Privacy Management Rule

Section 1 - Overview and Scope

(1) The ability of an individual to control their personal information is an important right protected by Commonwealth and State privacy legislation. UNE supports this right by effective information management incorporating all aspects of the information lifecycle (that is collection, use or disclosure, storage, accuracy and access and destruction or archiving).

(2) UNE's Privacy Management Rule established in accordance with the requirements of the Privacy and Personal Information Protection Act 1998 (PPIP Act) outlines how UNE supports the core privacy management principles and its 'privacy by design' approach.

(3) This Rule applies to all UNE Representatives, the University's decision-making bodies and any individuals providing personal information to the University.

(4) The UNE Senior Privacy and GIPA Officer is available to provide assistance and answer questions from the University community about privacy matters. Any circumstance where personal information is collected, stored, used or disclosed in a manner that is not in accordance with the privacy management principles outlined throughout this Rule, must be brought to the attention of the UNE Privacy Officer (refer to the UNE Privacy webpage for Senior Privacy and GIPA Officer contact details or email: privacy@une.edu.au).

(5) This Rule should be read in conjunction with the Privacy Management Toolkit which provides reference documents and templates designed to facilitate and inform the implementation of this Rule.

(6) This Privacy Management Rule is organised into the following sections:

a. Part A provides an overview of personal health and sensitive information;
b. Part B outlines each of the core Privacy Management Principles and how they are supported at UNE;
c. Part C describes the process for raising privacy concerns, making a compliant;
d. Part D summarises key roles and responsibilities in Privacy at UNE, and outlines how the implementation of this Rule is to be measured and recorded; and
e. Part E confirms the authority and basis for compliance regarding the Rule and outlines associated documents and tools which can help support UNE Representatives to effectively manage privacy and personal information at UNE.

Part A - Personal Information

What is personal information?

(7) Personal Information (PI), in accordance with section 4 of the PPIP Act, is any information or an opinion about an identified individual or information about an individual whose identity can be readily ascertained. Whether information is considered identifiable depends on a number of factors including context, access, and number of data points. It includes but is not limited to:

a. personal details such as name, address, and other contact information about an individual;

b. photographs, images, video or audio footage;
c. fingerprints, blood or DNA;
d. employee record information;
e. credit information;
f. banking and financial information;
g. unique government identifiers such as Medicare numbers or National Unique Student identifiers;
h. sensitive information (see more information below); and
i. health information(see below and note this is also subject to specific criteria under the Health Records and Information Privacy Act 2002(NSW); and
j. restricted information (such as Tax File Numbers which are key identifying information used by Government and are restricted in use by law).

(8) Common activities where personal information might be collected at UNE include:

a. applications for admission, enrolment, or participation in student learning activities (including work integrated learning, class attendance, system access logs etc.) and records of student learning outcomes;
b. information collected to help with student management and support (including for communications, attendance or records of inductions and training, and safety and wellbeing);
c. during payment of fees or registering for HECS-HELP loans;
d. information about an individual's participation in special activities (competitions, community awards, outreach activities, field trips, volunteer work etc.);
e. staff employment applications, performance management information and promotions, grievances, requests for leave, medical certificates;
f. photographic, audio or video recordings/excerpts and testimonials from events;
g. feedback via surveys and other mechanisms;
h. elections and nominations;
i. staff and student interactions – lecture recordings, tutorial recordings, verbal and written communications etc.;
j. institutional reporting and statistical analysis (not including satisfactorily de-identified or anonymised information);
k. behavioural analysis – including student learning analytics or staff usage information; and
l. complaints, grievance processes and/or internal review investigations.

Identifying and Managing Sensitive, Health and Restricted Information

(9) Sensitive, health and restricted information are types of personal information where there is a higher expectation of care to limit the collection, access, use and disclosure and to ensure that information is secured to the requisite standard.

a. UNE Representatives should be familiar with information that falls into these categories and take particular care that:
    i. these types of information should only be collected where necessary;
    ii. consent is obtained for collection or disclosure including between UNE business or operational areas.

Sensitive Information

(10) Poor management of sensitive information can introduce discrimination and bias into planning and decision making. As a result, collection (and therefore management) of sensitive information should generally be avoided or done only in circumstances where required by law, or where there are clear benefits to the individual and their consent has been obtained. The disclosure or specific categories of sensitive personal information under the PPIP Act is prohibited unless the disclosure is necessary to prevent a serious and imminent threat to the life or health of the individual concerned or another person. This information includes:

a. ethnic or racial origin;
b. political opinions;
c. religious or philosophical beliefs;
d. trade union membership; or
e. sexual activities.

Health Information

(11) The collection and use of health information is outlined in the Health Records and Information Privacy Act 2002 (HRIP Act)(NSW) which aims to promote the fair and responsible handling of health information. Health information includes:

a. any information or an opinion pertaining to the physical or mental health or disability of an individual, their express wishes about the future provision of health care and details of any health services provided or to be provided to them; or
b. other personal information collected to provide, or when providing, a health service; or
c. personal information about an individual collected in connection with the donation or intended donation of an individual's body parts, organs or body substances; or
d. any genetic information about an individual arising from a health service provided to that individual, that is, or could be, predictive of the health (at any time) of that individual or a genetic relative; or
e. healthcare identifiers.

(12) Information about an individual's health or medical condition attracts a higher standard of management, both in terms of security and access to such information within an organisation.Limits exist for disclosure to third parties (which can occur only when consent is provided or specific exemptions apply), including:

a. whether the information is disclosed for a secondary purpose directly related to the primary purpose and the individual would reasonably expect the information to be used for the secondary purpose;
b. the disclosure is reasonably believed to be necessary to lessen or prevent a serious and imminent threat to life, health or safety of another person; or
c. a serious threat to public health or safety; or
d. any other exemptions in Schedule 1, 11 of the HRIP Act.

