# Privacy Impact Assessment Guidelines

## 1. Purpose

The purpose of these Guidelines is to assist Staff Members undertake a Privacy Impact Assessment (PIA). Under the Privacy Policy, Staff Members must undertake a PIA when creating or changing a process or system that involves a new or changed collection, use or disclosure of Personal Information or that may impact the security or integrity of Personal Information already held by the University.

## 2. Application

Privacy is everyone's responsibility. These Guidelines apply to all Staff Members who may manage projects or systems that impact on Personal Information or who are responsible for making policy decisions about the way the University manages Personal Information.

## Guidelines

## 3. Privacy Impact Assessments

3.1 A Privacy Impact Assessment (PIA) should be considered whenever the University is making a change (large or small) to its systems or processes that:

(a) involves (or may involve) a new or changed collection of Personal Information;

*For example, the collection of category of Personal Information that is not listed in the Privacy Notice or a change to the way in which Personal Information is collected*

(b) involves (or may involve) the use or disclosure of Personal Information for a new purpose or to a new organisation; or

*For example, using Personal Information for a purpose not listed in the Privacy Notice or disclosing to an organisation not listed in the Privacy Notice. Other examples include, but are not limited to, outsourcing storage of Personal Information, uploading Personal Information to the cloud.*

(c) could be contrary to the expectations of, or could come as a surprise to, the Individuals whose Personal Information is affected; or

*Note: Ask yourself – if it was my Personal Information, would I be surprised to hear what was being done with it? If yes, then you should do a PIA*

(d) involves (or may involve) the use of a new or intrusive technology; or

*For example, the use of surveillance, profiling or automated decision making technology*

(e) results in the merger of existing databases or the creation of new databases; or

*For example, changing organisational processes to use Personal Information in different ways, moving from paper-based to electronic forms, major IT projects that impact on Personal Information*

(f) alters the storage or security of Personal Information.

For the purposes of these Guidelines, any of these is referred to as an "Initiative".

*Note: An individual research project is not considered an "Initiative" for the purposes of these guidelines. Staff Members should contact the Research Office for assistance.*

## 4. Who is responsible for a PIA?

4.1 Responsibility for assessing the need for a PIA and ensuring one is completed where appropriate depends on whether or not the Initiative being considered is connected to a project being undertaken by the University.

(a) Where the Initiative is connected to a project, the relevant project manager is responsible.

(b) Where the Initiative is not connected to a project, the relevant manager initiating or leading the Initiative is responsible.

*Note: For the purposes of these Guidelines, this person is referred to as the "Responsible Manager"*

4.2 The Responsible Manager should ensure that the PIA takes place early in the process to ensure that privacy is embedded in the design of the Initiative.

4.3 The Responsible Manager will need to obtain and coordinate input from project staff, privacy experts, information security experts and the project sponsor in order to complete the PIA

4.4 Where a PIA identifies an Initiative as being particularly high risk, the Responsible Manager should consult with the Privacy Officer.

## 5. When is a PIA required?

5.1 Responsible Managers should work through the following questions to identify whether a PIA is required for a particular Initiative.

1. Does the Initiative involve or alter the collection, storage, use or disclosure of Personal Information? If not, no PIA is required. If yes, move to Q2

   *Note – see the examples in clause 3.1 above. See also the definition of Personal Information in this Guideline*

2. Is the collection, storage, use or disclosure of Personal Information covered by the University's Privacy Notice? If yes, no PIA is required. If not, move to Q3

   *Note – for example, will the Change involve the collection of new personal information that is not listed in the Privacy Notice; will existing personal information be used for a purpose not listed in the Privacy Notice; will existing personal information be disclosed to parties not listed in the Privacy Notice*

3. Is the Personal Information involved sensitive? If it is, then a PIA is required. If not, move to Q4

   *Note – for example, is the information particularly likely to raise privacy expectations or concerns? 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.*

4 Would the Initiative be contrary to the expectations of Individuals or put a significant amount of Personal Information at risk? If not, no PIA is required (although you should contact the Privacy Officer to ascertain whether changes to the Privacy Notice may be required). If yes, a PIA is required

