Privacy Management Rule

Section 1 - Overview

(1) This Rule has been developed under Section 29 of the University of New England Act, 1993. It has been informed by external legislation, being the Privacy Act 1988 (Cth), the Privacy and Personal Information Protection Act 1998 (NSW) (PPIP), the Health Records and Information Privacy Act 2002 (NSW) (HRIP) and any other applicable laws and is the University's reference instrument for meeting its obligations under these Acts.

(2) Any circumstance where personal information is collected, stored, used or disclosed in a manner that is not in accordance with the 'Privacy Management Principles' must be brought to the attention of the UNE Privacy Officer.

(3) For the purposes of Section 33 of the Privacy and Personal Information Protection Act 1998 (NSW), the Privacy Management Rule is also the University's Privacy Management Plan, demonstrating to the public and the University community, UNE's respect for the privacy of students, staff and others for whom we hold personal information.

Section 2 - Scope

(4) This Rule is binding for all UNE Representatives, as well as the University's decision-making and advisory bodies. It applies to all personal information and health information (including sensitive information) held by the University and its controlled entities.

(5) This Rule has been prepared in accordance with Section 33 of the Privacy and Personal Information Protection Act 1998(NSW).

Section 3 - Rule

Privacy Context

(6) UNE is an Australian public university, established and operating under the University of New England Act 1993 and its associated By-laws. The University holds a vast amount of personal information not only pertaining to the students we serve, but also relating to our staff, patients and those contributing to the teaching of University programs of study. The University will protect privacy with the use of this Plan as a reference instrument.

(7) As a NSW public sector agency responsible for the holding of personal information, the University must comply with the PPIP Act and HRIPA.

(8) In addition, 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)

(9) Each of the Acts (PPIPA, HRIPA and the Privacy Act 1988 (Cth) focus upon 'privacy principles':

a. The PPIPA covers personal information other than health information, and requires the University to comply with 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 HRIPAcovers 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; and
c. The Privacy Act regulates the way that personal information is collected, used, disclosed, secured and accessed. It requires the University to comply with the Australian Privacy Principles (APPs) in terms of the information in Section 8 (above).

(10) As an institution within the higher education sector of Australia, UNE is required to collect and manage a range of personal and health information about our staff, students, patients and those contributing to the teaching of University programs of study. Some information may also be collected for statistical purposes for use in University planning and for government reporting as required.

Privacy Management Principles

(11) The full life cycle of personal information handling at UNE (Click here for life cycle) is based upon University's privacy management principles. These are a combination of the IPPs, HPPs and the APPs. These principles are:

a. That collection of information is lawful, direct, relevant, open and transparent;
b. That information is stored securely, not kept any longer than necessary and disposed of appropriately;
c. That information is accurate and accessible to the person to whom it relates; and
d. That information collected for a particular purpose, is not used or disclosed for another purpose.

Collection of information

(12) Personal information is only collected by lawful and fair means and will be held by the University for the purpose it was provided, for purposes necessary to its functioning and for any secondary purposes associated with the functioning of the University. Those functions and the strategic goals to achieve them are outlined within the University of New England Act 1993 and the most recent iteration of the UNE Strategic Plan.

(13) Personal information is to be collected directly from the individual about whom it relates. When collecting personal information, the purpose for collection will be clearly explained and will not be collected from an individual without their consent, unless:

a. It is collected from a third party who can provide evidence that they have collected the information from the individual concerned, with their consent; or
b. It is collected from a parent or legal guardian of the individual concerned (in the event that the individual is under the age of 16 years); or
c. The individual is involved in a life threatening, health or other emergency; or
d. It is unreasonable or impractical to do so.

(14) In the cases referred to at 13(b - d) above, the decision to collect information, the rationale for doing so and the purpose for which it was required, should be formally documented and filed as a corporate record to clearly demonstrate that due diligence and appropriate processes have been followed to collect the information.