(13) Individuals may be given the opportunity for anonymity wherever lawful and practicable (e.g. in reporting). Examples of instances where the University collects and subsequently uses health related information includes, but is not limited to:

a. when recording details of disability or special needs at enrolment or when required to facilitate adjustment to student learning materials and learning environments;
b. during physical activities and practicals in the Health Sciences such Exercise Science or Biomedical Science, where physical characteristics may be studied and recorded;

c. at a staff member's point of employment, or as required, should they wish to advise the University of a disability that may require adjustments to be made to their workplace in order to undertake their work;
d. at the point of approving staff travel/equipment/vehicle use where an existing medical condition may need to be considered in that approval;
e. at the point of lodging forms such as medical certificates, accident reports and counselling records relating to staff sick leave and/or student special considerations for exams or study purposes;
f. at the point of attending the UNE Medical Centre to receive attention and healthcare services;
g. during the provision of clinical practice services or teaching and learning (such as related to counselling, nursing or other medicine and allied health activities or sports science);
h. for work health and safety ('WHS') related purposes, including monitoring of health during use of some facilities or equipment (including sports or activities where there may be chemical/biological exposure etc.), for reporting of safety related incidents/hazards and for WHS claims;
i. during ethics approved research projects where health related information might be collected from participants; and
j. where prospective donors provide health-related information in relation to the donation of their body, via the UNE Body Donor Program.

(14) Restricted information: Examples of restricted information include:

a. Tax File Numbers (TFN): The Privacy (Tax File Number) Rule 2015 (TFN Rule) issued under section 17 of the Privacy Act 1988 (CTH) regulates the collection, storage, use, disclosure, security and disposal of an individual's TFN information. UNE Representatives should seek advice regarding collection of TFNs as:
    i. there are strict processes to be followed in regards to the collection and storage of TFNs in Australia;
    ii. TFNs should never be used as an identity verification tool and should only be collected if explicitly required by law; and
    iii. the loss, use or exposure of TFNs has mandatory reporting requirements to the Office of the Australian Information Commissioner and in some circumstances the Australian Tax Office. If you know or suspect such a disclosure has occurred you must contact the UNE Privacy Officer via privacy@une.edu.au.
b. Information subject to Professional Legal Privilege: Access to, or use of some information may be restricted where the information is covered by legal professional privilege. Often this will relate to personal information provided in response to a request from a legal professional who is providing advice on a matter of a legal nature. If you are unsure about what information might be subject to Professional Legal Privilege, please contact the Legal Office.
c. Classified information: in some circumstances, personal information might be collected at UNE that has been classified by a Government agency as sensitive, protected, secret or top secret, for example research information relating to defence or national security matters. For more information, see the Australian Government's Attorney Generals Department Protective Security Policy Framework.
d. Personal information at UNE which may require restricted access includes:
    i. some staff related files/information; and
    ii. some confidential matters of Council or Academic Board Standing Committee relating to identified individuals; and
    iii. grievances or serious complaints including fraud or information relating to ICAC investigations.

(15) Particular categories of personal information are exempt from the scope of both the PPIP ACTand the HRIP Act. These include:

a. information about an individual who has been deceased for more than 30 years;
b. information about an individual contained in an official publication which is open and freely available to the

public e.g. in books, newspapers, television, or some internet publications (not including social media, please discuss with the Senior Privacy and GIPA Officer if unsure);

c. where disclosure is permitted or required by law e.g. requested under a subpoena, for law enforcement purposes or related matters (personal information impacted by this exemption should be discussed with the UNE Legal Services); and
d. information or an opinion about an individual's suitability for appointment or employment as a public sector official; and
e. Under s41 of the PPIP Actand s62 of the HRIP Act, the Privacy Commissioner may make a direction or modify the requirement for an agency to comply with an Information Privacy Principle (IPP) or a code of practice. These directions can be found on the Information and Privacy Commission website.

(16) The University must comply with the Privacy Act 1988 (Cth) in relation to:

a. Personal information the University collects and holds regarding student assistance provided by the Commonwealth (which is an obligation under Section 19-60 of the Higher Education Support Act 2003 (Cth)); and
b. Tax file number information (in accordance with the Tax File Number Guidelines, a legislative instrument under the Privacy Act 1988 (Cth)).

Part B - UNE's approach to supporting the core Privacy Management Principles

(17) UNE's Privacy Management Principles are outlined below and their application summarised in Table 1:

a. The collection of personal and health information is lawful, direct, relevant, open and transparent;
b. Personal information is stored securely, not kept any longer than necessary and disposed of appropriately;
c. Personal and health information is accurate and accessible to the person to whom it relates; and
d. Personal and health information collected for a particular purpose, is not used or disclosed for another purpose (unless permitted by law).

Table 1 – Personal information handling lifecycle at UNE

1. Collection	2.Storage	3. Access and Accuracy	4. Use and Disclosure
is lawful, direct, relevant, open and transparent	Is secure and retention is managed in accordance with consent gained and records management obligations.	Information is accessible, amendable and accurate.	is limited, restricted for sensitive information and safeguarded

(18) UNE's Privacy Management Principles (refer to the Privacy Toolkit 'Principles Mapping') have been derived primarily from:

a. The PPIP Act's twelve (12) Information Protection Principles;
b. the Health Privacy Principles (HPPs) found at Schedule 1 of the HRIP Act, and
c. the key principles associated with the processing of personal data under the European General Data Protection Regulation.

Collection

Lawful, Direct, Relevant, Open(UNE Principle 1, IPP's -1,2,3 and HPP's -1,2,3,3)

(19) Personal and health information is to be collected in an open and transparent manner and unless otherwise

permitted by law, can only occur on the basis of having the consent of an individual. The collection of personal and health information must be relevant for the purposes for which it is collected, not be excessive and not unreasonably intrude into the personal affairs of individuals. It is the responsibility of all UNE Representatives to ensure that collection of personal and health information maintains the principles of being lawful, direct, relevant and open.

(20) Lawful - Unless otherwise permitted by law, the collection of personal and health information by UNE will only occur:

a. for a purpose related to the University's functions (as outlined within the University of New England Act 1993 (NSW)) or which is necessary for the provision of specific health services provided by the University;
b. for a secondary purpose on the basis of having the consent of an individual to collect their information, where consent is specific and freely given on an informed and unambiguous basis; and
c. where collection is by lawful and fair means.

