Privacy Management Plan

(1) The University of Newcastle ("University", "we," "us" or "our") is a great place to learn, work and engage. Our purpose is to deliver an exceptional student experience, preparing graduates for life in an increasingly interconnected society and to serve our regions by taking research that matters to the world and bringing our global expertise home.

Section 1 - Audience

(2) This Privacy Management Plan (Plan) should be read and understood by our staff, students, contractors, volunteers, affiliates, and the public.

Section 2 - Scope

(3) This Privacy Management Plan applies to personal information and health information collected by us.

(4) In addition to our comprehensive educational services, we offer a wide range of services to support you, which include:

a. Wollotuka Institute;
b. Art galleries;
c. medical centres;
d. a legal centre;
e. student counselling;
f. libraries;
g. family and community programmes;
h. a podiatry teaching clinic;
i. an oral health clinic;
j. occupational therapy clinic;
k. Hunter Family Outreach project;
l. a nutrition and dietetics telehealth clinic;
m. a speech pathology clinic; and
n. a tax clinic.

Section 3 - Introduction

(5) This Plan details how we manage the personal and health information of staff, students, and the public in their dealings with us and is a supporting document to the Privacy Policy. The Privacy Policy establishes the Privacy and Rights to Information Manager function within the University.

(6) Section 33 of the Privacy and Personal Information Protection Act 1998 (PPIP Act) requires agencies like us to have a privacy management plan. More importantly, we want to help you understand our commitment to respecting your privacy rights. You can find the current version of our Privacy Management Plan on our publicly available Policy

Library.

(7) We are committed to compliance with the Privacy and Personal Information Protection Act 1998 (PPIP Act), Health Record and Information Privacy Act 2002 (HRIP Act), Privacy Act 1988 (Privacy Act), Privacy (Tax File Number) Rule 2015 (TFN Rule) issued under s 17 of the Privacy Act 1988, Higher Education Support Act 2003 and Healthcare Identifiers Act 2010 (HI Act) Act by:

a. informing you of how your personal information will be handled by us;
b. informing you of your rights under the legislation;
c. establishing and maintaining a culture of privacy awareness; and
d. considering the Information Protection Principles, Health Privacy Principles, Privacy Act, TFN Rule, Higher Education Provider Guidelines, and HI Act where relevant, in the design and/or review of processes, systems and projects undertaken or implemented by us.

Section 4 - Public Registers maintained by the University

(8) We maintain Public Registers as part of our commitment to open government.

Graduation Book

(9) We publish graduation books which include the name of each graduate and the degree conferred upon them. You may opt out of inclusion in such graduation books by contacting graduation@newcastle.edu.au

Contracts Register

(10) We maintain and publish 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.

(11) If you have any concerns about information published as it relates to a person's personal or health information, please let us know at Complaints.

Section 5 - Definitions

(12) In the context of this document the following definitions apply.

(13) "Personal Information" means 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. Personal information can also include things like your fingerprints, retina prints, body samples or genetic characteristics.

(14) "Personal information in relation to students" means for the purposes of paragraph 19-60(3)(a) of the Higher Education Support Act 2003, a higher education provider must comply with the Australian Privacy Principles set out in Schedule 1 of the Privacy Act 1988, in respect of student personal information obtained for the purposes of section 19-43 of the Act, see the Support for Students Policy.

(15) "Sensitive information" means personal information about your ethnic or racial origin, political opinions, religious or philosophical beliefs, sexual activities, or trade union membership.

(16) "Health information" means:

a. personal information that is information or an opinion 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 them; or
    iii. a health service provided, or to be provided, to an individual; or
    iv. other personal information collected to provide, or in providing, a health service; or
b. other 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
c. other personal information that is genetic information about an individual arising from a health service provided to the individual in a form that is or could be predictive of the health (at any time) of the individual or of a genetic relative of the individual; or
d. healthcare identifiers, but does not include health information, or a class of health information or health information contained in a class of documents, that is prescribed as exempt health information for the purposes of the HRIP Act generally or for the purposes of specified provisions of the HRIP Act.

(17) "NSW privacy laws" means Privacy and Personal Information Protection Act 1998 (PPIP Act) and Health Record and Information Privacy Act 2002 (HRIP Act).