(15) Personal information is to be collected in an open and transparent manner. When the University for the purpose of undertaking its official functions and responsibilities collects personal information, the University must ensure transparency of purpose confirming that those concerned are aware of the following (either at the point of collection or as soon as possible thereafter):

a. The purpose for which the information is being collected (which should relate to the key functions of the University);
b. The intended recipients of the information;
c. Whether the information collected is required by law or is being requested on a voluntary basis. If information is requested on a voluntary basis, participants must be provided with a means to 'opt out'.
d. Any consequences that might arise as a result of not providing information upon request;
e. Any third parties that might also be entitled to this information, including whether the University is likely to disclose the personal information to recipients from other jurisdictions;
f. The existence of any right of access to, or correction of the information by the individual concerned;
g. Information about where the collected material will be held and by whom; and
h. Information about how an individual may lodge a privacy complaint.

(16) Personal information must only be collected when it is relevant to the activities and functions of the University. It should be accurate, complete and up-to-date and limited (ie. not excessive). Collection of personal information must not unreasonably intrude into the personal affairs of an individual.

(17) When dealing with the University, an individual must have the option of not identifying himself or herself, or of using a pseudonym should they wish. However, this option would not be feasible and does not apply if the University:

a. Is required or authorised by or under an Australian law, or a court order, to deal with specific individuals; or
b. Finds it impractical to address the issues raised by the individual without knowing their true identity.

(18) Where it is not necessary to identify the person that information relates to (for example, if information is being collected via a show of hands, survey tools, generic data generation) then information should be collected in such a way as to ensure anonymity. This may include the use of unique identifiers (eg. numbers) if it is reasonably necessary to differentiate one person's response from another's in order to carry out your functions efficiently.

Special protocols - Health Information

(19) Health related personal information will only collected from the person concerned, unless it is unreasonable or impracticable to do so (see 17 above).

(20) If health information about a person is collected from a third party, the University must take reasonable steps to notify the person that this has occurred.

Special protocols - Sensitive Information

(21) Sensitive information cannot be used for direct marketing.

(22) Sensitive information cannot be shared by related bodies corporate in the same way that they may share other personal information.

Special protocols - other

(23) When collecting personal information from an individual using online or hard copy media (or face-to-face) reference will always be made to the UNE Privacy Management Rule in writing or verbally (whichever is appropriate).

Special exemptions

(24) Unsolicited information: If unsolicited personal information is received by UNE from another organisation, it should be determined whether the University would have been permitted to have collected the information in any case, under the APPs. If not, the University should de-identify the information or dispose of it using secure means outlined within its Records Management Rule.

(25) Information collected before 1 July 2000 (as the PPIPAdoes not apply to material collected before this date).

Key message - Personal information gathered via the use of UNE online systems/websites

(26) Whilst visitors to the UNE website are able to access the site anonymously and to access information without revealing their identity, the University may collect information about visitors to sites via the use of cookies or other automated means including server logs. A cookie is a packet of data that a website puts on a visitor's computer's hard disk to identify them as a visitor to that site for a limited time. This information could include: your server address; your domain name; your IP address; the date, time and duration of your visit; the page accessed before your visit to our site; the pages accessed and documents downloaded from our site; the previous site visited; the type of browser you used. You may choose to disallow cookies through your web browser settings.

(27) UNE may embed a link to a third party site, within a webpage. Where this is the case, the UNE site operates as a launching page to the third party site. The third party site will have its own privacy statement or other relevant information which may deal with personal information differently to the UNE Privacy Management Rule.

(28) Information that an individual may disclose in online forums or other interactive media associated with the University is considered public information by both UNE and common law and is not protected under the PPIPA.

Key message - Email

(29) If you send us a message, the University will record your email address. This email address will only be used for the purpose in which you have provided it (and it will not be disclosed to anyone without your consent). Some email traffic may be de-identified and monitored for statistical and quality purposes.

Key message - Human Resource Services (HRS)

(30) Prospective staff who may be applying for a vacant position at UNE, include a range of personal information as part of their job application. This material has been provided to the University for a specific purpose and is kept for the duration of the recruitment process associated with the role that the person had applied for. Once the recruitment has been finalised, all applicants will be notified using the contact details provided to HRS and the applications for unsuccessful candidates will be destroyed.