(21) Direct and relevant – Personal information is to be collected directly from the individual about whom it relates. It will not be collected from an individual without their consent, unless:

a. it is collected from another agency or third party who has the authority to produce/disclose it whether via consent from the individual or other lawful means; or
b. there are circumstances permitted by law, including:
    i. to provide emergency support to an individual involved in a health or life-threatening incident;
    ii. when the person is a vulnerable person and consent is provided by a parent, guardian, or other person authorised person; or
    iii. where non-compliance is lawfully authorized or permitted under any law;
    iv. exemptions related to legal proceedings, law enforcement, ICAC, the NSW Police Force, NSW Crime Commission and others;
    v. authorised exchanges between public sector agencies;
    vi. when the collection relates to an exempt activity (such as some collection activities for research or statistical purposes, or in the public interest) and where:
        - it is unreasonable or impractical for the information to be collected from the individual; and
        - the collection use or disclosure is in accordance with the NSW Information and Privacy Commission (IPC) guidelines.

(22) Consent – where consent is required for the collection of personal or health information it must be:

a. specific, freely given, provided on an informed and unambiguous basis, timely, given by a person with capacity, and with clear options to withdraw consent or correct information;
b. relevant to the purpose for the collection, and be limited (i.e. not excessive), accurate, complete and up-to-date;
c. not unreasonably intrusive; and
d. wherever possible provide the option of anonymity or the use of a pseudonym (where the University is not required (or authorised) by law, a court order, or a UNE policy document, to deal with specific individuals, an individual must have the option of not identifying themselves).

(23) Open and Transparent: Personal and health information is to be collected in a clear and conspicuous manner. When the University collects personal information it must ensure transparency of purpose so that the individual concerned is aware of:

a. the fact the information is being collected;

b. the purposes for which the information is being collected;
c. the identity of the organization and how to contact it (health information only);
d. the persons to whom (or the types of persons to whom) the organization usually discloses information of that kind (health information only);
e. the right of access to, or correction of, the information by the individual concerned;
f. any repercussions that might arise if an individual chooses not to provide all or part of the personal information upon request (e.g. access to services)whether the information collected is required by law or is voluntary; and
g. the intended recipients of the information;

Privacy Impact Assessments

(24) UNE Representatives planning the collection of information are to undertake a Privacy Impact Assessment(see templates in UNE's Privacy Toolkit)in conjunction with the UNE Senior Privacy and GIPA Officer.The purpose of a Privacy Impact Assessment is to:

a. understand the scope and nature of the personal information to be collected and the reasons/authority for that collection;
b. inform planning for information management throughout the information handling lifecycle, (including system or service design, access requests and access restrictions);
c. inform the content of an appropriate transparent and open collection notice; and
d. manage institutional risk and inform any controls (such as contractual arrangements) required to secure personal information.

(25) A Privacy Impact Assessment must be completed, in consultation with the UNE Privacy Officer:

a. prior to the commencement of a new project or activity using:
    i. an initial Privacy Impact Threshold Assessment (PITA) to determine whether the project includes personal information; and/or
    ii. a more detailed Privacy Impact Assessment (PIA) for large scale, ongoing or high risk projects;
b. during change or renewal of an existing project, system or process involving the collection, use, or processing of personal information where:
    i. a periodic review of the project/process as it progresses is undertaken to ensure all privacy considerations are being addressed; and
    ii. by having a 'privacy by design' approach, detailed requirements in the investigation phases of new products, systems, applications or processes help guide decisions on selection of solutions which support privacy compliance from the outset, avoiding more costly and time consuming processes to retrofit information management standards.
c. when a contract involves goods or services provided to UNE that may have trans-territorial implications for compliance with privacy legislation of jurisdictions outside of NSW and Australia;
d. with a record of all PIAs or PITAs added to the project or activity file in the authorised records management system and a copy sent to privacy@une.edu.au.

Collection Notice:

(26) UNE Representatives planning to collect information are to prepare a collection notice in conjunction with the Senior Privacy and GIPA Officer, noting that:

a. A collection notice is a structured communication which meets legal requirements and provides an individual with details of how the University will collect, use, manage, store, disclose and dispose of the personal

information being collected for that specific purpose or activity, and a link to this Privacy Management Rule. Please note:

i. the University has a number of template Collection Notices in the UNE Privacy Toolkit that may be used as the basis for a custom notice; and

ii. all collection notices should be reviewed by the Senior Privacy and GIPA Officer in the first instance. A review by the Legal Services may be required for complex or potentially high risk collection activities.

Storage

Personal Information storage is protected, secure (UNE Principle 2, IPP5, and HPP5).

(27) It is the responsibility of all UNE Representatives to ensure that plans are in place to secure personal and health information, to control and monitor the period of time the information is retained, and to control and evidence appropriate disposal of information which is no longer required to be held.

(28) Protected – This includes ensuring that personal and health information collected by the University will be stored, so that the personal information is protected from:

a. misuse, interference and loss;
b. unauthorised access, modification or disclosure; and
c. unauthorised disposal (being retained as a corporate record in accordance with the University's Records Management Rule and retention and disposal standards consistent with the State Records Act, 1998 (NSW).

