Privacy Management Plan

Section 1 - Audience

(1) This Privacy Management Plan (Plan) applies to University of Newcastle (University) staff, contractors, controlled entities, volunteers, affiliates and the general public.

Section 2 - Introduction

(2) This Plan details how the University manages personal information of staff, students, and the general public in their dealings with the University, and is a supporting document to the Privacy Policy. The Privacy Policy establishes the Privacy Officer function within 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 is committed to 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. establishing and maintaining 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.

Section 3 - Public Registers Maintained by the University

Graduation Book

(5) The University publishes graduation books which include the name of each graduate and the degree conferred upon them. Students may opt out of inclusion in such graduation books by contacting graduation@newcastle.edu.au

Contracts Register

(6) 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.

(7) 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

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

(9) The University is governed by NSW privacy legislation but may have obligations under other legislation such as the Privacy Act 1988 (Cth) and the General Data Protection Regulation (EU 2016/679).

(10) Particular functions or Commonwealth funded research projects may be governed by the Australian Privacy Principles(APPs) which are outlined in the Privacy Act 1988 (Privacy Act).

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

Section 5 - Information Collection

Lawful Collection

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

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

a. providing courses of study (including all associated administrative processes); conferring degrees and other awards;
b. research and administration of higher degree by research candidature;
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 and associated administrative processes for the management of staff;
i. providing and administering 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.

Direct Collection

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

a. the individual has authorised the 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, it is unreasonable or impracticable to do so.

(15) Where the University collects personal or health information from another individual, agency or party, consent

may be obtained by the individual to whom the information relates:

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

(16) Another party may manage the 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 information to the University.

(17) The University may collect personal or health information indirectly where:

a. the information is collected in connection with actual or anticipated proceedings before any court or tribunal;
b. the University is investigating a complaint which has or may be referred to, or made to or from an investigative agency;
c. direct collection of the personal or health information would prejudice the interests of the individual to whom the information relates; or
d. indirect collection is otherwise authorised or required.

Open Collection

(18) 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.

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

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

Relevance of Collection

(20) The University aims to ensure that personal information and health information:

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

Section 6 - Storage, Protection and Disposal of Personal Information

(21) The University protects personal information and 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 authorised to be destroyed and destroyed securely, that is, paper records are shredded or placed in a confidential bin, and electronic systems are erased; and
i. ensuring information is not kept for longer than necessary.

(22) The University comprises a number of colleges, schools, divisions, and business units who each may hold information in electronic format, hard copy, or both depending on their individual practices and procedures. These practices and procedures will be subject to the University's overarching policies which determine how the University will use, manage, secure, and dispose of information which may include personal or health information, including but not limited to:

a. this Plan;
b. Records and Information Management Policy;
c. Information Technology Conditions of Use Policy;
d. Information Security Policy; and
e. Research Data and Primary Materials Management Procedure.

Section 7 - Information Access and Accuracy

Transparency

(23) 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.

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

Accessibility and Accuracy

(25) Personal or health information collected by the University may be provided to the person to whom the information

relates either informally, via an existing process, or on request. In some cases an administrative fee may apply (for example, student transcripts are available for purchase).

(26) 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 for requests from staff; or
b. Student Central for requests from students.

(27) In response to a request, the University may amend an individual's personal or health information 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, the individual will be provided with information outlining the reasons for this decision.

(28) 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

(29) The University takes reasonable steps to verify the accuracy of personal or health information, especially where the use of the information could lead to negative consequences for the individual.

Limitation

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

(31) The University must not use information it holds for a purpose other than for which it was collected, unless:

a. the individual to whom the personal information relates has consented to the use of the personal information for another purpose;
b. the other purpose for which the information is to be used is directly related to the purpose for which the personal information was originally collected; or
c. the use of the personal information is necessary to lessen or prevent a serious and imminent threat to the life or health of any individual.

(32) Where personal or health information is to be used for a purpose that is directly related to the original purpose, staff should take reasonable steps to identify and document, as appropriate, why they have considered the use is directly related to the original purpose.

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

Section 9 - Information Disclosure

Restricted and Limited Disclosure

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

(35) The University and its staff must undertake reasonable actions to ensure that personal or health information is not disclosed, either routinely or on a single occasion, without consent, unless:

a. the individual concerned is reasonably likely to have been aware, or has been made aware at collection, that personal information of that kind is usually disclosed to another person or body;
b. the disclosure is directly related to the purpose for which the personal information was collected and the University has no reason to believe that the individual concerned would object to the disclosure;
c. the disclosure of the personal information is necessary, on reasonable grounds, to prevent or lessen a serious and imminent threat to the life or health of any individual; or
d. an exemption applies under the Privacy and Personal Information Protection Act 1998 No 133 or Health Records and Information Privacy Act 2002 No 71.

(36) 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.

(37) The University must not use or disclose health information for another purpose (secondary purpose) other than the original purpose for which it was collected unless:

a. an exception at law applies;
b. the individual has provided consent;
c. the secondary purpose is directly related to the original purpose and within the expectations of the individual; or
d. there is reasonable belief that the use or disclosure is necessary to lessen or prevent a serious and imminent threat to the life or health of the individual concerned or another person, or a serious threat to public health and safety.

