Privacy Management Plan

Section 1 - Audience

(1) This policy applies to University staff, contractors, controlled entities, conjoints, volunteers, affiliates and the general public.

Section 2 - Introduction

(2) This Privacy Management Plan (Plan) details how the University of Newcastle manages personal information of staff, students and the general public in their dealings with the University.

(3) Section 33 of the Privacy and Personal Information Protection Act 1998 (NSW) (PPIP Act) requires the University to implement a Privacy Management Plan.

(4) The University supports compliance with the PPIP Act and the Health Records and Information Privacy Act 2002 No 71 (the HRIP Act) by:

a. informing individuals how their personal information will be handled by the University;
b. informing individuals of their rights under the legislation;
c. confirming a culture of privacy awareness across the University so that staff are aware of their responsibilities under the legislation; and
d. considering the Information Protection Principles and Health Privacy Principles, where relevant, in the design and/or review of processes, systems and projects undertaken or implemented by the University.

(5) University policies and processes that support this Plan are listed in Appendix 3.

Section 3 - Public Registers Maintained by the University

Graduation Book

(6) The University publishes graduation books which include the name of each graduate and the degree completed. Students may opt out of inclusion by contacting graduation@newcastle.edu.au.

Contracts Register

(7) The University maintains and publishes a Contracts Register as required by the Government Information (Public Access) Act 2009 (NSW) (GIPA Act). It is unlikely the register will include personal or health information.

(8) The Privacy Officer may be contacted with any concerns about information published as it relates to a person's personal or health information via email at privacy@newcastle.edu.au.

Section 4 - Protection and Privacy Principles

(9) This Plan is prepared based on the 12 Information Protection Principles (IPPs) and 15 Health Privacy Principles (HPPs) in the PPIP Act and HRIP Act respectively.

(10) The IPPs can be found on the NSW Informaton and Privacy Commission - Information Protection Principles webiste. The HPPs can be found on the NSW Information and Privacy Commission - Fact Sheet Health Privacy Principles website.

(11) The University is governed by NSW privacy legislation.

(12) Particular functions or Commonwealth funded research projects may also be governed by the Australian Privacy Principles (APPs) which are outlined in the Privacy Act 1988 (Privacy Act). The APPs can be found online (Australian Privacy Principles).

(13) Certain information (such as Tax File Numbers) is expressly governed by the Privacy Act.

Section 5 - Information Collection

Lawful Collection

(14) The University may only collect personal and health informations for a lawful purpose, where it is needed for and directly relates to the University's activities.

(15) Personal or health information may be collected and used by the University for purposes including:

a. providing courses of study; conferring degrees and other awards;
b. research;
c. exercising commercial functions;
d. fundraising;
e. promoting events and students;
f. surveys and competitions;
g. news and updates;
h. selection, employment, appraisal and remuneration of staff;
i. providing accommodation for students;
j. providing support services such as counselling/disability services or advocacy services;
k. managing complaints or disputes;
l. managing or facilitating scholarships; and/or
m. managing requests for academic consideration.

(16) Appendix 4 contains examples of University functions for which the University may collect personal or health information.

Direct Collection

(17) Personal or health information is collected directly from the individual to whom the information relates, unless:

a. the individual has authorised collection of the personal information from someone else;
b. the personal information is provided by a parent or guardian of a person who is under the age of 16 years; or

c. for health information, if it is unreasonable or impracticable to do so.

(18) Where the University collects personal or health information from another individual, agency or party, consent may be obtained by the individual:

a. accepting terms and conditions;
b. entering into a contract; or
c. providing valid and express consent.

(19) Another party may manage consent and authorisation for the provision of personal or health information prior to the information being provided to the University. This may include where a student authorises another tertiary institution to provide the information to the University.

Open Collection

(20) At the time of collecting personal or health information, or as soon as possible afterwards, the University must inform the individual/s concerned about:

a. why it is collecting the information;
b. the use;
c. who else might see it;
d. how they can view and correct their personal information;
e. whether the information is required by law or is voluntary; and
f. any consequences if they decide not to provide the information.

(21) This advice may be provided by way of:

a. terms and conditions;
b. collection notice on a form or agreement;
c. published privacy notice;
d. correspondence (i.e. email communication or file note).

Relevance of Collection

(22) The University aims to ensure that:

a. personal and health information is relevant, accurate, complete, up-to-date, not excessive and that collection does not unreasonably intrude into the personal affairs of the individual;
b. information is not collected or unnecessarily duplicated and that databases and systems are maintained and reviewed to ensure information is accurate;
c. processes are in place and are easily identifiable for individuals to update or amend their information; and
d. only information required is sought (this will depend on the purpose for which the information is collected).