Key message - Publishing to the UNE website, photography, filming and media

(31) Staff may be engaged in filming or photo activity at events held by the University or may participate in and use image media for promotional purposes. When we take photos or film events, we will always seek permission of people (including our own staff) before we include them in captured media and we will advise how we will manage that information. We will ask people to sign a consent form for this purpose and the images will only be used for that purpose and will be kept securely in our corporate records management system. We will also respect the wishes of those who do not wish to be photographed or filmed.

Key message - Public seminars and conferences

(32) When UNE units delivers or participates in seminars, conferences or other events, we will consider our privacy obligations when organising these events and aim to notify affected people how we will manage their personal and health information if we collect it, such as on registration forms.

(33) If an event management company assists the University with delivering an event, UNE will ensure that company has appropriate privacy management practices in place.

Storage of information

(34) Personal information collected by the University, will be stored securely. It is to be protected from misuse, interference and loss, from unauthorised access, modification or disclosure; retained as a corporate record in accordance with the University's Records Management Rule and the State Records Act, 1998 (NSW).

(35) Schools and business units should only store personal information locally for as long as it is necessary to support the purpose it was collected for. Personal information held in corporate record systems (eg. Callista, SRMs, TRIM, LMS, Alesco etc.) is not to be stored locally.

(36) 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 Commonwealth record and not required by or under an Australian law, or court/tribunal order) the information should be de-identified or destroyed in a secure manner, in accordance with the University's Records Management Rule.

Special protocols - Health Information

(37) No

Special protocols - Sensitive Information

(38) No

Special protocols - Other

(39) No

Special exemptions

(40) No

Key messages

(41) No

Access and Accuracy

(42) The University upon request by an individual, will provide them with access to their personal information:

a. Within a reasonable period after the request is made;
b. Without expense to the individual for general record keeping purposes (unless the access is being sought in accordance with a formal GIPA request); and
c. For the purposes of amending their personal information to ensure accuracy.

(43) If the University holds personal information about an individual it must, upon the individual's request, give them access to that information (and within a reasonable period after the request is made) unless:

a. The University believes that giving access would pose a serious threat to the life, health or safety of any individual, or to public health or safety; or
b. Giving access would have an unreasonable impact on the privacy of other individuals; or
c. The individual's request for access was frivolous or vexatious; or

d. The information relates to existing or anticipated legal proceedings between the University and the individual; or
e. Giving access would reveal the intentions of the University in relation to negotiations with the individual in such a way as to prejudice those negotiations; or
f. Giving access would be likely to prejudice one or more enforcement related activities conducted by or on behalf of, an enforcement body; or
g. Giving access would reveal evaluative information generated within the University, in connection with a commercially sensitive decision-making process; or
h. Giving access would be unlawful; or
i. Denying access is required or authorised by or under an Australian law or a court/tribunal order; or
j. Both of the following apply:
    i. The University has reason to suspect that unlawful activity, or misconduct of a serious nature that relates to the University's functions or activities has been, is being or may be engaged in; and
    ii. Giving access would be likely to prejudice the taking of appropriate action in relation to the matter.

(44) If the University refuses to provide an individual with access to their personal information for any of the reasons outlined above, the University must advise the individual in writing, outlining:

a. The reasons for the refusal (unless given the grounds for refusal, it would be unreasonable to do so); and
b. The mechanisms available to the individual, to complain about the refusal (at Privacy Complaints Section of this Rule).

(45) If the personal information has been shared with a third party for purposes of the University conducting its business, the University will advise the third party of the amendment unless it is impractical or unlawful to do so.

(46) UNE systems should enable individuals to maintain the accuracy of personal information held about them. Access may be provided securely via an online login and password system, or where this is unavailable, via the appropriate and available UNE forms and associated procedures.

Special protocols - Health Information

(47) No

Special protocols - Sensitive Information

(48) No

Special protocols - Other

(49) Where it is not possible to amend or correct personal information (eg. 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 (eg. 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.

Special exemptions

(50) As per Section 43 above.

