Research projects not progressed; New courses not developed or introduced; Ability to seek new research opportunities are limited	Suspension of/conditional Provider Status; Partial closure of Dept; Suspension of viable/signature course; Material breach of Research grants / conditions; Limitations on research opportunities	Closure of a viable or signature course; Planned research activity and growth not viable; Closure of Dept; Loss of Provider Status; LT union action; Inability to staff Dept
Risk Category – Legal and Compliance	Technical non-compliance	Regulator enquiry; Minor legal issues and, or breach of regulation	Regulator issues warning; Fine and legal costs up to $15M; Major litigation; Class Action;	Regulatory sanction resulting in suspension of license and or conditions on accreditation; Fine and legal costs up to $50M; Major litigation; Class Action	Regulatory sanction resulting in loss of license / accreditation; Fine and legal costs exceeding $50M; Major litigation; Class Action
Risk Category – Financial	Loss/gain able to be absorbed in the current budget; Cash loss of <$5M (or <0.5% of revenue budget)	Loss/gain able to be absorbed in the current budget in year by reprioritising to current year initiatives; Cash loss of $5M-10M (or 0.5% - 1% of revenue budget)	Non-major initiatives are reallocated to the following financial year; Cash loss of $10-20M (or 1% - 2% of revenue budget)	Loss/gain is not able to be absorbed in current year budget or provisions; funds are diverted to support critical activities only; Cash loss of $20-50M (or 2% - 5% of revenue budget)	Loss/gain cannot be funded in the current environment; Cash loss of >$50M (or >5% of revenue budget)
Risk Category – Workplace Health and Safety	Injury not requiring first aid or can be self-managed	First aid incident not resulting in medical treatment	Medical treatment without hospital admission	Hospitalisation and ongoing or longer-term treatment	Death or permanent disability to one or more persons
Risk Category – Environmental	Minor reversible impact to low significance environmental location	Short term reversible impact on environment	Significant localized impact to environment	Long term damage to the environment	Permanent damage to the environment
Risk Category – Infrastructure	Teaching facilities are unable to be occupied at the allocated time; Small no of users impacted by IT systems being temporarily unavailable	Parts of a building within the Uni is unable to be occupied for prolonged period (greater than 1mth during teaching semester); IT Systems do not operate efficiently eroding performance	One building within the Uni is unable to be occupied for prolonged period (greater than 1mth during teaching semester); IT Systems do not operate efficiently eroding performance	More than one building within the Uni are unable to be occupied for prolonged period (greater than 1mth during teaching semester); Temporary loss of one or more Faculty / Dept data; Critical IT Systems unable to be recovered to support operations for up to 1mth	More than one building within the Uni are unable to be occupied for prolonged period (greater than 1mth during teaching semester); Temporary loss of one or more Faculty / Dept data; Critical IT Systems unable to be recovered to support operations for up to 1mth
Risk Category – Research	Research activities or outputs will not result in harm to people, animals or the environment; or to Australia's national security [Unclassified and non-critical technology research].	Research activities or outputs have the potential to result in limited harm to people, animals or the environment; or to Australia's national security [Unclassified and non-critical technology research].	Research activities or outputs result in limited harm to people, animals or the environment; or to Australia's national security [Sensitive information or critical technology research].	Research activities or outputs result in some harm to people, animals or the environment; or to Australia's national security [Classified information or large quantities of sensitive information, or critical technology research with national security impact rating of high].	Research activities or outputs result in significant harm to people, animals or the environment; or to Australia's national security [Highly classified information or large quantities of classified information, or intentional/reckless/negligent critical technology research with national security impact rating of high].

MQ Risk Assessment Matrix and Criteria