(18) "Commonwealth privacy laws" means the Privacy Act 1988 (Privacy Act), the Privacy (Tax File Number) Rule 2015 (TFN Rule) issued under S17 of the Privacy Act, the Higher Education Support Act 2003, and the Healthcare Identifiers Act 2010 (HI Act) Act.

(19) "Tax File Number information" (TFN Information) means information that connects a TFN with the identity of a particular individual (for example, a database record that links a person's name and date of birth with the person's TFN).

(20) "Individual Healthcare Identifier" (IHI information) information means a unique number used to identify an individual for health care purposes. It helps ensure health professionals are confident that the right information is associated with the right individual at the point of care. You already have an IHI if any of the following apply:

a. you have a Medicare card;
b. you have a DVA card; or
c. you are enrolled in Medicare.

(21) "Government-related Identifier" (GRI information) means an identifier that has been assigned by an agency, a State or Territory authority, an agent of an agency or authority, or a contracted service provider for a Commonwealth or State contract e.g. Centrelink Customer Reference Number (CRN), Medicare number, driver's license number or passport number.

(22) "Emergency" has the same meaning as in the State Emergency and Rescue Management Act 1989. If personal information is collected, used or disclosed during an emergency:

a. the public sector agency must not hold the information for longer than 18 months, unless extenuating circumstances apply or consent has been obtained.

Section 6 - Information Protection Principles and Health Privacy Principles

(23) There are 12 Information Protection Principles (IPPs) that apply under the PPIP Act and 15 Health Protection Principles (HPPs) that apply under the HRIP Act. The IPPs are obligations that we must abide by when we collect, store,

use or disclose personal information. We are governed by New South Wales privacy legislation but may have obligations under other legislation such as the Privacy Act 1988 (Cth), the General Data Protection Regulation (EU2016/679) and other global privacy regimes.

(24) At the start of each point below, we will provide a snapshot of the IPPs and HPPs. Where appropriate, this will be followed by more detailed information about how we apply those principles to the functions of the University.

Collection of information

IPP 1 and HPP 1 – Lawful

> SNAPSHOT: We must only collect your personal information or health information for a lawful purpose, which is directly related to our functions or activities and necessary for that purpose.

(25) We may collect your personal or health information for the following purposes:

a. providing courses of study (including all associated administrative processes);
b. conferring degrees and other awards;
c. research and administration of higher degree by research candidature;
d. exercising commercial functions;
e. fundraising;
f. marketing;
g. promoting events and students;
h. surveys and competitions;
i. providing news and updates;
j. selection, appraisal, remuneration of staff and associated administrative processes;
k. employment and managing staff and students;
l. providing and administering accommodation for students;
m. providing support services such as counselling, disability services, medical services, or advocacy services;
n. managing complaints or disputes;
o. providing taxation assistance;
p. providing legal assistance;
q. managing or facilitating scholarships; and/or
r. managing requests for academic consideration.

IPP 2 and HPP 3 – Direct Collection

> SNAPSHOT: We must only collect your personal information or health information directly from you, unless you have authorised collection from someone else, or you are under 16 and the information has been provided by your parent or guardian or for health information, or it is unreasonable or impracticable to do so.

(26) We may collect personal information from you when you interact with us, for example:

a. in person;
b. over the telephone; or
c. online.

(27) Whenever possible, we will collect your personal information directly from you. If you wish to authorise another party to act on your behalf, we will require written express consent from you to do so, or unless you have authorised that party by law, for example, under a Power of Attorney document.

(28) Where we collect personal or health information from another person, agency or party about you consent may be obtained from you by:

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

(29) Another party may manage the consent and authorisation for the provision of personal or health information prior to the information being provided to us, for example where a student authorises another tertiary institution to provide information to us.

(30) We 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. we are 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.

(31) We may collect personal or health information where we have been contacted by a health practitioner, law enforcement, or another person who holds grave concerns for the safety and wellbeing of you, or another person.

IPP 3 and HPP 4 – Open

> SNAPSHOT: We must inform you, or the person you have authorised, why we are collecting your personal or health information, what we will do with it, and who else might see it. We will also tell you, or the person you have authorised, how they can view and correct the personal or health information, if the information is required by law or voluntary, and any consequences that may apply if you or they decide not to provide the information.