Key messages

(51) No

Use and disclosure

(52) The use and disclosure of personal information will be limited by the University and restricted to the purpose for which it was collected, unless the individual to whom the information relates, provides their consent or the use of the information directly relates to the purpose for which it was collected or, the information is provided to a third party in order to prevent or lessen a serious or imminent threat to any person's health or safety.

(53) In addition, the University may collect, use and disclose personal information where it is required, authorised or permitted by legislation, a court order or other enforcement body to do so. The University must ensure that all requests for disclosure will be in writing (and where applicable on corporate letterhead). Specific details relating to New South Wales, Commonwealth or other jurisdictions, are outlined within 'Special Protocols' at Clauses 56 - 61 of this Rule).

Special protocols - Health Information

(54) No

Special protocols - Sensitive Information

(55) Sensitive information must be safeguarded and will not be disclosed unless the disclosure is necessary to prevent a serious and imminent threat to the life or health of the individual concerned, or another person.

Special protocols - Other

(56) Personal information must not be disclosed to any person or body who is in a jurisdiction outside New South Wales or to a Commonwealth agency unless:

a. It is legally required via an Australian law, court/tribunal order or enforcement agency and presented to the University in writing (and on corporate letterhead);
b. A relevant privacy law that applies to the personal information concerned is in force in that jurisdiction or applies to that Commonwealth agency; or
c. The disclosure is permitted under a relevant Privacy Code of Practice (Part 3, Division 1 of the PIPPA).

(57) Where the University engages a third party contractor to undertake functional activities (eg. mailing houses, IT support agencies, online voting services, specialist contractors) UNE's privacy obligations also apply to the third party and must be incorporated into any contract or contractual obligations between them and the University.

(58) Personal information must not be used or disclosed for the purpose of direct marketing, unless:

a. It has been made clear to the individual at the time of collecting the information, that it would be used for direct marketing purposes; and
b. The University provides individuals with a simple means by which they may easily consent to or request not to receive any further direct marketing communications.

(59) In each direct marketing communication with the individual, the University is to include a statement that an individual may request to not receive any further direct marketing communique (eg. via an unsubscribe option for online marketing channels).

(60) If the University intends to disclose personal information to third party marketing organisations, it must explain its intention and ensure individuals have an option to not take part in third party operations.

(61) Disclosure of personal information to recipients (also referred to as 'cross-border' disclosures) in other jurisdictions:

a. The University must take reasonable steps to ensure that any entity in receipt of personal information from its records, does not breach the APPs in relation to the management and use of that information.
b. Personal information will not be disclosed to entities associated with other jurisdictions unless the disclosure had been requested when the information was collected, and the individual concerned had consented to its disclosure. Personal information may be disclosed however, if:
    i. It is required or authorised in writing (and on corporate letterhead) by or under an Australian law or a court/tribunal order, or an enforcement body;
    ii. The overseas entity is an agency and:
        - the disclosure of the information is required or authorised by or under an international agreement relating to information sharing to which Australia is a party; or
        - the entity reasonably believes that the disclosure of the information is reasonably necessary for one or more enforcement related activities conducted by or on behalf of an enforcement body and the recipient is a body that performs functions or exercises powers that are similar to those performed or exercised by an enforcement body.

Special exemptions

(62) As per Section 43 above.

Key message - Online forums or other interactive/social media

(63) Information disclosed in online forums or other interactive/social media (including chat rooms, discussion forums, message boards, news groups, blogs etc.) is considered by common law to be public information. Engaging with these online communication channels is an opt-in event and it is important that any UNE representative considering developing or joining an online forum understand that owners of forum sites will require details (eg. your email address, name etc.) to be transmitted to third parties. Staff and students as a result of their association with the University should exercise caution when engaging with online communication channels and social media and when posting material should ensure that they do not post any confidential information, or material that has the potential to damage the reputation of the University or others. UNE representatives should refer to policy information surrounding the social media environment (via the UNE Social Media Policy) in relation to this issue.

Key message -Mailing and contact lists

(64) The University and individual units within the University may keep subscriber, mailing and contact lists that contains personal information. The lists will not be used for any other reason than those explained to subscribers when they were invited to join the list and the University requested and received their consent to include their personal information within it. With each piece of promotional or other correspondence generated using the mailing/contact list, the University will also include an 'opt-out' provision, to allow subscribers to unsubscribe should they wish.