Section 6 - Storage, Protection and Disposal of Personal information

(23) The University protects personal or health information by:

a. identifying and classifying records and handling them accordingly;

b. storing records in University approved systems (appropriate privacy and security measures are incorporated into agreements with external system providers or contractors);
c. ensuring access to systems or databases containing personal information is only granted on a need to know basis and that these systems are password protected;
d. ensuring that, wherever available, systems established to collect information are used effectively;
e. ensuring information within systems is only accessed or viewed as required for a University function;
f. ensuring information is only transferred between parties when it is necessary to fulfil a University function and that steps are taken to prevent accidental disclosure;
g. storing paper records securely, for example, in locked offices or cabinets, as appropriate;
h. ensuring information is destroyed securely, that is, paper records are shredded or placed in a confidential bin, and electronic systems are erased;
i. ensuring information is not kept for longer than is necessary.

(24) Examples of systems used by the University to manage or hold personal information is included in Appendix 5.

Section 7 - Information Access and Accuracy

Transparency

(25) An individual may obtain details on:

a. how their personal or health information is being stored;
b. why it is being used; and
c. any rights they have to access it.

(26) This information will generally be available at the time of collection, via University systems, or upon request as appropriate.

Accessibility and Accuracy

(27) Personal or health information will generally be provided informally, via an existing process or on request. In some cases an administrative fee may be required (for example, student transcripts are available for purchase).

(28) Staff and students may generally correct or amend their personal or health information automatically or routinely. In cases where personal or health information cannot be provided or corrected and amended electronically or by contacting the officer involved, assistance may be sought from:

a. Human Resource Services Support for requests from staff; or
b. Student Central for requests from students.

(29) In response to a request, the University may amend an individual's personal or health informations or make an annotation on the document to detail the request. If the University considers that the personal or health information held is correct and does not require amendment, information will be provided advising the reasons for this decision.

(30) Requests for correction or amendment of personal or health information may also be sent to the Privacy Officer for advice or action as appropriate. In certain cases, requests may be referred for action under the GIPA application process. Such cases include where the information:

a. contains personal or health information about another individual;
b. may require further consideration and advice; or

c. is held across several different units of the University.

Section 8 - Information Use

Accuracy

(31) The University takes reasonable steps to verify personal or health information and follows relevant processes relating to evidence required before using information, especially where the use of the information could lead to negative consequences for the individual.

Limitation

(32) The use of personal or health informations primarily refers to its use within the University.

(33) Where personal or health information is to be used for a directly related purpose that is not the original purpose, staff should take reasonable steps to identify and document as appropriate why they have considered that use to be directly related to the original purpose.

(34) In considering whether a purpose is directly related to the original purpose, staff may consider the reasonable expectations of an individual.

Section 9 - Information Disclosure

Restricted and Limited Disclosure

(35) Disclosure primarily refers to sharing information held by the University with another agency or individual outside of the University.

(36) Staff should undertake reasonable actions to ensure that personal or health information is not disclosed, either routinely or on a single occasion, without the knowledge of the individual, unless an exemption applies.

(37) Individuals would likely be considered to have knowledge of a disclosure if:

a. there is documentation to indicate the individual provided valid consent;
b. they were made aware that the information may be disclosed on collection; or
c. there is a clear policy or process indicating that information of that type is usually disclosed.

Safeguarded

(38) University staff should undertake reasonable actions to ensure that any sensitive personal information (such as information about ethnic or racial origin; political opinions; religious or philosophical beliefs; sexual activities or trade union membership) is not disclosed without an individual's consent.

(39) The University may only disclose sensitive information without consent to deal with a serious and imminent threat to any individual's health or safety.

Section 10 - Information Identifiers and Anonymity

(40) Individuals may be identified by using unique identifiers if it is reasonably necessary to carry out University functions efficiently.

(41) Services may be provided anonymously, where lawful and practicable.

(42) The University will generally require information about an individual to deliver a service. However anonymity may be allowed wherever possible.

Section 11 - Information Transferrals and Linkages

(43) Health information may be transferred outside New South Wales if:

a. the recipient is subject to privacy principles that are substantially similar;
b. the individual consents to the transfer;
c. the transfer is necessary for the performance of a contract (either between the individual and the University or in the interests of the individual if the contract is between the University and a third party);
d. the information is required to prevent or lessen a serious or imminent threat; or
e. the use is authorised or required by another law.

(44) Health records linkage systems may only be used if the individual has provided or expressed their consent.

(45) Where the University seeks to use or disclose health information without the individual's consent, research proposals must be submitted to the Human Research Ethics Committee.

Section 12 - Law Enforcement Agencies

(46) The University requires law enforcement agencies to present a warrant, notice to produce or subpoena where they require the University to disclose personal information. All warrants, notices to produce and subpoenas must be served to the University's Legal & Compliance unit.

(47) The University may exercise discretion and provide personal or health information to a law enforcement agency if legislation permits it to do so in the particular circumstances.

