# Privacy Toolkit

## Section 1 - Overview & Scope

(1) The Privacy Toolkit is designed to support the implementation of the Privacy Management Plan and to help all UNE representatives to understand and manage their privacy obligations via the use of scenarios, tips and templates.

(2) **Personal information** with which UNE has been entrusted is an asset, the value of which can be enhanced and protected by appropriate security practices and business processes including education, policy and procedures. Whenever and wherever personal information from staff students or the community is collected at UNE we must think privacy first.

(3) **The risks to personal information** and the extent to which an individual can control the use, disclosure, and collection of their personal details is outlined in Australian Privacy legislation. Breaches of UNE obligations can harm both the university and the individual staff, students, patients or the community whose information we collect in our day to day operations.

## Section 2- Contents of the Privacy Toolkit

(4) The Privacy Toolkit incorporates information and aids to support the implementation of privacy obligations and a privacy by design culture at UNE:

a. Part A - Collection of personal information (PI)
    i. UNE's Privacy Statement
    ii. Risk Management - Privacy Impact Assessment Form (PIA)
    iii. Risk Management – Privacy Impact Threshold Assessment (PITA)
    iv. Fact Sheet - Surveys
    v. Collection and Consent Templates
        - Template Consent Form
        - Alumni Collection
        - Application for Employment
        - Personal Information/ Audio Visual Release Form
b. Part B - Storage
c. Part C - Access & Accuracy
d. Part D - Use
    i. Management of Personal Information Checklist
e. Part E - Disclosure.
    i. Transborder Disclosure and Cloud Computing
    ii. Request for Access to Personal Information
    iii. Reporting a potential Privacy Breach

iv. Privacy and Data Breach Management

f. Part F – Complaints and concerns

i. Making an Informal Privacy Compliant

ii. Making an Formal Privacy Compliant & Process of Appeal

iii. Appointment of Internal Review Officer (Complaints)

g. Part G – Principles Mapping

## Part A - Collection of Personal Information

**Lawful, direct, open, relevant**

(5) The collection of personal information must be lawful, direct, open, and relevant, but what is personal information (PI) and how do you collect it?

(6) The below matrix helps to determine whether privacy rules are likely to apply and the sensitivity of the information. The more sensitive the information the greater the need to ensure restricted access or increased securities. Please remember UNE has a responsibility to protect **all** personal information it collects from unauthorised access, use, or disclosure.

<table>
<tr><td colspan="3">Is it about an individual?</td></tr>
<tr><td>Yes<br>It includes one of the following - images, audio, names, addresses, student numbers, course patterns or enrolment of an individual, DNA, fingerprints, an opinion, any information that could reasonably identify an individual.<br><br>Privacy must be considered</td><td>Maybe<br>I am not sure an individual can be identified or if its information anyone may know. Sometimes even publically available information is subject to privacy laws depending on the context.<br><br>Complete the remaining items and if there is any doubt contact privacy@une.edu.au<br><br>The information does not have to be considered sensitive or undiscoverable information to be covered by privacy legislation.</td><td>No<br>The data is about animals or contains no information that could be attributed to an individual.<br><br>Privacy is not a concern.</td></tr>
<tr><td colspan="3">Are they identifiable? Identification can occur by matching information or using identifiers (e.g. student numbers) in a specific context and does not necessarily have to be a name or image of an individual. If in any doubt treat the information as identifiable.</td></tr>
<tr><td>Yes<br>Privacy must be considered</td><td>Unsure<br>Consult privacy@une.edu.au.<br><br>Sometimes it is difficult to determine whether seemingly irrelevant facts could identify an individual however in the</td><td>No<br>Information which has been appropriately de identified is no longer personal information and privacy obligations do not apply. To be sure you</td></tr>
</table>