(29) Secure – UNE Representatives are responsible for ensuring the security of personal information kept by the University and should consider the following practices and measures (refer also to the Privacy Toolkit).

a. Control collected information: Action should be taken to ensure personal information is controlled at point of collection. This means:
   i. wherever feasible, information should be collected via secure digital means and captured within a University approved recordkeeping system with the requisite security and access controls (see Tip 1 below); and
   ii. where information is not captured directly into an approved recordkeeping system:
      - the UNE Representatives responsible for collection of personal information must uphold all obligations under the Privacy Management Rule whilst the information is in their care (e.g. security measures and physical controls are exercised over paper records, emails, forms or other documents); and
      - the UNE Representative should liaise with the Records Team via records@une.edu.au regarding the transfer of information into the University's recordkeeping system and appropriate retention, access and disposal arrangements.
b. Control access to information: Measures are to be enacted to ensure personal information is only accessible by those UNE Representatives (including authorised third party service providers) who have a genuine need to do so, and where:
   i. digital access controls and encryption are established where necessary; and
   ii. hard copy files are locked in secure storage until such time as they can be transferred to records@une.edu.au for digitising and disposal as relevant. Please also note:
      - The "Management of Personal Information Checklist" can assist you in knowing your obligations and identifying risks.
      - The storage of health information, detailed personal information or sensitive information may require a higher standard of digital or physical security, restricted access and greater care. Seek

advice from the UNE Senior Privacy and GIPA Officer, IT Security and/or the Legal Office when planning personal information management.

c. Control Metadata: Whenever personal information is collected ensure appropriate metadata is maintained to provide context and provenance to that information including where appropriate:
    i. date and location of collection, consent status, document number of consent, contact information of individual, duration and end date of consent, limits to consent, requests to withdraw consent or update information, limits to use.

d. Control retention and disposal of records: The University needs to dispose of information when it is no longer required, and keep evidence of that disposal, for example:
    i. if the University stores personal information about an individual and that information is no longer required for any purpose associated with the University (and provided it is not contained in a State Archive, a Commonwealth record and not required by or under an Australian law, or court/tribunal order), the information should be either
        - de-identified to a requisite standard and stored securely; or
        - destroyed in a secure manner, in accordance with the University's Records Management Rule.
    ii. Evidence of the collection, storage & destruction of the personal information that is no longer required, should be produced on request from the Senior Privacy and GIPA Officer or other governance structures at UNE. In practice:
        - Evidence and authorities for disposal of personal information records that are held within the UNE Records Management System (RMS) are kept by the Records Team; and
        - UNE Representatives should ensure that any third party service providers provide UNE with copies of disposal standards and activities as part of their service agreement with the University and that all such reports and saved in the University's Records Management System (RMS).

Tip 1: UNE's IT Security Team can and should be consulted on plans for secure storage of personal information. The IT Security Team can also assist with planning for high levels of security and access controls for particular types of personal information – including health, sensitive and restricted information.

Remember too that information collected via certain online forms, survey providers etc. may not be secure. If you have a solution in mind – make sure you ask the Security Team to review the proposed approach so you can be assured it meets all relevant security standards.

If you have not investigated and implemented appropriate security and privacy measures, then collection must be delayed until such time as security and privacy measures are implemented or not occur at all.

Access and Accuracy

Personal Information management is transparent, accessible, correct, accurate – (UNE Principle 3, IPP's-6,7,8 and HPP's 6,7,8,9)

(30) The University will plan and establish processes to maintain and update personal and health information and to facilitate access to that information for the person to whom it relates. Students and staff can request access to or amend their personal information or health information held by UNE via self-service accounts, the relevant UNE directorate responsible e.g. Human Resources for staff or Student Success for students, or through contacting the UNE Senior Privacy and GIPA Officer via privacy@une.edu.au.

(31) The University will establish processes for:

a. Requests for Access: The University will upon request from an individual:
    i. provide them with access to their personal and health information without delay or expense, and provide it in a structured, commonly used and machine-readable format (unless UNE is authorised or otherwise permitted by law not to comply, Schedule 1,7(2) of the HRIP Act);
    ii. ensure the request is in writing by an authorised individual and provided only after reasonable steps to verify identity have been taken; or
    iii. if the University does not agree to provide an individual with access to their information for any reason, the University will advise the individual in writing, outlining:
        - the reasons for the refusal (unless given the grounds for refusal, it would be unreasonable to do so); and
        - the mechanisms available to the individual, to query the refusal (provided at the Privacy Concerns and Complaints section of this Rule).
    iv. transmit, where it is technically feasible to do so, the individuals personal information directly to another party in a structured, commonly used machine-readable format.
b. Requests for amendments: The University must upon request from an individual either:
    i. make appropriate amendments (whether by corrections, deletions or additions) to the individual's personal information to ensure the personal information held by the University:
        - is accurate; and
        - is relevant, up to date, complete, and not misleading; or
    ii. enable, where the information is kept in UNE systems, individuals to maintain the accuracy of their own personal information, via secure systems; or
    iii. facilitate changes to information via providing individuals with a relevant UNE form and/or associated procedures to request amendments to information; and
    iv. ensure that,
        - where it is not possible to amend or correct personal information (e.g. if a corporate system is temporarily unavailable; if a system will not allow it; if the change is in conflict with legislation, the University's Records Management Rule or other UNE policy; or if the question of accuracy is contentious) the request for change is to be recorded on an official record (e.g. alternate online or hard copy record) in lieu of making the change upon a corporate personnel system or database.
        - The record should be made available as an addendum to any system or record where the original information is kept so that users at the original information source are aware of the discrepancy. The information should be updated and the corporate record amended as soon as possible.

(32) Relevant and Accurate – UNE must not use health information without taking such steps as are reasonable in the circumstances to ensure that, having regard to the purpose for which the information is proposed to be used, the information is relevant, accurate, up to date, complete and not misleading.

Use and Disclosure

Personal Information use and disclosure is restricted, limited, accurate, safeguarded (UNE Principle 4, IPP's – (9,10,11,12 and HPP's -10,11)

(33) Limited and restricted - the use and disclosure of personal and health information will be limited by the University and restricted to the purpose for which it was collected, unless an exemption applies, for example:

a. the individual to whom the information relates, provides their consent;

b. the secondary purpose is directly related to the primary purpose of collection and the individual would reasonably expect the information to be used for the secondary purpose;
c. the use of this information is necessary to prevent or lessen serious and imminent threat to the individual to whom the information relates or another person;
d. the use is necessary to prevent a serious threat to public health or public safety;
e. non-compliance is lawfully authorized or permitted under any law;
f. exemptions related to legal proceedings, law enforcement, ICAC, the NSW Police Force, NSW Crime Commission and others; or
g. authorised exchanges between public sector agencies.

