Privacy Policy

Section 1 - Audience

(1) This policy applies to the University of Newcastle (“University”, we”, “us”, or “our”) students, staff, contractors, volunteers, affiliates, and the public (“you” or “your”).

Section 2 - Purpose

(2) The purpose of this policy is to assist you to understand how we meet our obligations under the:

a. Privacy and Personal Information Protection Act 1998 NSW ("PPIP Act");
b. Health Records and Information Protection Act 2002 NSW ("HRIP Act");
c. Privacy Act 1988 (“Privacy Act”); and
d. Healthcare Identifiers Act 2010 (“HI Act”).

(3) The PPIP Act and the HRIP Act are regulated by the NSW Information and Privacy Commissioner (IPC). The Privacy Act and HI Act are regulated by the Federal Office of the Australian Information Commissioner (“OAIC”). This Policy outlines our approach to ensuring compliance with our obligations under the legislation.

Section 3 - Definitions

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

(5) “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.

(6) “Sensitive information” means personal information about your ethnic or racial origin, political opinions, religious or philosophical beliefs, sexual activities, trade union membership and biometric data.

(7) “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
b. other personal information collected to provide, or in providing, a health service; or
c. 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
d. 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

e. healthcare identifiers; but,
f. 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 Health Records and Information Privacy Act 2002 No 71 generally or for the purposes of specified provisions of this Act.

(8) "NSW Privacy Laws" means Privacy and Personal Information Protection Act 1998 (PPIP Act), and the Health Record and Information Privacy Act 2002 (HRIP Act).

(9) "Commonwealth Privacy Laws" means the Privacy Act 1998 (Privacy Act), the Privacy (Tax File Number) Rule 2015 (TFN Rule) issued under S17 of the Privacy Act, and the Healthcare Identifiers Act (HI Act) Act.

(10) "Tax File Number information" (TFN Information) means information that connects a tax file number (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).

(11) "Individual Health Care Identifier information" (IHI 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.

(12) "Government-related Identifier information" (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.

(13) "Data breach" means a breach of a privacy obligation where there is a failure that has the potential to cause unauthorised access to our data. Whilst first thoughts that come to mind when envisage a data breach are a cyber-attack, ransomware, phishing or malware, a data breach can also include the accidental loss of a paper file, a USB stick, or a laptop.

Section 4 - Privacy Management Plan

(14) We maintain a Privacy Management Plan which explains our processes for the management and maintenance of personal information, health information, TFN Information, IHI Information and GRI Information held by us. The Privacy Management Plan has been developed in accordance with relevant sections of PPIP Act and HRIP Act, Privacy Act, and HI Act.

Section 5 - Information Protection Principles and Health Privacy Principles

(15) 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 NSW Privacy Laws 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.

(16) Below you will find a description of the IPPs and HPPs. A detailed explanation of how we apply each of the principles to our functions can be found in the Privacy Management Plan.

Collection of information

IPP 1 and HPP 1 – Lawful

(17) We must only collect your personal information for a lawful purpose, which is directly related to our functions or activities and necessary for that purpose.

IPP 2 and HPP 3 – Direct Collection

(18) We must only collect your personal 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, it is unreasonable or impracticable to do so.

IPP 3 and HPP 4 – Open

(19) We must inform you, or the person you have authorised, why we are collecting it, 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 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.

IPP 4 and HPP 2– Relevant

(20) We will ensure that the personal information is relevant, accurate, complete, up-to-date, and not excessive and that the collection does not unreasonably intrude into your personal affairs.

Storage of information

IPP 5 and HPP 5– Secure

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

Access and Accuracy of information

IPP 6 and HPP 6 – Transparent

(22) We will explain to you what personal information about you is being stored, why it is being used and any rights you have to access it.

Access and Accuracy of information

IPP 6 and HPP 6 – Transparent

(23) We will explain to you what personal information about you is being stored, why it is being used and any rights you have to access it.

IPP 8 and HPP 8 – Correct

(24) We will allow you to update, correct or amend your personal information where necessary.

Use of information

IPP 9 and HPP 9 – Accurate

(25) We will make sure that your personal information is relevant, accurate, up to date and complete before using it.

IPP 10 and HPP 10 – Limited

(26) We will only use your personal information for the purpose it was collected unless you have given us your consent, or the purpose of 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.