| | | |
|---|---|---|
| | digital age data matching can be a very real possibility – if there is any doubt further investigation must occur. | can find further information regarding appropriate standards for de identification from the CSIRO's Data De Identification Framework, view the De-Identification Fact Sheet, or contact privacy@une.edu.au |
| *Does the information include health information?* | | |
| **Yes**<br>It includes information about the physical or mental health of an individual, information about a health service received or their intentions or wishes related to future health services, or body donation. Health information has an increased requirement for consent and a higher risk and must be kept securely. | **No**<br>But it includes other personal information. Privacy considerations still apply but security risks and consent requirements, may be reduced.<br><br>I am unsure - it includes measurements of physical characteristics but it isn't related to a person's health. This is likely still health information or at the least PI – contact privacy@une.edu.au for further assistance. | **No**<br>There is no PI or health information and therefore privacy requirements will not need to be considered. |
| *Is the information sensitive?* | | |
| **Yes**<br>It includes one or more of the following – sexual orientation, race or ethnic origins, union membership, religious beliefs. | **I don't know**<br>I would be happy to provide this information but it does seem more then standard personal details – contact privacy@une.edu.au | **No**<br>The information is not personal information (no privacy obligations apply). |
| *Does the information include tax file numbers?* | | |
| **Yes**<br>This information is high risk requiring increased security and vigilance. Breaches of TFNs have mandatory notification requirements. | **Maybe**<br>There may be historic TFNs included in the data set but we do not include them anymore or there may be TFNs included in historic paper files.<br><br>The existence of TFNs are classified at high risk, if there is any doubt please contact privacy@une.edu.au and in the interim treat the | **No**<br>Specific requirements relating to TFNs do not apply. |

| | | |
|---|---|---|
| | information/data as high risk – minimise access, enact security measures and seek advice. | |
| *Does the information include financial information?* | | |
| **Yes**<br>Financial information can be considered more sensitive and higher risk and may require particular care – credit card information cannot be kept and must be securely destroyed. | **Unsure**<br>We don't collect this information any longer but may have some details in hard copy.<br><br>I believe we do but it is handled by a third party contractor and therefore we are not responsible.<br><br>If in doubt contact privacy@une.edu.au UNE is responsible for all personal information it collects or information which is collected on our behalf. *This includes historic information which should be destroyed or transferred into our corporate records database.* | **No**<br>If none of the other criteria apply and you are not collecting personal information then privacy legislation may not apply. |

(7) **Tools** – The Privacy Impact Assessment is a detailed document designed to help manage the risks associated with the collection of personal information throughout a new project, application, system or process which involves the new or changed management of PI or may impact the PI of individuals. If unsure whether the use of PI in your particular circumstance requires such in depth management or has high risks which need particular care and security measures, the Privacy Impact Threshold Assessment is a smaller checklist to help you and the privacy team assess the risk associated with PI.

**TIP:** If there is PI involved you must complete the PIA, PITA or both. The Privacy Officer can assist you in determining what is required or provide training on completing Privacy Impact Assessments. In large or ongoing projects or changes, the management of PI must be iterative and the PIA updated throughout.

(8) Consent – Consent is not required when photographs are taken in public places or when the collection of information is implied by action (e.g. when filling in a digital form, it is obvious personal information is being collected). However wherever and whenever personal information is collected then a collection notice should be displayed prominently explaining what will happen to the personal information disclosed. If the information is to be used or disclosed for a secondary purpose, if it is health or sensitive information, or if a person's image is readily identifiable consent must be obtained.

(9) Consent in order to be lawful must be:

a. Freely given;
b. By the individual whose information is involved or their legal guardian;
c. Be voluntary and informed;
d. Be current and specific; and
e. Be given by an individual who has the capacity to understand and communicate consent.

**Tools:** Sample collection notices and release forms to assist you in collecting personal information are available. The Privacy Officer can also work with you to tailor a notice or form to your specific needs, seeking legal advice wherever appropriate**.**

(10) Surveys can involve the collection of detailed personal information and opinions and should be managed with care. All surveys must be conducted in accordance with strict privacy and security protocols. Please read the Survey Fact Sheet for approved platforms, collection notices and security and privacy standards.

(11) If in doubt of the existence of personal information or if old information is discovered please enact protection procedures and contact privacy@une.edu.au every time.