(34) This means that the University:

a. must, wherever it is practicable to do so, ensure that all requests for disclosure by third parties will be in writing. All such requests will be saved to the University's Records Management System (RMS);
b. must take reasonable steps to ensure that any entity in receipt of personal information from the University, does not breach Australian privacy principles (HPPs or IPPs or under the Privacy Act 1998to the extent it applies), in relation to the management and use of that information, including establishing controls and assurance processes:
    i. in any agreements or contractual arrangements with third parties; and
    ii. within UNE systems or storage facilities via periodic review of access logs or similar evidence relating to the re-use and disclosure of personal and health information; and
c. will take reasonable steps to ensure the safe transfer of personal information across systems during transit. Personal information should not be requested or sent by unsecured means and all transfers must adhere to UNE's Information Security Policy and the Electronic Transactions Act 1999 (Cth).

> Tip 2: Did you know that UNE remains responsible for the practices of any third party organisations which it engages to provide goods/services relating to personal information (collection, storage, management, use and disclosure)?
>
> Contracts with third parties who assist UNE with the management of personal information or use personal information in the provision of their services, must incorporate appropriate steps (within contracted terms and contract performance review arrangements) to ensure compliance with Australian Privacy principles.
>
> UNE Representatives should refer to the IPC Guidance note on Transborder Disclosure, contained within the Privacy Toolkit for more information on how to ensure compliance of third parties operating outside of NSW.

(35) Accurate – All staff involved in the use of personal information will enact reasonable processes to confirm validity and accuracy of that information prior to its use. This means using information from central databases and confirming accuracy prior to use wherever possible. The impacts on the individual if accuracy is not confirmed should be considered.

(36) UNE Representatives will need to ensure they are aware of UNE's Privacy Management Principles before using or disclosing personal information. For example:

a. Verbal disclosure: Lectures, public forums, meetings, discussions etc;
b. Social Media and Online: Information disclosed in online forums or other interactive/social media (including chat rooms, discussion forums, message boards, news groups, blogs etc.) may be deemed to be public information. It is important that UNE Representatives:

i. understand that owners of forum sites will require personal details (e.g. an individual's email address, name etc.) to be transmitted to third parties;
ii. are clear that engagement with external social media is an opt-in event
iii. exercise caution when engaging with online communication channels and social media ensuring that:

- they do not represent the University unless they are authorised to do so (please refer to the UNE Social Media Policy); and
- they do not post any confidential information or material that has the potential to damage the reputation of the University or others.

c. Collection of material at events: Staff engaged in the collection of audio visual or testimonial materials at events held by the University or who collect material for promotional purposes will always seek permission from individuals involved (including UNE staff) before using or capturing the material and will advise how that information will be managed or used. After obtaining consent, UNE Representatives will ensure the material is used only for the purpose for which it was collected and is stored securely in an authorised system. UNE will respect the wishes of those who do not wish to be photographed or filmed by endeavoring to provide times or locations at events where they can be enjoyed without any media collection.
d. Mailing and Contact Lists: The University and individual units within the University may keep subscriber, mailing and contact lists that contain personal information. The lists are not to be used for any other reason than those explained to subscribers and for which consent was obtained.

(37) Safeguarded under the PPIP Act the disclosure of certain types of sensitive personal information is prohibited, unless necessary to prevent a serious and imminent threat to the life or health of the individual concerned or another person;

a. unauthorised access or requests for sensitive and health information must be reported to your immediate supervisor and UNE's Privacy Officer; and
b. management of sensitive and health information should be planned with advice from the UNE Senior Privacy and GIPA Officer at privacy@une.edu.au, Technology and Digital Services and/or the Legal Services as required.

(38) The University maintains a number of public registers (which are defined by the PPIP Act as a register of personal information that is required by law to be, or is made, publicly available or open to public inspection that highlights a connection between the organisation and those who support it). These may include:

a. Student registers, including:
    i. Graduate lists; and
    ii. Lists of Scholarship and prize recipients.
b. Alumni registers, including:
    i. Distinguished Alumni Award recipients; and
    ii. Donor lists.
c. Staff registers, including:
    i. Staff contact lists
d. Council/Board members including:
    i. UNE Council and Council subcommittees;
    ii. UNE Academic Board; and
    iii. UNE Life Pty Ltd Pty Ltd Board.
e. Business registers including:
    i. Register of Government Contracts; and

ii. Disclosure log of information released under the Government Information (Public Access) Act 2009

(39) Prior to information being published to a register (e.g. the names of the members of Council and their current term and qualifications), the person(s) to whom the information relates should have the opportunity to review the information for accuracy.

(40) At section 58 of the PPIP Act it states that in circumstances in which an individual's safety or wellbeing may be affected, that individual can request their information is not published or removed. Under these circumstance UNE must suppress this information unless the public interest in maintaining public access to the information, outweighs any individual interest in suppressing the information.

(41) Individuals included in a public register can request amendment or removal by contacting the University (see clause 30), the UNE Senior Privacy and GIPA Officer at privacy@une.edu.au, or via details published within the particular register.

Identifiers, Transferals and Linkage

Health information is controlled, authorised, anonymous (HPP's- 12,13,14,15)

(42) The Health Privacy Principles 12 and 15 at Schedule 1 of the HRIP Act provide additional usage and disclosure protocols, as follows:

a. Anonymous – Identifiers may be used to protect an individual's identity under Schedule 1 s 12 (1) of the HRIP Act if the assignment of identifiers is reasonably necessary to enable the organisation to carry out any of its functions efficiently. The identifier represents the individual and protects their identity and health-related data. University researchers may use identifiers to ensure anonymity of research participants. Identifying details (names, dates of birth and addresses) are replaced by a unique identifier, preferably a running number. If the de-identification of data is adequate (to the relevant de identification standard), the data is no longer subject to associated legislation. Wherever it is lawful and practical UNE will provide the option of anonymity when utilizing health services or providing health information.
b. Authorised - Linkage of health records and information. The University must not include health information about any individual in a health records linkage system unless the person involved has provided their consent for this to occur or an exemption under the HRIP Act applies.