(32) At the time of collecting personal or health information, or as soon as possible afterwards, we must inform you about:

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

(33) For example, if you wish to enrol in a course of study with us, your supply of your personal information is voluntary. IF you do not wish to provide your name, we would not be able to identify you, issue you with a student identification card, a student email address, or provide you with proof of your completion of your course. Another example could be if you required time away from your course of study or employment due to illness, and you did not wish to provide a medical certificate, we may not be able to grant that leave of absence. This advice may be provided to you 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).

IPP 4 and HPP 2– Relevant

> SNAPSHOT: We will ensure that the personal information and health information that we collect is relevant, accurate, complete, up-to-date, and not excessive and that the collection does not unreasonably intrude into your personal affairs.

(34) We aim to ensure that your personal information and health information is:

a. relevant, accurate, complete, up to date, not excessive, and that collection does not unreasonably intrude into your personal affairs;
b. not collected or unnecessarily duplicated and that databases and systems are maintained and reviewed to ensure the information is accurate;
c. able to be updated or amended by you 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 (see IPP1 and HPP1).

(35) We will only ask you for personal information that is necessary for the stated purposes of collection in IPP1 and HPP1. If you feel that a request for your personal is not relevant, or excessive please let us know at either point of collection or by contacting privacy@newcastle.edu.au. If you believe that your personal information is not accurate, complete, or up to date please see IPP7.

Storage of information

IPP 5 and HPP 5– Secure

> SNAPSHOT: We will store your personal information and health information securely, keep it no longer than necessary and dispose of it appropriately. It will be protected from unauthorised access, use, modification, or disclosure.

(36) We protect personal and health information by:

a. identifying and classifying records and handling them accordingly;
b. storing records in our 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 or health information is only granted on a need-to-know basis and that these systems are password protected;
d. ensuring that, whatever available, systems established to collect information are used effectively;
e. ensuring information within systems is only accessed or viewed as required for our functions;
f. ensuring information is only transferred between parties when it is necessary to fulfil our functions 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.

(37) We consist of 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 our overarching policies and procedures which determine how we will use, manage, secure, and dispose of information which may include personal or health information, including, but not limited to:

a. this Plan;
b. Privacy Policy;
c. Records Governance Policy;
d. Support for Students Policy;
e. Digital Technology Conditions of Use Policy;
f. Digital Security Policy and its associated documents; and
g. Research Data and Primary Materials Management Procedure.

Access and Accuracy of information

IPP 6 and HPP 6 – Transparent

> SNAPSHOT: We will explain to you what personal information and/or health information about you is being stored, why it is being used and any rights you have to access it.

(38) You may obtain details on:

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

(39) This information will generally be available at the time of collection, either from a person collecting it, via our website, or upon request as detailed below.

IPP 7 and HPP 7 – Accessible

> SNAPSHOT: We will allow you to access your personal or health information without excessive delay or expense.

(40) Personal or health information collected by us 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).

(41) Staff and students may generally correct or amend their personal or health information automatically or routinely. In cases where personal information 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; or
c. If neither of the above apply, you can contact the Privacy and Rights to Information Manager at privacy@newcastle.edu.au.

IPP 8 and HPP 8 – Correct

> SNAPSHOT: We will allow you to update, correct or amend your personal or health information where necessary.

(42) In response to a request, we may amend your personal or health information or make an annotation on the document to detail the request. If we consider that the personal or health information held is correct and does not require amendment, you will be provided with the reasons for this decision.

(43) Requests for correction or amendment of personal or health information may also be sent to the Privacy and Rights to Information Manager for assistance or action as appropriate. In some cases, requests may be referred for action under the Government Information (Public Access) Act 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.

Use of information

IPP 9 and HPP 9 – Accurate

> SNAPSHOT: We will make sure that your personal information and health information is relevant, accurate, up to date and complete before using it.

(44) We take reasonable steps to verify the accuracy of your personal or health information, especially where the use of the information could lead to negative consequences for you.

IPP 10 and HPP 10 – Limited

> SNAPSHOT: We will only use your personal information or health information for the purpose it was collected (see IPP1 above) unless you have given us your consent, or the purpose of its use is directly related to the purpose for which it was collected, or to prevent or lessen a serious imminent threat to any person's health or safety.

(45) We must not use information we hold for a purpose other than for which it was collected, unless:

a. you or a person you have authorised have consented to the use of the personal information or health 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 or health information was originally collected; or
c. the use of the personal information or health information is necessary to lessen or prevent a serious and imminent threat to the life or health of any person.