   *Note – for example, will the Change involve the use of new or intrusive technology (such as technology that uses location information, profiling or automated decision making); will existing databases be merged or new databases created; or would the change come as a surprise to the Individuals affected by it?*

## 6. How is a PIA completed?

6.1 Responsible Managers should work through the following steps and use the PIA Template to complete a PIA that covers all the key issues.

| What? | How? | Who? |
|---|---|---|
| What's the Initiative? | Describe the Initiative, its purposes and its desired outcomes.<br>*This will help you understand what objectives might compete with your privacy obligations.* | Responsible Manager |
| What Personal Information is being collected, used or disclosed? Why is that necessary? | Describe the personal information involved, how it will be used or disclosed.<br>*This will help you to identify the risks created by the* Initiative *and consider whether the collection, use and disclosure of personal information is necessary and proportionate.* | Responsible Manager |
| Does the initiative raise any privacy risks? | Work through the PIA Template, and answer questions honestly and accurately.<br>*This will help you create solutions that ensure compliance with the Privacy Policy and the Privacy Act.* | Responsible Manager |
| What ways can these risks be addressed? | Consider ways to lessen or eliminate these risks. If possible, try to accommodate privacy while delivering the desired outcomes. Add your solutions to the comments section in the PIA Template<br>*This will help you to ensure that the initiative is a success, but not at the expense of individual privacy.* | Responsible Manager |
| If privacy risks were identified, now share with the Privacy Officer | | |
| If the initiative raised privacy risks, have these been addressed? | The Privacy Officer will review the PIA and provide advice on addressing any privacy risks identified. | Privacy Officer |
| Now share with the Project Sponsor for sign off | | |
| Sign off PIA | The PIA should be reviewed and signed off by the Project Sponsor or Relevant Manager.<br>*This ensures oversight and accountability by those responsible for privacy compliance and project governance.* | Project Sponsor |
| Incorporate PIA outcomes into initiative | Ensure that the solutions are incorporated into the design of the initiative and are actioned.<br>*This reduces the risk of the PIA being treated as a "tick the box" exercise.* | Responsible Manager |

## Definitions

In these Guidelines, unless the context otherwise requires:

| | |
|---|---|
| Individual: | any person about whom the University collects and holds personal information and includes students, Staff Members, contractors, alumni, donors, and visitors to the University's websites or campuses<br>*Note: The term "Individual" comes from the Privacy Act 2020 and is synonymous with the global term "Data Subject". The University's Privacy Framework uses "Individual" rather than "Data Subject" for plain language purposes* |
| Initiative | has the meaning in clause 3.1 of these Guidelines |

| | |
|---|---|
| Personal Information | any information, whether electronic or hard copy, about an Individual whether or not the information directly identifies the Individual. Personal Information includes, but is not limited to, contact, demographic, health and academic information (including grades), CCTV footage, staff HR and performance information, emails and other correspondence, and opinions about the Individual |
| PIA | Privacy Impact Assessment |
| PIA Template | the PIA template published by the University |
| Privacy Notice | the privacy notice published by the University that describes how the University collects, uses, and shares Personal Information. |
| Responsible Manager | the manager responsible for completing a PIA as determined under clause 4.1 of these Guidelines. |
| Staff Member | an employee of the University |
| University | Victoria University of Wellington |

## Related Documents and Information

### 7. Related Documents

Education and Training Act 2020
Health Information Privacy Code 2020
Information Security Policy
Privacy Act 2020
Privacy Policy
Privacy Notice
PIA Template
Victoria University of Wellington Act 1961

### 8. Document Management and Control

| | |
|---|---|
| Approver | Chief Operating Officer |
| Approval Date | 8 December 2020 |
| Effective Date | 8 December 2020 |
| Last Modified | N/A |
| Review Date | 1 December 2023 |
| Sponsor | Chief Operating Officer |
| Policy Owner | General Counsel & Privacy Officer |