(43) Controlled - In addition to normal disclosure rules, UNE will only provide the personal and health information of individuals to another person or body who is in a jurisdiction outside New South Wales or to a Commonwealth agency, where:

a. the University reasonably believes the recipient of the information is subject to a law, binding scheme or contract that effectively upholds principles for fair handling of information that are substantially similar to the IPPs or HPPs; or
b. the individual to whom the information relates consents to the transfer; or
c. the transfer is necessary for the performance of a contract between the individual and the organisation, or for the implementation of pre-contractual measures taken in response to the individual's request; or
d. the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the individual between the organisation and a third party; or
e. the transfer is reasonably necessary to lessen or prevent serious and imminent threat to the life, health or safety of the individual (whose information is disclosed) or another person; or
f. a serious threat to public health or public safety; or
g. the University has taken reasonable steps to ensure the information won't be dealt with inconsistently with the HPPs, or

h. the transfer is permitted or required by any law; or
i. all of the following apply:
    i. the transfer is for the benefit of the individual;
    ii. it is impracticable to obtain consent from the individual to that transfer; and
    iii. if it were practicable to obtain consent, the individual would be likely to give it.

Part C - Privacy Applications, Concerns and Complaints and Management of Potential Breaches

(44) The University's Senior Privacy and GIPA Officer is the first point of contact for all privacy related matters. They should be informed of all privacy concerns and complaints in the first instance. To contact the UNE Senior Privacy and GIPA Officer see the Privacy website or email privacy@une.edu.au.

(45) The Senior Privacy and GIPA Officer will take action to assess an eligible data breach, and notify individuals affected by data breaches in accordance with the law.

Making a Complaint

Informal Complaint Process

(46) An informal complaint or enquiry is where a person wishes to explore their concerns in relation to the management of personal information whether anonymously or otherwise. Informal complaints can be made by contacting the UNE Senior Privacy and GIPA Officer at privacy@une.edu.au.

(47) In most cases, it is possible to address informal complaints without the need to lodge an internal review request.

(48) The UNE Senior Privacy and GIPA Officer will address informal complaints collaboratively, with a view to alleviating privacy concerns and identifying/developing future activities to raise awareness of privacy issues and ensure privacy breaches do not occur.

(49) If an individual is dissatisfied with the outcome of the informal complaint, they may request an internal review to be conducted in relation to the privacy issue raised.

Internal Review Process

(50) A formal privacy compliant when lodged, triggers an internal review process by UNE of the complaint.

(51) A request for internal review must be lodged within six months of the date when the conduct/issue became apparent. Requests can be made via the Privacy complaint - Internal review application form and submitted to privacy@une.edu.au. If more than six months have passed, the complainant will need to ask the University for special permission to lodge a late application via privacy@une.edu.au.

(52) Internal reviews are undertaken in accordance with any relevant legislative requirements and guidelines. An internal review must be completed by UNE within 60 days of receiving a valid application, unless an extension is negotiated with the applicant.

(53) The University will appoint an Internal Review Officer to undertake the internal review. The Internal Review Officer must be someone who was not substantially involved in any matter relating to the conduct/issue complained about previously.

(54) The University is required to inform the Information and Privacy Commission of any applications for internal review, and must:

a. as soon as practicable after receiving the application notify the Privacy Commissioner of the application; and
b. keep the Privacy Commissioner informed of the progress of the internal review; and
c. inform the Privacy Commissioner of the findings of the review and of any actions proposed to be taken, in relation to the matter.

(55) If it is considered that the information being investigated is not specifically related to personal or health information, the Internal Review Officer will not investigate the conduct in question any further. If appropriate, the matter will be forwarded to the relevant member of the UNE Senior Executive team, for consideration and any appropriate action.

(56) If the Internal Review Officer determines that the review should be brought to the attention of a particular member of the UNE Senior Executive (eg. if the matter was related to a business practice within their portfolio), the matter will be shared with that member of the Senior Executive for their consideration and any appropriate action.

(57) UNE Representatives are to fully co-operate with any privacy-related investigation, providing access to any relevant or requested documentation as requested. Where UNE Representatives are aware of any activities relating to the potential request of personal information (eg. legal action or a privacy investigation) any material relating to the investigation on corporate record and IT systems is to be preserved until the investigation is finalised and any external appeal timeframes have been met.

(58) If an individual suspects that any corrupt conduct has been entered into in relation to the management by the University of personal or health information, the matter should be addressed in accordance with the University's Public Interest Disclosure and Whistleblower Policy and its associated procedures.

(59) If a review is not completed within the required 60 days or an applicant is not satisfied with the outcome or handling of an internal review, they can apply for an external review with the NSW Civil and Administrative Tribunal (NCAT). An application must be made within 28 calendar days of receiving notice about the decision or the expiration of the 60 day period. Further information on reviews by the NCAT is available on the NCAT website under privacy of personal information.

(60) Individuals may also make a complaint directly to the Information and Privacy Commission or directly to the NSW Privacy Commissioner whether verbally or in writing.

Data Breach Response

(61) A data breach occurs when a failure or potential failure causes unauthorized access to UNE's data. When this access involves the unauthorized access to, disclosure of or loss of personal information of UNE's staff, student's or community members it can cause serious harm to individuals. This harm can include financial, social, reputational, or physical harm and may damage the ability of the individual to study successfully at UNE. It also poses the risk of reputational damage or financial penalties to UNE. A data breach could include but is not limited to:

a. the loss of a USB, laptop or other personal device;
b. loss of hardcopy files or papers containing personal details;
c. the inadvertent sending of an email to the wrong recipient or disclosure of email addresses unauthorized in an email carbon copied to multiple recipients;
d. phishing, hacking or other external attacks on UNE's information repositories; and
e. unauthorized access by a staff member to files containing personal information.