Safeguarded

(38) University staff must 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 and personal information (where relevant) may be transferred outside New South Wales if:

a. the University reasonably believes that the recipient is subject to a law, binding scheme, or contract in relation to privacy principles that are substantially similar to those detailed in the PPIPA Act;
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;
e. the use is authorised or required by another law;
f. the transfer is for the benefit of the individual and it is impracticable to obtain the consent of the individual to that transfer, and the individual would otherwise be likely to give consent; or
g. the University has taken reasonable steps to ensure that the transferred health or personal information will not be held, used, or disclosed by the recipient inconsistently with the Information Protection Principles or Health Privacy Principles.

(44) Health record 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 or personal information for research purposes without the individual's consent, the research proposal must be submitted and approved by the Human Research Ethics Committee prior to the use or disclosure of information.

Section 12 - Law Enforcement Agencies

(46) The University will only disclose personal information or health information to law enforcement agencies in circumstances where it is required or permitted to do so by law. Examples of circumstances where the University will be required to disclose personal information are where the law enforcement agency issues the University a warrant, notice to produce, or subpoena, or the University is seeking to report a serious indictable offence. The University may, at its discretion, disclose personal information or health information to law enforcement agencies if it is permitted to do so under law, such as where the University has reason to believe that an offence has been committed and the law enforcement agency has requested that the University disclose personal information that is reasonably necessary to investigate that offence.

(47) In accordance with clause 46 above, the discretion to disclose personal or health information to law enforcement agencies as permitted by law may be exercised by:

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

Section 13 - System Design and Review

(48) Staff must adopt a privacy by design approach by considering the requirements of the IPPs and HPPs when implementing or reviewing a project, process, or system to identify privacy issues, and implement strategies to address those issues and ensure ongoing compliance.

Section 14 - Training and Awareness

(49) The University offers privacy training sessions for new and continuing staff in the staff learning and development portal 'Discover'. Privacy training sessions, both general and tailored to a specific area, are available on request to the Privacy Officer.

Section 15 - Complaints or Review

(50) Individuals may raise concerns and complaints about the way in which the University has handled their personal or health information by submitting a complaint to the Privacy Officer at privacy@newcastle.edu.au. Unless the Privacy Officer considers that the complaint constitutes a request for an internal review, a privacy complaint will be considered under the University's complaint handling processes.

(51) A request for an Internal Review can only be made where it is alleged that the University's conduct has:

a. breached any of the IPPs in PPIPA or any of the HPPs in HRIPA;
b. breached a privacy code of practice that applies to the University; or
c. disclosed personal information kept in a public register.

(52) The University will only accept an application for internal review if it meets the thresholds specified in Part 5 of PPIPA. Such an application should:

a. be in writing (or by using the internal review form);
b. be addressed to the University;
c. specify a return address in Australia; and
d. be lodged with the Privacy Officer within 6 months of the date the applicant first became aware of the alleged conduct. The University may exercise its discretion to accept an application which may be received after the end of the 6-month period.

(53) The Internal Review, as far as practicable, will be conducted by the Privacy Officer, or an appropriately qualified employee of the University, who does not have a conflict of interest (Reviewing Officer).

(54) The Reviewing Officer will assess the request for Internal Review in accordance with Part 5 of PPIPA and:

a. will complete the Internal Review within 60 calendar days of the day the application was received; and
b. notify the applicant of the outcome within 14 calendar days of the completion of the Internal Review.

(55) The University may, as result of the outcome of an Internal Review, do any of the following:

a. take no further action on the matter;
b. make a formal apology to the applicant;
c. take such remedial action as it thinks appropriate;

d. provide undertakings that the conduct will not occur again; and/or
e. implement administrative measures to ensure that the conduct will not occur again.

(56) 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

Section 16 - Breach of a Principle

(57) Where the University becomes aware of a breach of the IPPs or HPPs, 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.

(58) A breach of the Privacy Management Plan, the Privacy Policy, and any associated policy and procedure by a member of University staff may constitute misconduct.

(59) It is an offence under PPIPA and HRIPA for a University staff member, as a part of their employment, to:

a. intentionally disclose or use personal or health information that the staff member has accessed, unless it is for a lawful or authorised purpose; and/or
b. supply, by way of a bribe or other similar corrupt conduct, any personal or health information about an individual to another individual.

Section 17 - Controlled Entities

(60) Controlled entities must manage personal and health information in accordance with this Plan. Controlled entities must determine if they have other requirements under the Australian Privacy Principles and/or other legislation and develop appropriate policies and systems to comply with these requirements.

(61) 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

(62) 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

Status and Details

Status	Historic
Effective Date	20th October 2021
Review Date	20th October 2023
Approval Authority	Vice-Chancellor
Approval Date	23rd August 2021
Expiry Date	22nd May 2023
Responsible Executive	David Toll Chief Operating Officer
Enquiries Contact	Daniel Bell General Counsel 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.

"Course" - When referring to a course offered by the University, a course is a set of learning activities or learning opportunities with defined, assessed and recorded learning outcomes. A course will be identified by an alphanumeric course code and course title. Course types include core courses, compulsory courses, directed courses, capstone courses and electives. For all other uses of this term, the generic definition applies.

"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.

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

"Research" - As defined in the Australian Code for the Responsible Conduct of Research, or any replacing Code or document.

"School" - An organisational unit forming part of a College or Division, responsible for offering a particular course.

"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.

"Affiliate" - A person or organisation legally obligated to, or informally associated with the University. Categories of affiliates are outlined on the University website.

"College" - An organisational unit established within the University by the Council.