When you discover PI, you must:

- Minimise Access (control who can view or change the information)
- Enact Security Measures (keep digital files secured via passwords and/or encryption in approved locations, secure hard copy files in a locked storage cabinet). If items are lost, security may involve remote deletion.
- Seek Advice via privacy@une.edu.au and/or It Service Desk cierrors@une.edu.au.

We can then investigate to determine whether they are corporate records and need to be transferred to the approved record keeping system or if they can be destroyed

**Scenario – Personal Information and potential harm**

When collecting information it is important not to forget that you are managing the details of individuals and as such you have a duty of care to respect the information you collect by not being overly intrusive or collecting information which you are unable to manage effectively.

James set out to collect the views of a number of visitors to determine their opinions of the UNE campus. His aim was to create a tour which would provide visitors with insight into both the culture and the facilities at UNE. He created a questionnaire but curious about who was visiting, added fields requesting age, gender, marital status, political affiliation and the number of children they had. The questionnaire informed participants that the survey would be used to improve the experience for others and that no personal details would be shared or retained.

When he received the results many people had filled in all of the fields and provided great detail in the free text box. James could see that the answers provided valuable feedback on the food available and the town itself, as an amateur journalist he decided to use the responses to publish an article on his own blog. He told a humorous story of recent tours making some generalisations about the lives behind the participants, the post was later published in the local news.

**Things to think of**:

- Did James need to collect all of the information requested? Is it okay to ask other questions in the hope that you can solve other problems as well?

- Give the participants provided all of the details, however personal, is it reasonable to expect that the individuals wouldn't mind if they were used as material for the blog and article?
- If you receive survey answers that you didn't expect can you use them for other purposes?

**Response:** All surveys must meet criteria outlined in the survey factsheet, including privacy and security standards. Asking irrelevant questions and collecting unrelated information is unlawful and using the material for an unrelated secondary purpose breaches UNE's privacy obligations.

**Tips:** View the Survey fact sheets for further information and remember wherever possible to limit the information you collect and allow anonymity and pseudonymity wherever possible.

Put yourself in the shoes of the individual concerned and pay the same level of respect to their personal details as you would a close relative or friend. Just because you wouldn't mind if your details were shared, doesn't mean others share your opinion or make such disclosures lawful.

When collecting personal information ensuring you have appropriate meta data (time, location, contact details, when and where it was collected). This means that if you would like to use the information for an additional purpose it will be easy to request clear informed consent from the individual concerned or their parent or guardian.

## Part B - Storage

**Secure**

(12) It is important that personal information is stored securely, not kept any longer than necessary, and disposed of appropriately. To ensure the collection use and disposal of personal information is dealt with correctly, refer to the Record Management Policy and Privacy Management Plan. Records equal evidence and it is important to ensure proper documentation of all transactions of the University whilst ensuring respect for our privacy obligations. The official record keeping system can meet requirements of corporate record keeping and security measures with auditable access and disposal elements.

Tools: Please refer to the Storage of Personal Information Fact Sheet for tips on how to ensure the personal information you collects is safely secured. If in doubt stop and contact privacy@une.edu.au.

**Scenario - the importance of record keeping**

A student has received some advice related to a personal study plan to allow them to enrol in alternative units. This variation is approved by the Course Coordinator via email.

The student graduates and later their suitability for registration in their field is questioned. The student approaches UNE for proof that their variation of study plan was deemed as equivalent by the Course Coordinator. Unfortunately it cannot be found and the student takes legal action, the reputation and standards of the university are damaged and the individual needs of the student are not met.

**Things to think of:** Whose responsibility is it to record the decisions related to the student's study plan?

Is the storage of personal information within our email files secure?

**Response:** In this case information collected from the student in the course of assisting them to find meaningful and appropriate study options is also evidence that they have met the course requirements, as such it is a corporate record and is the responsibility of the person who facilitated the decision to ensure it is stored in the approved records management system in the student's file. If this had occurred the proof could easily have been found and a very stressful and damaging situation avoided.

**Tip**: Storing the information within the authorised records system ensures it is easy to find and secured against theft or misuse.