(62) In certain cases UNE is also subject to the national Notifiable Data Breaches scheme, under the Privacy Act 1988 (Privacy Act) (CTH). This scheme establishes a mandatory notification for federal agencies and any agency collecting TFN's. In the circumstances of unauthorised access to TFN, UNE must make a mandatory report in less than 30 days if

the breach is likely to result in serious harm to an individual which could not be adequately prevented.

(63) An eligible data breach occurs when:

a. there is unauthorised access to or unauthorised disclosure of personal information, or a loss of personal information, that UNE holds (or which is held by a third party on our behalf);
b. that is likely to result in serious harm to one or more individuals, and
c. UNE has been unable to prevent the likely risk of serious harm with remedial action.

(64) If you become aware of any data breaches or suspect one has or may occur, please inform the UNE Senior Privacy and GIPA Officer as soon as possible. The Privacy Officer will then report the breach to IT security and other key stakeholders where appropriate. If staff members receive a report of such activity or suspect that breach activity is being described, they also hold a responsibility to report the incident to the Senior Privacy and GIPA Officer via privacy@une.edu.au.

Part D - Summary of Key Privacy Roles and Responsibilities

Roles	Responsibilities
Alumni	UNE Alumni should be aware how their personal information is collected and used by the University and how they may request further information or make a complaint about collection and usage, including when subscribing to or wishing to unsubscribe from mailing or other contact lists.
Chief Information Officer	Responsible for ensuring all reasonable steps are taken to ensure systems and information storage devices where UNE personal information is stored (including systems managed by UNE and those managed under arrangement with third parties) are managed in accordance with the Privacy Principles and UNE's Privacy Management Rule. Responsible for oversight of investigation of potential data breaches involving information systems in a manner commensurate with the severity of the potential breach and within the prescribed timeframes. Oversight of technological security.
Director of Governance and University Secretary	An escalation point for serious privacy matters, or if further review is required. Policy steward for the Privacy Management Rule.
Head of Records Policy & Governance	Responsible for ensuring effective Privacy management frameworks and support is in place at UNE which uphold Privacy Principles and ensure oversight of the entirety of Records, Policy, Privacy & Governance issues where they interrelate and where the maintenance of such issues impacts UNE's governance structures, and legislative compliance. An escalation point for some privacy matters.
Information Privacy Commission	The Information Privacy Commission (IPC) is the NSW Government Agency with responsibility for oversighting the implementation of Privacy laws in NSW. The IPC is responsible for reviewing voluntary and mandatory data breach notifications and privacy complaint appeals. The IPC has authority to provide UNE with directions regarding upholding privacy obligations, and may refer matters to a tribunal for a ruling. Email: ipcinfo@ipc.nsw.gov.au Phone: 1800 472 679
Audit Internal Review Officer	Internal Review Officers are appointed to undertake formal privacy complaint investigations, and are generally appointed for the period of the investigation only. Internal Review Officers are responsible for following correct administrative process for review of complaints including retaining confidentiality and independence.
Managers (faculty and operational areas)	Must ensure all staff are aware of their individual & group responsibilities to implement the Privacy Management Rule and promote a privacy culture at UNE.
NSW Ombudsman	The NSW Ombudsman may hear appeals regarding perceived administrative failures in the management of privacy complaints.

Roles	Responsibilities
NCAT – The NSW Civil and Administrative Tribunal	Individuals who are not satisfied with the findings of internal review or the actions taken (or proposed to be taken) by UNE can apply to the Administrative and Equal Opportunity Division of the NSW Civil and Administrative Tribunal (NCAT) for an external review.
Senior Executive	Responsibility for maintaining and promoting manager awareness of privacy responsibilities including ensuring key staff have undertaken training and that business processes are consistent with upholding privacy principles.
Students	Students have a responsibility to take reasonable steps to protect their private information and that of other students. Students should be aware how their personal information is collected and used by the University and how they may request further information or make a complaint about such collection and usage.
UNE Privacy Officer	Acts as the first point of contact for privacy related advice, queries, complaints or notifications of potential breaches, undertaking preliminary assessment of each matter and in depth assessment where required. Available to assist in the completion of Privacy Impact Assessments especially in complex or detailed projects where the management of personal information becomes an iterative part of the project. Key role in promoting a positive privacy culture, by advocating for privacy and supporting UNE Representatives to manage privacy compliance consistent with the Privacy Management Rule, the provision of training and specific assistance as required. Investigates complaints and is a part of the management of UNE's data breach response plan. Provides reports on compliance, breaches, and complaints (in general terms) as required internally to the Head of Records Policy and Governance and Director of Governance University Secretary and to external bodies such as the IPC. Responsible for maintaining a record of privacy related queries and outcomes.
UNE Representatives	UNE Representatives have a responsibility to promote a positive privacy culture at UNE which starts with being familiar with and adhering to UNE's Privacy Management Rule in the collection, storage, access, use and disclosure of personal information. UNE Representatives must take all reasonable steps to protect their private information and that of others, including following security protocols when undertaking day to day activities (including using social media). Individuals have a responsibility to report all suspected breaches of personal information and any privacy concerns. UNE Representatives should seek advice if they have questions or need support with regards to privacy related matters and treat personal information with integrity and respect by implementing security protocols in all circumstances.
UNE Representatives who collect, manage or use health information and/or medical records.	Have heightened responsibilities to ensure consent at collection, secure storage and appropriate access, management and use. Health information has a greater risk and thus must be treated with care.

