## Privacy Impact Assessment

This Privacy Impact Assessment (PIA) template can be used to assess the privacy implications of any new or updated projects, systems or processes which may impact the privacy of individual students or staff. This can include but is not limited to; new or amended policy, processes, programs, systems or databases, new methods or delivery of services or information handling and changes to the way information is stored. The PIA aims to identify and recommend solutions to manage, minimise or eliminate the privacy risks and is designed to evaluate compliance with the Australian Privacy Principles and the [Privacy Act 1988](https://www.legislation.gov.au/Series/C2004A03712) (CTH), the Information Protection principles and the [*Privacy and Personal Information Protection Act 1998* (NSW)](https://www.ipc.nsw.gov.au/node/83) and the [Health Privacy Principles](https://www.ipc.nsw.gov.au/health-privacy-principles-hpps-explained-members-public) and [Health Records and Information Privacy Act NSW, 2002](https://www.legislation.nsw.gov.au/#/view/act/2002/71) (HRIPA). It is also designed to ensure UNE operates in a way that promotes privacy principles as essential to everyday operations and enhances the information available to us. We aim to build a culture that values and promotes privacy not just as a means of compliance but in keeping with community and ethical considerations.

You can find additional information in the [Information and Privacy Commission NSW’s Guide to PIA](https://www.ipc.nsw.gov.au/sites/default/files/file_manager/2016.12.13_Privacy_Impact_Assessment_Guide.pdf) or engage in an [online training module](https://www.oaic.gov.au/privacy/guidance-and-advice/guide-to-undertaking-privacy-impact-assessments/#s4-identify-and-consult-with-stakeholders) delivered by the Office of the Australian Information Commissioner. This PIA builds on literature from both organisations.

The PIA should be completed by a senior member of the project team or business unit, with input from all team members and key stakeholders. The UNE Privacy Officer is available to answer questions and assist with this process by contacting privacy@une.edu.au. Once completed and endorsed by the project manager and after consultation with the Privacy Officer the PIA should be added to the Project container in the UNE Records Management system and forwarded to privacy@une.edu.au.

The PIA process is iterative and works best when it evolves and becomes a part of the project ensuring privacy is considered throughout the planning stages and updated to take account of any changes to the project or system as it evolves. The PIA is completed in these steps:

1. **Describe** the personal information \* flows included in the project, system, process or activity. What is collected, where and how will it be used, where and how will it be stored?

**2. Analyse** the possible privacy impacts of the information flows. Who has access? What kinds of information are collected? Is the information sensitive?

**3. Assess** the impact of the project as a whole on the privacy on individuals. What are the benefits or negative impacts on privacy on individuals? If the information was breached what are the consequences to an individual?

**4. Explain** how those impacts will be eliminated or minimised. Is it necessary for the reasonable operation of this project to collect the personal information identified? Could this be minimised.

**5. Build** privacy considerations into the design of the project.

**6. Achieve** a privacy compliance action plan to ensure ongoing compliance with our privacy obligations.

 \*Personal information has the meaning given to it in accordance with Section 4 of the Privacy and Personal Information Protection Act 1998 (NSW) and includes any information that identifies or can reasonably identify an individual (e.g. name, address, images, photographs or other information which identifies a person, fingerprints, blood or DNA samples). Sensitive information is a specific type of personal information and includes information or an opinion about a person’s: racial or ethnic origin; political opinion; membership of a political association; religious beliefs or affiliations; philosophical beliefs; membership of a professional or trade association; membership of a trade union; sexual preference or practices; criminal record. Sensitive information does not have to be proven to be true. Health information under HRIPA is personal information that is information or an opinion about: the physical or mental health or a disability (at any time) of an individual, or an individual’s express wishes about the future provision of health services to him or her, or a health service provided, or to be provided, to an individual, or information about body donation.