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

(47) In considering whether a purpose is directly related to the original purpose, our staff may consider the reasonable

expectations of the person whose information they are dealing with. For example, if you provide a medical certificate to validate an absence from study or employment, we would never use that information to invite you to participate in a health study related to your condition.

Disclosure of information

IPP 11 and HPP 11 – Restricted and Limited Disclosure

> SNAPSHOT: We will only disclose your personal information or health information with your consent, or consent from an authorised person; or, if you were told at the time that it would be disclosed. We will also disclose your personal information or health information if the disclosure is directly related to the purpose for which the information was collected, and there is no reason to believe you would object; or if you have been made aware that information of that kind is usually disclosed. We will also disclose your personal information or health information if it is necessary to prevent a serious and imminent threat to any person's health or safety.

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

(49) We 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. you are reasonably likely to have been aware, or have been made aware at collection, that personal information or health 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 or health information was collected, and we have no reason to believe that you would object to the disclosure;
c. the disclosure of the personal or health information is necessary, on reasonable grounds, to prevent or lessen a serious and imminent threat to the life or health of any person; or
d. an exemption applies under the PIPP Act 1998 or HRIP Act 2002.

(50) People 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.

(51) We 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.

(52) Please also see Section 9 – Specific Exemptions from Principles.

IPP 12 – Safeguarded

> SNAPSHOT: We cannot disclose your sensitive information without your consent, for example, information about your ethnic or racial origin, political opinions, religious or philosophical beliefs, sexual activities, or trade union membership. We can only disclose your sensitive information without consent to deal with a serious and imminent threat to any person's health or safety.

(53) We must undertake reasonable actions to ensure that any sensitive 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.

(54) We must not disclose personal information relating to your ethnic or racial origin, political opinions, religious or philosophical beliefs, trade union membership or sexual activities unless the disclosure is necessary to prevent a serious and imminent threat to the life or health of your or another person.

(55) If we hold personal information about you, we must not disclose the information to any person or body who is in a jurisdiction outside New South Wales or to a Commonwealth agency unless:

a. we reasonably believe that the recipient is subject to a law, binding scheme or contract that effectively upholds principles for fair handling of the information that are substantially similar to the information protection principles; or
b. you expressly consent to the disclosure; or
c. the disclosure is necessary for the performance of a contract between you and us, or for the implementation of pre-contractual measures taken in response to your request; or
d. the disclosure is necessary for the conclusion or performance of a contract concluded in your interest between us and a third party; or
e. all of the following apply:
    i. the disclosure is for your benefit;
    ii. it is impracticable to obtain your consent to that disclosure,
    iii. if it were practicable to obtain your consent, you would be likely to give it; or
f. the disclosure is reasonably believed by us to lessen or prevent a serious and imminent threat to your life, health or safety or of another person; or
g. we have taken reasonable steps to ensure that information that has been disclosed will not be held, used or disclosed by the recipient of the information inconsistently with the information protection principles; or
h. the disclosure is permitted or required by an Act (including Act of the Commonwealth) or any other law.

HPP 12 – Information Identifiers and Anonymity

> SNAPSHOT: You may be identified by using unique identifiers if it is reasonably necessary to carry out our functions efficiently.

(56) We may identify you by providing you with an employee or student identification number. This is particularly beneficial to differentiate between two or more employees, or students with the same name. You may also be identified by a computer user number plate.

HPP 13 – Anonymity

> SNAPSHOT: Services may be provided anonymously, where it is lawful and practicable. We will generally

require information about you to deliver a service to you, however, anonymity may be allowed wherever possible.

(57) In some situations, where you may be at risk of harm, you may request anonymity. In these situations, we may use an alias. It is important to note that there may be situations where anonymity is not practical, for example, where ongoing care is required and follow-up would not be possible, or where your medical status may compromise appropriate care.

(58) There are some situations where providing services may be unlawful, for example, when accessing Medicare benefits, or seeking benefits from the Pharmaceutical Benefits Scheme.

HPP 14 – Information Transferrals and Linkages

SNAPSHOT: We will only transfer health information outside of New South Wales in accordance with HPP 14.