## Part C - Access and Accuracy

**Transparent, Accessible, Correct**

(13) When collecting personal information, the reasons for that collection, where it will be stored and for how long, how it is to be used and by whom must be transparent. It also must be made clear how to access the personal information kept about an individual and who the individual should contact to amend, change or withdraw their information. Personal information must be correct. Ensuring transparency and access to an individual's information by maintaining registers of where it is stored, following our record keeping obligations and complying with the Privacy Management Plan makes maintaining the accuracy of information a simple task.

(14) The accuracy of information and an individual's ability to correct their information is included in the Information Protection Principles. Before using an individual's details to inform decisions or contact them we must take reasonable steps to ensure their details are correct:

- Always consult a student's official student record (if authorised to do so), don't rely on information entered into hard copy forms or held in obscure data bases.
- If a student requests an update to their details, assist them to ensure it occurs everywhere their information is held and follow protocols in regards to ensuring the changes are effectively documented.
- When implementing a system that will hold or store personal information consider how it will interact with existing systems and whether it can guarantee personal details remain current across all systems in which they are held.
- When extracting information to create reports try to ensure the data is used directly from the repository in which it is stored. Using downloaded information stored locally can cause significant security risks and increases the potential that the information is out of date or inaccurate.

## Part D - Use

**Accurate, Limited**

(15) When faced with a rich database it can be easy, with the best of intentions, to use that information for more than the intended use at collection. However the use of personal information must be limited to the purpose for which the information was collected or a related secondary purpose or additional consent will be required.

(16) It is also important that before using personal information you confirm its accuracy, using outdated information carries particular risks.

**Tools:** the Checklist for staff who deal directly with personal and sensitive information will ensure that you have all of the relevant knowledge to manage the information you collect with privacy in mind. If you have any uncertainty or concerns, or require training for your team, please contact privacy@une.edu.au.

**Scenario: Can I contact students using the personal information contained on their record?**

You would like to contact particular students to discuss their inclusion in a social media post about research in a particular discipline or to determine why they did not complete online orientation.

As you are a UNE staff member using the phone number or UNE email address included in the students' contact details, the use of this information is acceptable in principle. If you do not normally have access to these details, you can explain the details were provided by colleagues in for the purposes indicated.

In this circumstance transparency and communication will be key. It is important the students are not concerned where their details came from, or why they were included and others were not. If you want to contact the entire student body more generally you should use the Insiders blog or the SRM via approved communication, giving the students an option to volunteer.

Alternatively, if you are hoping to contact students for a more specific reason, which only an academic could identify e.g. a specific research field, or students who completed a particular task (e.g. half of an online enrolment) you should be transparent about your reasons. When contacting the student, identify that their contact details were passed on by (insert the name of their supervisor for example) and the reason. You should also be clear that their involvement is entirely voluntary and will in no way impact their studies. You should also provide an option for them not to receive further requests for such involvement and respect their wishes.

**Tip:** Be mindful that transparency is key and it is important that you are up front about your intentions, giving students the choice of opting out and being clear about who you are and why they are being contacted.

## Part E - Disclosure

**Restricted/Safeguarded**

(17) The disclosure of personal information can include internal disclosures as well as inadvertent disclosures, breaches and external disclosures. It is important to only disclose personal information:

a. with a person's consent; or
b. if the individual was informed; or
c. if disclosure is directly related to the purpose for which the information was collected and there is no reason to believe the person would object, or
d. the person is aware that information of that kind is usually disclosed, or
e. if disclosure is necessary to prevent a serious and imminent threat to any person's health or safety.

(18) Sensitive and health information requires increased safeguards. You cannot disclose sensitive or heath information without consent.

> **Tip:** Images can sometimes inadvertently disclose sensitive information e.g. member of a trade union due to participation at an event, or the race or ethnic origins of an individual. If images clearly show sensitive information, document consent prior to use.

**Scenario - a student has provided you with sensitive information**

During a trimester 1 unit a student contacts you for assistance providing sensitive information as evidence (a psychologist report and doctors certificate detailing the breakdown of their marriage and resulting health issues which caused difficulties in completing tasks this trimester). You use this information to facilitate assessment extensions and the student successfully completes the unit.

