PRIVACY IMPACT ASSESSMENT PROCEDURE

PURPOSE

This procedure provides a systematic approach to identify and manage the privacy risks associated with a new, or a change to a project, system or process ('project') to ensure compliance with privacy legislation and other associated legal obligations.

SCOPE

This procedure applies to all staff and associates of the University ('us', 'our' or 'we').

This includes staff, contractors, agents, official visitors and other individuals performing services/work for and on behalf of the University or who are engaged in activities reasonably connected with the University and hereinafter referred to as 'you'.

For the purpose of this procedure, the use of 'personal information' also includes sensitive and health information.

PROCEDURE STATEMENT

1. Privacy Impact Assessments

1.1 A Privacy Impact Assessment (PIA) will help you to identify privacy risks and determine appropriate risk mitigation strategies for any project, system or process (collectively referred to as 'project') which collects, uses, discloses or stores personal, sensitive or health information. This also assists us to ensure that any handling of personal information aligns with our privacy obligations and any privacy risks are appropriately considered and managed.

1.2 Other risks may also arise that do not relate directly to the Information and Health Privacy Principles. For instance, community expectations of how we should use personal information is an important consideration. Even where an act or practice does not contravene the IPPs or HPPs, individuals may be uncomfortable with the use of their information for particular purposes and we should be sensitive to such concerns.

1.3 For a summary of the Information Privacy Principles and the Health Privacy Principles visit these links.

1.4 The objective of a PIA is to review privacy impacts and to embed privacy enhancing approaches to all projects, which handle personal and health information.

1.5 Privacy issues that are not properly addressed can impact on the community's trust in the University and undermine the success of the project.

1.6 A PIA should be undertaken when there is a change to an existing project, or a new project is introduced, that involves a change in current practices for the collection, use, disclosure or storage of personal or health information. A PIA will:

- ensure legal obligations are met to protect the privacy of an individual in respect of any personal information we collect, store, use and disclose;
- support good governance and informed decision making;
- mitigate privacy risks; and
- consider non-legal risks related to the project such as, but not limited to, individuals being uncomfortable with the use of their personal information for particular purposes that we should be sensitive to.

1.7 Definitions of Personal, Sensitive and Health Information are available here.

When a PIA is required

1.8 PIAs should be an integral part of your project planning, not an afterthought. You should undertake this early on in order to influence the project design or, if there are significant negative privacy impacts, reconsider proceeding with the project.

1.9 A PIA should be completed:

- prior to the start of implementing any new process which handles personal and/or health information; or
- when developing or prior to making changes to a process which handles personal and/or health information; or
- prior to using or implementing a system or service (including external vendor application/s, external hosting of information, etc.) which handles personal and/or health information; and
- whenever there is a change to a process that may impact information privacy.

2. Completing a PIA

2.1 To commence a privacy impact assessment, the privacy impact assessment template must be used.

2.2 Should you require assistance to complete a PIA, please refer to the University Privacy website for contact details of approved external service providers who can assist you on a fee for service basis.

Stage 1 – Threshold Assessment (complete parts 1 & 2 of PIA)

2.3 Parts 1 and 2 of the form enable the project to be screened and threshold tests applied in order to determine if the handling of personal information is involved. If any personal information is involved in the project then the completion of a PIA is required.

2.4 If personal information is identified as a part of the project, a full PIA must be completed.

Stage 2 – Risk Assessment and Mitigation (complete parts 3-6 of PIA)

2.5 Parts 3 to 6 conducts an in-depth assessment of privacy risks and liabilities. They analyse privacy risks, and offer solutions to accept, mitigate or avoid the privacy risks thus allowing us to make informed decisions about the handling and management of personal information.

2.6 You may elect to complete parts 3–6 of the PIA yourself or alternately, you may elect to use the services of one of the approved external service providers. This will assist in the identification of potential privacy risks and impacts and identify appropriate risk minimisation strategies for the project.

2.7 If you complete Part 3-6 yourself, you must submit the complete PIA to one of the external service providers for assessment

Stage 3 – Adoption of risk mitigation strategies and declarations (Project Manager)

2.8 The project manager is responsible for reviewing the advice from the external service provider and to take measures to ensure appropriate risk mitigation strategies are put in place and privacy advice implemented.

2.9 Subject to Stage 4, the project manager may determine which recommendations will not be adopted and under what circumstances and is responsible for accepting and managing, the associated risk.

Stage 4 – Approval Process

2.10 The project must be externally reviewed for privacy compliance. The external service provider will advise of any issues in the assessment that need further consideration prior to proceeding to the approval process and will rate the assessment according to the Privacy Risk Matrix.

2.11 The following table outlines the required approval levels based on the assessment according to the Privacy Risk Matrix

Risk rating	Recommendations accepted	Recommendations not accepted
Low	Proceed	To proceed, Project Manager approval is required
Low to medium	Proceed	To proceed, Project Manager approval is required
Medium	Proceed	To proceed, Project Manager's Head of Department or Head of Unit approval is required
Medium to high	Proceed	To proceed, Senior Management approval is required
High	Proceed	To proceed, Senior Management approval is required

2.12 Senior Management approval means the project manager and:

- for Divisions, the Divisional Director
- for faculties, the Faculty Dean
- for non-faculty operations, the Chief Operating Officer
- for non-faculty academic/research, the Provost

2.13 Options relating to risk assessment outcomes according to the Privacy Risk Matrix include (but are not limited to):

- Low to medium risk – proceed (make minor adjustments);
- Medium risk – proceed providing recommendations and adjustments are made with option to resubmit for further assessment;
- Medium to High risk – implement all privacy and security recommendations;
- Medium to High risk – cancel project or approve to proceed after implementing risk mitigation recommendations.

2.14 For high-risk projects to continue, both the project manager and senior management must approve the PIA prior to implementation. When senior management approve a PIA post assessment, they are also accepting and managing any associated privacy risks.

2.15 You must forward a copy of the final PIA if any variations are identified post Stage 4 to the Privacy Officer.

3. Key Approvals and Responsibilities

3.1 The project manager is responsible for completing a PIA.

3.2 The project manager is responsible to mitigate associated privacy risks associated with the project.

3.3 When Senior Management approves a PIA post assessment, they are also accepting and managing any associated privacy risks.

DEFINITIONS

Key definitions	Refer to Privacy Key Definitions

ADMINISTRATION

Parent policy	Integrity and respect
Supporting policies	• Employment conditions • Ethics Statement • Equal opportunity • Leave and wellbeing • Pay, benefits and entitlements • Probation, performance and promotion • Recruitment and appointment
Supporting procedures	Privacy
Supporting documents	• Collection of personal information • Freedom of Information at Monash University • Health privacy principles • Information privacy principles • Key privacy definitions • Privacy at Monash • Privacy Impact Assessment Template • Privacy Incident Notification Guideline • Privacy Risk Matrix • Records and Archives Services at Monash University
Legislation mandating compliance	
Responsibility for implementation	
Approval body	Chief Human Resources Officer
Procedure owner	Director Workplace Relations
Date effective	20 March 2018
Review date	3 years from effective date

Category	Human Resources
Version number	1
Content enquiries	ask.monash or phone Monash HR on (03) 990 20400