(59) Health information and personal information (where relevant) may be transferred outside New South Wales if:

a. we reasonably believe 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 PPIP Act;
b. you consent to the transfer;
c. the transfer is necessary for the performance of a contract (either between you and us or in the interests of you if the contract is between us 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 your benefit, and it is impracticable to obtain your consent to that transfer, and you would otherwise be likely to give consent; or
g. we have 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.

(60) Where we seek to use or disclose health or personal information for research purposes without your consent, the research proposal must be submitted and approved by the Human Research Ethics Committee prior to the use or disclosure of information.

HPP 15 – Authorised

SNAPSHOT: We will only use health records linkage systems if you have provided or expressed your consent. For example, My Health Record.

Section 7 - Privacy Act 1988 (Cth)

(61) While we are predominantly regulated by NSW privacy laws there are areas of our functions where Commonwealth privacy laws govern our actions.

(62) Some examples of when the Commonwealth privacy laws apply are, when we collect:

a. TFN Information;

b. Individual Health Identifiers; or
c. Government-related Identifiers.

(63) Commonwealth privacy laws also apply when we manage personal information in relation to students under our Support for Students Policy. In accordance with our Support for Students Policy, for the purposes provided within the Higher Education Support Act 2003 (HESA) section 19.60, we must comply with the Australian Privacy Principles set out in Schedule 1 of the Privacy Act 1988 (Cth), in respect of personal information obtained for the purposes of subsection 36.12(2) or 36.20(1) or Chapter 3 – Assistance to students, or 4 – Repayment of loans, in respect of student personal informatio obtained for the purposes of section 19.43 of the HESA.

Section 8 - International Privacy Laws

(64) There are many international jurisdictions where if we market goods or services, or monitor the behaviour of residents in that jurisdiction, we may have obligations under the privacy laws of that jurisdiction.

Section 9 - Specific Exemptions to the Principles

(65) Relating to Law enforcement and related matters:

a. We are not required to comply if information is collected in connection with proceedings (whether or not actually commenced) before any court or tribunal.
b. We are not required to comply if the information concerned is collected for law enforcement purposes.
c. We are not required to comply if the use of the information concerned is for a purpose other than the purpose for which it was collected, is reasonably necessary for law enforcement purposes or the protection of the public revenue.
d. We are not required to comply if the disclosure of information concerned:
    i. is made in connection with proceedings for an offence or for law enforcement purposes; or
    ii. is to a law enforcement agency for the purposes of ascertaining the whereabouts of an individual who ha been reported to a policy officer as a missing person; or
    iii. is authorised or required by subpoena or by search warrant or other statutory instrument; or
    iv. is reasonably necessary:
        - for the protection of the public revenue; or
        - in order to investigate an offence where there are reasonable grounds to believe that an offence may have been committed.
e. Nothing in clause 63d requires us to disclose personal information to another person or body if the University is entitled to refuse in the absence of a subpoena, warrant or other lawful requirement.
f. We are not required to comply with the principles if:
    i. we are providing the information to another public sector agency or is being provided with the information by another public sector agency; and
    ii. the collection, use or disclosure of the information is reasonably necessary for law enforcement purposes.
g. We are not required to comply if the disclosure of the information concerned is reasonably necessary for the purposes of law enforcement in circumstances where there are reasonable grounds to believe that an offence may have been, or may be, committed.

(66) Relating to ASIO, for example, we are not required to comply with Section 13 or 14 of the PPIP Act if compliance would reveal to the public that ASIO had requested, or been provided with, information about a person. The University

is permitted (but is not required) to disclose any information requested by the Director-General of ASIO.

(67) Relating to investigative agencies:

a. We are not required to comply if compliance might detrimentally affect (or prevent the proper exercise of) our complaint handling functions or any of our investigative functions.
b. We are not required to comply if the if the use of the information concerned for a purpose other than the purpose for which it was collected is reasonably necessary in order to enable us to exercise our complaint handling functions or any of our investigative functions.
c. We are not required to comply if the information concerned is disclosed to another investigative agency.
d. We are not required to comply if:
    i. the information concerned is disclosed to a complainant; and
    ii. the disclosure is reasonably necessary for the purpose of:
        - reporting the progress of an investigation into the complaint made by the complainant; or
        - providing the complainant with advice as to the outcome of the complaint or any action take as a result of the complaint.

(68) We are not required to comply with Section 9 or 10 of the PPIP Act if compliance, in the circumstances, would prejudice the interests of the individual to whom the information relates.