# Part 1 – Description

|  |
| --- |
| 1.1 PROJECT/ACTIVITY DETAILS |
| Name of Project/Activity:  |
| Manager conducting PIA ( this can be the lead individual as part of a team approach) :  |
| Faculty/Business Unit /Area: Date:  |
| Work Email: Phone:  |
| Project Manager/ Immediate Supervisor:  |

.

|  |
| --- |
| 1.2 DESCRIPTION OF PROJECT/ACTIVITY |
| Provide a description of the project, system, process or activity, including the following information: • Purpose of the project/activity, what it hopes to achieve and why, how this fits within UNE’s objectives;• The nature and sensitivity of the personal information (list all PI fields);• Any links with existing programs/processes or other projects;• If an existing project, is the way that personal information is handled changing?• If information handling remains the same in an existing project explain how privacy implications have been assessed and managed. • Any expected benefits any perceived issues;• Timeframe for decision making;• Any other projects, systems or processes it is part of, related to or will impact;• Key stakeholders (e.g. including internal business units, external stakeholders and students) and their respective roles and responsibilities. |
|  |
| 1.3 INFORMATION DETAILS |
| Please describe in as much detail as possible the kinds of information which will be collected or implicated in the proposed project, system, process or activity. Please include:• Types of information collected or used by the project• Any instances where personal information, will be collected including any details which may identify an individual or any sensitive information , unique identifiers (including student numbers), health information and re-identifiable information• How each element will be collected, used, disclosed and stored, and by whom. Please include details of any third parties. • Any transfer of personal information to a location outside of NSW, this includes being held on a server or database outside NSW by a third party provider. • Will new information technologies be used for handling the information or a new method of handling or disclosing the information?• Will the personal information be used for data matching or aggregated into databases?• Is the collection of the information compulsory?• If the student/staff member/ participant does not agree to the data collection can they still access the service provided in any form? |
|  |

# Part 2 – Privacy Analysis

After describing the detail of the project or process, it will have been determined personal whether information is involved. The following section will assist in assessing the project/activity against the Information Protection Principles (IPP’s) which govern the collection, access, use, disclosure, and management of an individual’s information. In this section, ‘information’ collectively refers to all personal, sensitive and/or health information in this project/activity, including unique identifiers and re-identifiable information. If you are unsure you must include the information in this assessment or contact privacy@une.edu.au for advice.

|  |
| --- |
| Collection of Information – IPP 1, 2, 3, 4 |
| Q1. Please explain the primary purpose of the required information collected for this project/activity and how it relates to University services or functions. Personal Information may only be collected if it is necessary for the: *University to perform one or more of its functions/activities. It should only be used for the purpose for which it was collected and unless required by the State Records Act 1998 or other legislation, be destroyed as soon as practicable after use.* * How will the information be collected?
* Will it only be collected from the individual or will third parties such as public information sources or unsolicited information be used?
 |  |
| Q2 Please outline the steps to be taken to ensure that the individual whose information is collected is made aware of the following information (at or before the time, or if that is not practicable, as soon as practicable after the information is collected):* The identity of the organisation collecting the information (if external to UNE) and how to contact it;
* The fact that the individual is able to gain access to the information;
* The purposes for which the information is collected;
* To whom (or the types of individuals or organisations to which) the organisation usually discloses information of that kind;
* Any law that requires the particular information to be collected; and
* The main consequences (if any) for the individual if all or part of the information is not provided.

*Please explain how and when this information will be provided to individuals (if not already provided), including what steps will be taken when information is collected indirectly or from someone other than the individual who the information is about.* |  |
| Q3. Are there any opportunities for individuals to remain anonymous or refuse to give certain information, for example, where they have safety concerns around risk of misuse? *If yes, please describe how individuals will be informed of this option and the consequences of not providing the information.*  |  |
| Q4 Does the proposal intend to create or use an existing unique identifier (e.g. licence number, student number or employee number), to match or link different pieces of information? *If yes, please explain how the unique identifier is assigned and why it is necessary.* |  |
| Information Mapping  |
| Q5 Describe or map the personal information flows, creating a diagram of how personal information is collected, stored, and then moved around the university/used prior to being archived or destroyed. This map can be generated at the beginning of this stage and then updated as necessary to capture the following considerations:* determine whether identity verification will be necessary;
* the process for ensuring information quality;
* security safeguards that are or will be in place;
* the potential to use anonymized data;
* points in the flow of information that may be categorized as having the most risk.