Quality Assurance Measures

(65) Any privacy related instances will be recorded by the Privacy Officer and reported (anonymised where appropriate) in consultation with the Head of Records, Policy & Governance and the Director of Governance via the Senior Executive, relevant committees, bi annual compliance review and the UNE annual report. In addition:

a. A privacy Breach notice register will be established, keeping an up to date report of any breach activity whether reported externally to the Information and Privacy Commission or internally via committees or the Senior Executive, including mitigation strategies and improvements.
b. Substantial privacy breaches, will be reported to the Information and Privacy Commission as best practice when mandatory notification is not required.
c. A review of privacy training and education programs will be conducted periodically which considers any lessons learned from privacy requests, complaints, and any potential or actual breaches to ensure improvements in privacy outcomes.

d. Records of delivery of annual privacy training for existing staff and as part of new staff induction will be kept on a training register established to ensure a privacy culture is promoted and reinforced across UNE.
e. UNE will undertake to check the requirements of corporate record keeping prior to the destruction of any data and ensure ongoing compliance with the Records Management Rule & State Records Act 1998. A review of records kept will be conducted to measure compliance.
f. When storing personal information the collection of sufficient metadata will be assured to ensure UNE maintains the ability to confirm consent, accuracy and providence information of all types of personal information.
g. A register will be kept detailing the storage of personal information collected by or on behalf of UNE in hard copy and digital format including the type, format and location.
h. Regular reviews of the register will be undertaken to ensure UNE can effectively identify and manage personal information and mitigate privacy concerns.

Associated Documents

(66) The Privacy Management Toolkit provides additional support information and resources to assist UNE Representatives in the application of this Privacy Management Rule. Information includes a copy of UNE's Privacy Statement, forms (including the PIA and PITA), checklists, collection notice templates, factsheets relating to specific situations and personal information, links to training & support Information (e.g. Privacy Management Video and Privacy Management Induction) and to external resources (e.g. Storage and Protection of Tax File Number Requirements; Data Breach Notification Form; and to Privacy Related News and Updates).

(67) Preparing and responding to personal information data breach – Privacy Management Rule - Annexure 1 - Data Breach Policy

Part E - Authority and Compliance

(68) The Vice-Chancellor and Chief Executive Officer makes this Rule which has been approved by the UNE Council and has the effect of a Policy. The Director Governance and University Secretary is authorised to make supporting documents to aid the implementation of the Rule.

(69) This Privacy Management Rule:

a. has been informed by the Privacy and Personal Information Protection Act 1998 the Health Records and Information Privacy Act 2002 and any other applicable law including the Privacy Act 1988 (to the extent it applies); and
b. acknowledges the European General Data Protection Regulation (the GDPR) and its application to staff, students and alumni who are European citizens. The principles ascribed to the management of information for that cohort have been applied to the Rule and integrated into existing information wherever appropriate, to ensure a consistent, and well-considered 'privacy by design' approach to the management of personal information.
c. in the event of any inconsistency with applicable privacy legislation, the applicable privacy legislation prevails to the extent of the inconsistency.

(70) Privacy Act 1988 which governs the way that personal information is collected, used, disclosed, secured and accessed and requires the University to comply with the Australian Privacy Principles (APPs) applies in relation to:

a. Personal information the University collects and holds regarding student assistance provided by the

Commonwealth (which is an obligation under Section 19-60 of the Higher Education Support Act 2003; and

b. Tax file number information (in accordance with the Tax File Number Guidelines, a legislative instrument under the Privacy Act 1988.

(71) The PPIP Act and the HRIP Act, are underpinned by a suite of 'privacy principles' that act as a guiding framework for UNE's Privacy Management Rule:

a. The PIPP Act covers personal information other than health information, and requires the University to comply with the Information Protection Principles (IPPs). The IPPs cover the full 'life cycle' of information, from point of collection through to point of disclosure. They include obligations with respect to data security, data quality (accuracy) and rights of access and amendment to one's own personal information, as well as how personal information may be collected, used and disclosed;
b. The HRIP Act covers health- related personal information and requires the university to comply with the Health Privacy Principles (HPPs). Like the IPPs, the HPPs cover the entire information 'life cycle' but also include some additional principles with respect to anonymity, the use of unique identifiers and the sharing of electronic health records.

(72) Breaches of this Rule will be managed in line with the statements outlined in the policy. Individuals who deliberately breach privacy legislation may be personally liable for that action and attract legislative penalties under part 8 of the PPIP Act or the HRIP Act, or criminal prosecution under the Crimes Act 1900 (NSW). These penalties include fines of up to $11,000 or imprisonment of up to two years.

(73) This Rule operates as and from the Effective Date.

(74) Previous Privacy Statements, Privacy Management Rules and related documents, are replaced and have no further operation from the Effective Date of this new Rule.

(75) Notwithstanding the other provisions of this University Rule, the Vice-Chancellor and Chief Executive Officer may approve an exception to this Rule where it is determined that the application of the Rule would otherwise lead to an unfair, unreasonable or absurd outcome. Approvals by the Vice-Chancellor and Chief Executive Officerunder this clause must be documented in writing and must state the reason for the exception.

Section 2 - Definitions related to this Rule

(76) Collection (of personal information) means the way the University acquires the information (eg. by use of a written form, a verbal conversation, an online form, or taking a picture with a camera).

(77) Consent refers to the written consent from an individual for the University to undertake a particular action in relation to personal information, such as an additional use or disclosure to another party.

(78) Disclosure refers to the provision of personal information to a party or person external to the University. Provision of personal information internally may also be considered a disclosure where the personal information is about a staff member, or the information is health information.

(79) Health information has the meaning given to it in accordance with Section 6 of the Health Records and

Information Privacy Act 2002 (NSW).

(80) Holding of personal information: The University will be considered to be 'holding' personal information if it is in the University's possession or control, or if it is held by a contractor or service provider on the University's behalf.

(81) Personal information has the meaning given to it in accordance with Section 4 of the Privacy and Personal Information Protection Act 1998 (NSW).

(82) Unsolicited personal information is information that the University receives but has taken no active steps to collect. For example: an employment application sent to the University on an individual's own initiative and not in response to an advertised vacancy.

Status and Details

Status	Current
Effective Date	14th October 2022
Review Date	14th October 2023
Approval Authority	Director Governance and University Secretary
Approval Date	3rd June 2022
Expiry Date	To Be Advised
Unit Head	Susannah Warrick Director Governance and University Secretary swarrick@une.edu.au
Author	Alicia Zikan Privacy Officer +61267735190
Enquiries Contact	Susannah Warrick Director Governance and University Secretary swarrick@une.edu.au Records, Policy and Governance Unit