(69) There are specific exemptions for certain law enforcement agencies, for example, the Independent Commission Against Corruption (ICAC) or the NSW Crime Commission.

(70) We are not required to comply where information is being exchanged between public sector agencies, for example, we are providing the information to another public sector agency or we are being provided with the information by another public sector agency, and the collection, use or disclosure of the information is reasonably necessary:

a. to allow any of the agencies concerned to deal with, or respond to, correspondence from a Minister or member of Parliament;or
b. to enable inquiries to be referred between the agencies concerned; or
c. to enable the auditing of the accounts or performance of a public sector agency.

(71) Relating to research:

a. We are not required to comply with the principles with respect to the collection, use or disclosure of personal information if:
    i. the collection, use or disclosure of the information is reasonably necessary for the purpose of research, or the compilation or analysis of statistics, in the public interest; and
    ii. in the case where it is unreasonable or impracticable for the information to be collected directly from the individual to whom the information relates; and
    iii. in the case of the use or disclosure of the information, either:
        - the purpose referred to in clause 72(a)(i) cannot be served by the use or disclosure of information that does not identify the individual or from which the individual's identity cannot reasonably be ascertained and it is impracticable to seek the consent of the individual for the use or disclosure; or
        - reasonable steps are taken to de-identify the information; and
    iv. in the case where the use or disclosure of the information could reasonably be expected to identify individuals – the information is not published in a publicly available publication; and

v. the collection, use or disclosure of the information is in accordance with guidelines, if any, issued by the Privacy Commissioner for the purposes of this paragraph.

(72) Relating to emergency situations:

a. we are not required to comply with the principles in relation to the collection, use or disclosure of personal information if:
    i. the collection, use or disclosure of the information is reasonably necessary to assist in a stage of an emergency; and
    ii. the collection, use or disclosure is only for the purpose of assisting in the stage of the emergency; and
    iii. it is impracticable or unreasonable to seek the consent of the individual to whom the information relates to the collection, use or disclosure for the purpose of assisting in the stage of the emergency.

Section 10 - Law Enforcement Agencies

(73) We 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. Some examples where we will be required to disclose personal information are where a law enforcement agency issues us a warrant, notice to produce, or subpoena; or, we are seeking to report a serious indictable offence. We may, at our discretion, disclose personal information or health information to law enforcement agencies if we are permitted to do so under law, such as where we have reason to believe that an offence has been committed and the law enforcement agency has requested that we disclose personal information that is reasonably necessary for them to investigate the offence.

(74) In accordance with the clause 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 Senior Deputy Vice-Chancellor (Academic) 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 11 - Mandatory Data Breach Reporting

(75) From 28 November 2023, NSW public sector agencies, like us, are subject to mandatory data breach reporting.

(76) All staff must report any suspected breach of privacy immediately to the Privacy and Rights to Information Manager, at the email address privacy@newcastle.edu.au.

(77) Staff must take all reasonable steps necessary to contain a suspected breach, for example attempting to recall an email that has been addressed to a mistaken recipient.

(78) Mandatory data breach reporting requires us to assess any suspected breach to determine if there is a breach and if there is, if there is a serious risk of harm to impacted individuals. If it is identified that there is a data breach, and it is likely to result in a serious risk of harm to an individual to whom that information relates (an eligible data breach), then we must notify the NSW Information Privacy Commissioner and the impacted individual(s) within a specified timeframe. However, if we can mitigate harm before it impacts the individual(s), we do not need to notify them.

(79) The reporting scheme means we will work together with the Information Privacy Commissioner, to minimise the

impact of any eligible data breach and keep those impacted informed.

(80) Not reporting a suspected breach or a data breach could result in disciplinary action.

(81) For more information about data breach reporting, please see our Data Breach Policy (Personal and Health Information).

Section 12 - System Design and Review

(82) All staff should adopt a privacy by design approach by considering the obligations of the IPPs and HPPs and the Privacy Act when implementing or reviewing a project, process, service, or system to identify privacy issues, and implement strategies to address those issues and ensure ongoing compliance. When appropriate, for example where high-risk information is being shared with a third party, a Privacy Impact Assessment should be conducted and the Privacy and Rights to Information Manager can help you with this.