 *Please ensure when mapping information flows that both internal and external movement is captured. If data is to be stored outside of Australia this should including, primary and any secondary storage locations.*  |  |
| Use and Disclosure of Information – IPP 9, 10, 11, |
| Q6 Will the proposal change or create any process of regular disclosure of, or direct access to information, including by another part of UNE, third party service provider or government agency? *If yes, please describe how the information will be used and/or disclosed and state the parties or persons to which the information will be disclosed or made accessible.*  |  |
| Q7 Is the intended use or disclosure of information in the project consistent with the primary purpose of collection, communicated to individuals at the time of collection (refer to Qs 1 & 2 above)?*Please explain how the intended use and/or disclosure of the information is consistent with the primary purpose of collection.*  |  |
| Q8 Are there any intentions to use or disclose of the information for any other secondary purpose (e.g. marketing, research/analysis)? If so, please state the secondary purpose(s) and whether steps of de identification will occur:  |  |
| Transborder Data Flow |
| The University has an obligation to ensure any information that is transferred outside of NSW will continue to be held, used, or disclosed in a manner that is consistent with relevant legislation and Information Privacy Principles. If your project/activity uses a cloud-based service, the information may be transferred to and stored on, servers outside of NSW. |
| Q9 Will the information collected be transferred to a location outside of NSW? If yes, please describe the information to be transferred and where/to whom it will be transferred and why. If a cloud-based service is used, please state the service provider and the location of the server where the information is stored.  |  |
| Q10 Are there measures in place to ensure that privacy protections travel with the information that is transferred outside of NSW (i.e. contractual provisions with technology service providers)?*If yes, please describe these measures and attach supporting evidence where available and evidence of review by UNE Privacy or Legal team (i.e. contract).*  |  |
| Data Quality - IPP 9 |
| Q11 What steps will be taken to ensure the information collected, used and/or disclosed will be accurate, complete and up to date? *Examples include ensuring that information is obtained from a reputable source, periodic reviews of information for accuracy, system checks, etc.* Furthermore, will the individual be able to access and correct personal information collected as part of this proposal?  |  |
| SECURITY OF PERSONAL INFORMATION - IPP 12The Information Protection Principles require UNE to take reasonable steps to protect the personal information it holds from misuse, loss, and unauthorised access, modification and disclosure.  |
| Q12 What measures will be in place to protect information from misuse, loss, unauthorised access or modification (i.e. applying security measures such as encryption, access controls, etc.)? *Please reference and attach supporting documentation where available, e.g. protocols, terms of reference, process manuals.*  |  |
| Q13 Has the proposal been subjected to a threat and risk assessment, penetration testing, or other assessment? *If yes, please describe the assessment, who performed it and attach any available reports as supporting evidence.* |  |
| Q14 Are there measures in place to ensure that the information is de-identified or destroyed when no longer required? *The Records, Policy & Governance Unit may need to be consulted to determine whether an existing Retention & Disposal Authority and its prescribed retention period covers the records associated with the proposal. Please contact records@une.edu.au for further information. No record should be destroyed without consultation.* |  |
| COMPLIANCE WITH UNE POLICY |
| Information handling practices should comply with the University’s Privacy Management Plan, Records Management Rule and relevant ITD policies including the  |
| Q15 Have you assessed your proposal against the requirements of these policies? Do any of the University’s policies concerning fair handling of information need to be updated as a result of this project (e.g. Privacy and Information Management Policy, or relevant Privacy Statements)? *If yes, please provide details of changes required. Policies will routinely only change if they have become inconsistent or incorrect or no longer reflect relevant legislative compliance.*  |  |
| Q15 Please provide details of other actions or assessments that have been or will be completed as part of this project. For example: • Procurement requirements• ITS Project Management Framework: Impact Assessment• Data Security Assessment • Contract Review by UNE Legal Services  |  |

# Part 3 – PRIVACY COMPLIANCE ACTION PLAN

Please review your responses in Part 1 and 2, and using the table below, identify any actions required to mitigate identified privacy compliance risks (i.e. the development of consent forms, security access protocols, system integrity improvements, etc.). You may wish to request specialist assistance from IT Security or UNE Privacy to assist you.

|  |  |  |  |
| --- | --- | --- | --- |
| Identified Potential Privacy Risk | Action Required | Area and Person Responsible | Timeframes |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| low | Medium  | High  | Very High  |

Potential Risk Rating =

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Type of personal, sensitive, health Information**  | **Impacts a few individuals** | **Impacts small group** | **Affects all staff or whole student body**  | **Entire UNE community/ general public**  |
| **Highly sensitive/very high impact -** TFN, Financial information, health information, Union membership, sensitive PI e.g. sexual preference |  |  |  |  |
| **Multiple PI fields of lower level sensitivity which can be used to create a detailed profile** e.g. name, D.O.B, contact information, unit and course enrolment, gender, home address. |  |  |  |  |
| **Limited PI - name or student number (isolated PI fields), internal identifiers** |  |  |  |  |
| **Publically available information**  |  |  |  |  |