Privacy complaints

(65) The University's Privacy Officer should be informed of all privacy complaints, including potential breaches of privacy, that are associated with the University and its controlled entities in the management of its operations and obligations.

(66) Informal complaints are addressed in the first instance, by the Head of School or business unit in collaboration with the UNE Privacy Officer. Informal complaints regarding a breach of privacy in relation to the management of an individual's personal information should be made known to the Head of School or business unit as soon as possible (and within 60 days of the individual becoming aware of the breach).

(67) Formal complaints requesting that the University undertake an internal review of any alleged breach relating to its management of personal and private information should be forwarded directly to the UNE Privacy Officer. These will be investigated in accordance with the requirements of Privacy and Personal Information Protection Act, 1998(NSW).

(68) UNE representatives are to fully cooperate with any privacy-related investigation, providing access to any relevant or requested documentation as requested. Where UNE representatives are aware of 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.

(69) 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 UNE's Public Interest Disclosures Rule and its associated procedures.

(70) The UNE Privacy Officer is contactable via email, at: privacy@une.edu.au

Authority and Compliance

(71) The UNE Council, pursuant to Section 29 of the University of New England Act, makes this University Rule.

(72) University Representatives must observe it in relation to University matters.

(73) The Rule Administrator is authorised to make procedures and guidelines for the operation of this University Rule. The procedures and guidelines must be compatible with the provisions of this Rule.

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

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

(76) Notwithstanding the other provisions of this University Rule, the Vice-Chancellor 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 under this clause must be documented in writing and must state the reason for the exception.

Section 4 - Definitions

(77) Collection (of personal information) means the way the university acquires the information, for example: a written form, a verbal conversation, an online form, or taking a picture with a camera.

(78) 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.

(79) 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.

(80) Effective Date is the date on which this Rule will take effect.

(81) 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 our behalf. Most of the privacy principles apply to when the University is 'holding' personal information, which means we remain responsible

for what our contractors or service providers do on our behalf.

(82) Personal information refers to information or an opinion (including information or an opinion forming part of a database and whether or not recorded in a material form) about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion. It includes such things as:

a. a person's name, address, information about a person's family life, information about a person's sexual preferences, financial information, photos, contact details, opinions, health conditions or illnesses, housing or tenancy information, work history, education and criminal histories;
b. an individual's fingerprints, retina prints, body samples or genetic characteristics;
c. payroll details, information about next of kin, emergency contacts, superannuation fund and tax file numbers.
d. Health information, incorporating information or opinions about:
    i. The physical or mental health or a disability (at any time) of an individual, or
    ii. An individual's express wishes about the future provision of health services to him or her, or
    iii. A health service provided, or to be provided, to an individual, or
    iv. Other personal information collected to provide a health service, or in providing a health service, or in connection with the donation of human tissue; or
    v. Genetic information that is or could be predictive of the health of a person or their relatives or descendants.
e. Some things (such as information about an individual who has been dead for more than 30 years and information about an individual that is contained in a publicly available publication) are exempt from the definition of "personal information" and these are listed in full, under Section 4(3) of the PPIPA.

(83) Sensitive personal information relates to information about a person's racial or ethnic origin, political perspectives, religious/philosophical beliefs, sexual activities or union membership.

(84) UNE Act means the University of New England Act1993 No 68 (NSW).

(85) UNE Representative means a University employee (casual fixed term and permanent), student, contractor, agent, appointee, UNE Council member, adjunct, visiting academic and any other person engaged by the University to undertake some activity for or on behalf of the University. It includes corporations and other bodies falling into one or more of these categories.

(86) 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	Historic
Effective Date	1st October 2015
Review Date	1st October 2018
Approval Authority	Vice-Chancellor and Chief Executive Officer
Approval Date	18th September 2015
Expiry Date	26th September 2016
Unit Head	Kate McNarn Director Governance and University Secretary
Author	Leanne Nisbet
Enquiries Contact	Records, Policy and Governance Unit