Section 13 - Training and Awareness

(83) The University offers privacy training sessions for new and continuing staff in the staff learning and development portal 'Discover.' You may also enquire about privacy training sessions, both general and tailored to a specific area, by contacting the Privacy and Rights to Information Manager.

Section 14 - Complaints and Reviews

(84) We are committed to protecting your privacy. If you believe that we have not handled your personal or health information well, we ask that you give us the first opportunity to address your concerns. This will often be the more timely, efficient, and informal way of addressing your complaint.

(85) You can raise concerns and complaints about the way in which we have handled your personal or health information in one of the following ways:

a. submitting a complaint under the University's complaint handling processes at Complaints;
b. applying for an internal review (see below);
c. contacting the Privacy Commissioner (see below).

(86) A request for an internal review can only be made where it is alleged that our conduct has:

a. breached any of the IPPs in PPIP Act or any of the HPPs in HRIP Act;
b. breached a privacy code of practice that applies to us; or
c. disclosed personal information in a public register.

(87) We can only accept an application for internal review if it meets the thresholds specified in Part 5 of PPIP Act. This includes that the application should:

a. be in writing;
b. be addressed to the University;
c. specify a return address in Australia; and
d. be lodged with the Privacy Office within 6 months of the date the applicant first became aware of the alleged conduct.

(88) We may exercise our discretion to accept an application which may be received after the end of the 6-month period.

(89) The request for an internal review should be mailed to the below address, or made online at Complaints:

Privacy and Rights to Information Manager
Legal and Compliance
University of Newcastle
University Drive
Callaghan NSW 2308

(90) The internal review, as far as practicable, will be conducted by the Privacy and Rights to Information Manager, or an appropriately qualified employee, who does not have a conflict of interest (Reviewing Officer).

(91) The Reviewing Officer will,as soon as practicable, notify the Privacy Commissioner of the application, keep the Privacy Commission informed of the progress of the internal review, and inform the Privacy Commissioner of the findings of the review and of the action proposed to be taken in relation to the matter.

(92) The Privacy Commissioner is entitled to make submissions to us in relation to the application.

(93) The Reviewing Officer will assess the request for internal review in accordance with Part 5 of PPIP Act and:

a. will complete the internal review within 60 calendar days of the day the application was received; and
b. notify you of the outcome within 14 calendar days of the completion of the internal review.

(94) As a result of the outcome of an internal review we may do any of the following:

a. take no further action on the matter;
b. make a formal apology to you;
c. take remedial action as 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.

(95) If you are still unhappy with how we have addressed your concerns, you 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 Information Privacy Commission		NSW Civil and Administrative Tribunal
Level 15, McKell Building		PO Box K1026
2-24 Rawson Place		Haymarket NSW 1240
Haymarket NSW 2000		Phone: 1300 006 228
Free call: 1800 472 679		
Fax (02) 6446 9518		
ipcinfo@ipc.nsw.gov.au		

Section 15 - Breach of a Principle

(96) Where we become aware of a breach of the IPPs or HPPs or the Privacy Act, we will take appropriate steps to identify and address the breach. Reports of breaches or potential breaches should be sent to the Privacy and Rights to Information Manager at privacy@newcastle.edu.au.

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

(98) It is an offence under PPIP Act, HRIP Act or Privacy Act for a 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 16 - Administration

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

Section 17 - Privacy Information available in other languages

(100) The Information Privacy Commissioner has Fact Sheets available "A guide to privacy laws in NSW available in other languages".

Status and Details

Status	Current
Effective Date	24th February 2025
Review Date	24th February 2026
Approval Authority	Vice-Chancellor
Approval Date	28th January 2025
Expiry Date	Not Applicable
Responsible Executive	David Toll Chief Operating Officer
Enquiries Contact	Daniel Bell General Counsel Legal and Compliance

Glossary Terms and Definitions

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

"Risk" - Effect of uncertainty on objectives. Note: An effect is a deviation from the expected, whether it is positive and/or negative.

"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.

"Candidature" - The period of time between acceptance of offer and termination, withdrawal from, or completion of a higher degree by research program, including periods when a candidate is not enrolled.

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

"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.

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

"Disciplinary action" - When used in relation to staff of the University, this is as defined in the applicable and current Enterprise Bargaining Agreement, or the staff member's employment contract. When used in relation to students of the University, this refers to the range of penalties that may be applied under the Student Conduct Rule.

"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.