(48) This discretion may be exercised by:

a. the Vice-Chancellor;
b. the Deputy Vice-Chancellor (Academic) and Vice President where the information relates to a student or former student; or
c. the Chief People and Culture Officer, where the information relates to a staff member or former staff member.

Section 13 - System Design and Review

(49) Staff should consider the requirements of the IPPs and HPPs when implementing or reviewing a project, process or system to identify issues and implement strategies to address those issues.

Section 14 - Training and Awareness

(50) Information on the University's Training and Awareness programs is included in Appendix 7.

Section 15 - Complaints or Review

(51) Individuals may raise concerns and complaints about the way in which the University has handled their personal or health information. A privacy complaint will be considered under the University's complaint handling processes.

(52) An individual may also request that the University undertake an internal review of the University's handling of their person or health information by completing the internal review form.

(53) Individuals may lodge a complaint with the Information and Privacy Commission New South Wales or seek an external review with the NSW Civil and Administrative Tribunal at:

NSW Privacy Commissioner GPO Box 7011 SYDNEY NSW 2001 Phone: 1800 472 679 Email: ipcinfo@ipc.nsw.gov.au	NSW Civil and Administrative Tribunal PO Box K1026 HAYMARKET NSW 1240 Phone: 1300 006 228

(54) Further information on privacy complaints and the Internal Review process is set out in Appendix 6.

Section 16 - Breach of a Principle

(55) Where the University becomes aware of a breach, it will take appropriate steps to identify and address the breach. Reports of breaches or potential breaches should be sent to the Privacy Officer at privacy@newcastle.edu.au who will advise the Vice-Chancellor accordingly.

Section 17 - Controlled Entities

(56) Controlled entities must manage personal and health information in accordance with this Plan. Controlled entities may also have other requirements under the Australian Protection Principles and/or other legislation.

(57) If a complaint or internal review is received by the University about the conduct of a controlled entity, the University may conduct a review if necessary.

Section 18 - Administration

(58) An issues register is maintained by the Privacy Officer to support the review process. Issues or feedback may be e-mailed to privacy@newcastle.edu.au.

Section 19 - Suggested Review Process

(59) This Plan will be reviewed within three years of approval.

Status and Details

Status	Historic
Effective Date	24th October 2017
Review Date	31st December 2019
Approval Authority	Vice-Chancellor
Approval Date	24th October 2017
Expiry Date	19th October 2021
Responsible Executive	David Toll Chief Operating Officer
Enquiries Contact	Legal and Compliance

Glossary Terms and Definitions

"Graduate" - (Noun) Has the same meaning as in section 3(2) of the University of Newcastle Act 1989.

"University" - The University of Newcastle, a body corporate established under sections 4 and 5 of the University of Newcastle Act 1989.

"Award" - When referring to a University qualification, this term means an academic qualification approved by Academic Senate that is conferred when a student has met the relevant program requirements. For all other uses of this term, the generic definition applies.

"Complaint" - As defined in Australian/New Zealand Standard - Guidelines for complaint management in organisations.

"Controlled entity" - Has the same meaning as in section 16A of the University of Newcastle Act 1989.

"Law" - All applicable statutes, regulations, by-laws, ordinances or subordinate legislation in force from time to time anywhere in Australia, whether made by the Commonwealth, a State, a Territory or a local government and, where the context permits, includes the common law and equity.

"Personal information" - Has the same meaning as in the Privacy and Personal Information Protection Act 1998 (NSW).

"Student" - A person formally enrolled in a course or active in a program offered by the University or affiliated entity.

"Disability" - As defined by the Disability Discrimination Act 1992 (Cth) (as amended from time to time, or as per any replacing legislation).

"Dispute" - Any dispute, difference or issue between the parties concerning or arising out of or in connection with or relating to an agreement or the subject matter of an agreement or the breach, validity, rectification, frustration, operation or interpretation of an agreement.

"Exemption" - When referring to a student's learning pathway, exemption means being excused from undertaking preparatory subjects, units, modules or competencies in a course or program, while still being required to undertake the same number of subjects, units, modules or competencies as would be completed if an exemption had not been granted. For all other uses of this term, the generic definition applies.

"Health information" - As defined in the Health Records and Information Privacy Act 2002, or any replacing

legislation.

"Staff" - Means a person who was at the relevant time employed by the University and includes professional and academic staff of the University, by contract or ongoing, as well as conjoint staff but does not include visitors to the University.

"Term" - When referring to an academic period, term means a period of time aligned to an academic year for the delivery of a course in which students enrol and for which they are usually charged fees for example semesters, trimesters, summer, winter or full-year term. The academic year for a term is determined by the academic year in which the course commences, not concludes. For all other uses of this term, the generic definition applies.

"Third party" - A person or group other than the University or any of the University's partner institutions.