However, you know the student well and they are not performing to the best of their abilities. With their best interests in mind, you disclose this information to their trimester 2 coordinators and other faculty staff to ensure the student receives particular care and assistance to facilitate their continued success.

**Things to think of**:

- Is it ethical and lawful to disclose the details of the student in this way?
- These documents constitute health information, where are they stored and who has access to them?

**Response:** The disclosure of this information to a wider then intended audience without the students consent results in considerable harm. Some of the other staff know the student's spouse on a personal level and they feel exposed and fearful that their mental health issues have been communicated to others. The student's health concerns are exacerbated and they leave the University, not wanting to face the wide number of staff members that are privy to what they feel is public humiliation.

In this case, the student provided this information for a specific purpose and it breached privacy principles to further disclose this information without their consent.

**Tip:** The storage of this information is a particular concern. If it must be kept this should be in a secure folder with restricted access on UNE's corporate records system, for only as long as is lawfully necessary. It should be deleted from the staff member's email, any hard copies must be shredded and access strictly limited only to those staff members who must process the extension request. This kind of health information should not be kept in the SRM, on a desktop, or in any other non-secure format.

> **Tip:** If you are unsure, ask for and record consent, or consult privacy@une.eu.au

**Scenario: Aggregated data**

Aggregated Data from unit monitoring surveys is used in the continuous improvement of teaching and in keeping with this purpose, the de identified data may be used to support presentations or research papers which present improvements to teaching technique or other pedagogical

improvements. Information collected via unit monitoring surveys can only be utilised for its stated purpose or a directly related purpose necessary for administering the survey or acting upon the provided feedback. If any other use is proposed, consent and privacy assessments would need to be undertaken prior to the survey.

**Data Breaches**

(19) A data breach occurs when a failure or potential failure causes unauthorised access to UNE's data. There is a risk to privacy due to any unauthorised access to personal information. While the risk of external attacks should not be under estimated, many breaches occur as a result of human error, carelessness, or technical faults rather than malicious intent.

(20) Unauthorised access to the information for which UNE is responsible includes access by unauthorised staff members, physical loss, and unintended virtual replication or disclosure on a third party site. It can also involve verbal discussion or broadcast of personal details to others, gossip, and disclosure of personal information to a family member without consent.

(21) The existence of harm to an individual resulting from a breach of their personal details is contextual and may relate to their own specific set of circumstances. When managing personal information of others it is important to remember that for some the disclosure of personal details that you may personally share about yourself could result in permanent and irreversible harm including:

a. physical harm or danger;
b. psychological harm;
c. damage to personal relationships or reputation; and/or
d. financial harm/

(22) Consult the Privacy and Data Breach Management Fact Sheet for further information and if in any doubt refer to privacy@une.edu.au.

Data Breaches are everyone's responsibility. Should you suspect or become aware of a data breach it must be reported immediately to privacy@une.edu.au. The earlier we can implement steps to mitigate harm the better and the 30 day disclosure period commences as soon as a breach becomes known. Know your privacy responsibilities and remain vigilant.

## Part F - Complaints

(23) UNE Representatives must fully cooperate with any privacy related investigation (either via the Privacy Officer or by other internal review), including providing access to any relevant information or documents as requested in a timely fashion.

(24) It is important that any documents related to a privacy investigation are securely stored as a corporate record and kept until after the review is complete, external reporting obligations are met and any record keeping retention periods are satisfied.

(25) As part of a privacy by design culture, UNE would like all staff to proactively respond to any concerns they may have regarding privacy by ensuring that the Privacy Officer is notified.

## Making an Informal Privacy Compliant

(26)An informal complaint or investigation is where an individual wishes to raise privacy concerns in relation to their own personal information or more generally. The process is:

a. Contact privacy@une.edu.au (you can remain anonymous if you prefer) and include the nature of your concerns, the kinds of information they include (e.g. contact details, health information, sensitive image, images) and how you became aware of the issue;
b. The UNE Privacy Officer will then liaise with you to begin an investigation, this may include follow up questions and emails or phone calls;
c. Should your details need to be given to any other staff member to continue the investigation your consent will be requested;
d. If you are happy with the solution the matter will be considered closed and records of the investigation including your original contact email will be stored securely as corporate records, with restricted access;
e. Anonymised accounts of all privacy complaints and investigations will be used for reporting and training purposes.
f. Should you wish to contest the solution or believe more in depth investigation is required you can request further investigation is conducted or make a formal complaint.

## Making a Formal Privacy Complaint – Internal Review

(27)A formal complaint is triggered when a request for internal review is lodged via this form from the Information and Privacy Commission NSW, (Form: Privacy Complaint Internal Review Application (fillable, printable pdf)).

a. The form should be lodged via privacy@une.edu.au no longer than 6 months after the date the conduct occurred.
b. Once received, the UNE Privacy Officer will advise receipt to the applicant and an Internal Review Officer will be appointed to undertake the investigation.
c. The Internal Review Officer may seek further information from the complainant and will conduct an investigation into the conduct in question.
d. If it is considered that the matter in question is not related to personal or health information, the Internal Review will end the investigation and refer to a member of the UNE Senior Executive.
e. If the matter is considered to relate to personal or health information a formal investigation will be conducted by the Internal Review Officer. This may include accessing systems and staff at UNE to determine the events that resulted in the matter which has now resulted in complaint.
f. As part of the investigation the following documents will be sent to the Information and Privacy Commission NSW:
    i. the internal review application;
    ii. a draft review report; and
    iii. a final review report;
e. Documents will also be stored securely and confidentially within UNE's corporate records system.

## Appointment of Internal Review Officer (Complaints)

(28) If an Internal Review is requested the Privacy Officer will liaise with the relevant Business Unit or School and the Director of Governance to appoint an appropriate Review Officer:

(29) If the review contains issues or concerns with previous investigations conducted by the Privacy Officer, the review will be sent directly to the Director of Governance.

(30) The Review Officer will be appointed on the basis of their knowledge of the School/Business Unit at which the issues requiring investigation occurred and their impartiality to any of the processes or staff members potentially being investigated.

(31) The Privacy Officer and Director of Governance will provide support to ensure the Review Officer understands the issues and requirements of the investigation.

(32) Any recommendations or findings from the review Officer will be reviewed by the Director of Governance prior to being communicated to the applicant.

## Part G - Principles Mapping

Table 1: Mapping the Australian Privacy Principles and NSW Information Protection Principles to UNE's Privacy Management Principles

| **Australian Privacy Principles,** Schedule 1, Privacy Act 1998 (Cth) | **Information Protection Principles (IPPs)** Part 2, Division 1, PPIP Act 1998 (NSW) | **UNE's Privacy Management Principles** |
|---|---|---|
| APP 1 – Open and transparent management of personal information<br>APP 2 – Anonymity and pseudonymity<br>APP 3 – Collection of solicited personal information<br>APP 4 – Dealing with unsolicited information<br>APP 5 – Notification of collection of personal information | IPP 1 - Collection of personal information for lawful purposes<br>IPP 2 Collection of personal information directly from individual<br>IPP3 - Requirements when collecting personal information<br>IPP 4- Other requirements relating to collection of personal information | **1. Collection** must be lawful, direct, open and relevant |
| APP 11—Security of personal information | IPP 5- Retention and security of personal information | **2. Storage** must be secure and retained in accordance with the stated purpose obtained with consent |
| APP 10—quality of personal information<br>APP 12—access to personal information<br>APP 13—correction of personal information | IPP 6 - Information about personal information held by agencies<br>IPP 7 - Access to personal information held by agencies<br>IPP 8 - Alteration of personal information | **3. Access & Accuracy**: Information is accessible, amendable and accurate |

| | | |
|---|---|---|
| APP 6 – Use and disclosure of personal information<br>APP 7—direct marketing<br>APP 8—cross-border disclosure of personal information<br>APP 9—adoption, use or disclosure of government related identifiers | IPP 9 - Agency must check accuracy of personal information before use<br>IPP 10- Limits on use of personal information<br>IPP 11 - Limits on disclosure of personal information<br>IPP 12- Special restrictions on disclosure of personal information | **4. Use & Disclosure** is limited, reasonable, restricted for sensitive information, safeguarded |