Disclosure of information

IPP 11 and HPP 11 – Restricted and Limited Disclosure

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

IPP 12 – Safeguarded

(28) 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 in order to deal with a serious and imminent threat to any person's health or safety.

HPP 12 – Information Identifiers and Anonymity

(29) You may be identified by using unique identifiers if it is reasonably necessary to carry out our functions efficiently.

HPP 13 – Anonymity

(30) Services may be provided anonymously, where it is lawful and practicable.

HPP 14 – Information Transferrals and Linkages

(31) We will only transfer health information outside of NSW in accordance with HPP 14.

HPP 15 – Authorised

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

Section 6 - Privacy Act 1988 (Cth)

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

(34) Three examples of when the Commonwealth privacy laws apply are, when we collect:

a. TFN information;
b. Individual Health Identifiers; or

c. Government-related identifiers.

Section 7 - Law Enforcement Agencies

(35) 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.

(36) 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 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 8 - System Design and Review

(37) 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 Right to Information Manager can help you with this.

Section 9 - Training and Awareness

(38) 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 Right to Information Manager.

Section 10 - Complaints and Reviews

(39) We are very committed to protecting your privacy, so 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 (link here to complaints handling). This will often be the more timely, efficient, and informal way of addressing your complaint, as opposed to a request for an internal review or contacting the Privacy Commissioner.

(40) You can raise concerns and complaints about the way in which we 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).

(41) 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 PPIPA or any of the HPPs in HRIPA;
b. breached a privacy code of practice that applies to us; or
c. disclosed personal information by placing it in a public register.

(42) We can only accept an application for internal review if it meets the thresholds specified in Part 5 of PPIPA. 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. We may exercise our discretion to accept an application which may be received after the end of the 6-month period.

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

Privacy Officer and Rights to Information Officer
University of Newcastle
University Drive
Callaghan NSW 2308

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

(45) 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 from the day the application was received; and
b. notify you of the outcome within 14 calendar days of the completion of the internal review.

(46) We 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 you;
c. take such 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.

(47) 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 Level 15, McKell Building 2-24 Rawson Place HAYMARKET NSW 2000 Free call: 1800 472 679 Fax: 02 6446 9518 ipcinfo@ipc.nsw.gov.au	NSW Civil and Administrative Tribunal PO Box K1026 HAYMARKET NSW 1240 Phone: 1300 006 228

Section 11 - Data Breach

(48) Where we become aware of a breach of the IPPs or HPPs or the Privacy Act, we will take appropriate steps as detailed in the Data Breach Policy. A reports of a breach or suspected breach must be immediately reported to the Privacy and Right to Information Manager here.

(49) Some data breaches are serious and can potentially cause serious harm to you and us. As of 28 November 2023 NSW has mandatory notifiable data breach reporting obligations for eligible data breaches (where there is a serious risk of harm to those impacted individuals). The mandatory notifiable data breach scheme means that if we have experienced a serious data breach we may report the details to the Privacy Commissioner, so the Privacy Commissioner can assess, provide advice and/or investigate and where there is a serious harm to impacted individuals, that we cannot mitigate, we will notify those individuals.

(50) Where a data breach relates to the Privacy Act, we will respond in accordance with the OAIC's mandatory data breach reporting obligations.

(51) We will assess the specific risks based on the type of data held, and the specific circumstances surrounding the data breach to determine our response actions.

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

(53) It is an offence under PPIPA, HRIPA 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 12 - Administration

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

Section 13 - Agency Information Guide

(55) We maintain an Agency Information Guide which provide our processes for information access to your personal information.

Section 14 - Concerns and Complaints

(56) You may raise concerns and complaints about the way in which we manage privacy. The Privacy Management Plan, and the Agency Information Guide provide information on the relevant pathways. In addition, PPIP Act, and HRIP Act and the Privacy Act stipulate review pathways.

Section 15 - Roles and Responsibilities

(57) All staff, representatives, conjoints, affiliates, volunteers and contractors are responsible for personal information, health information, TFN Information, IHI Information and GRI Information including the collection, use, storage, retention, and disclosure of personal information in accordance with the relevant legislation and this Policy. Staff, affiliates and conjoints granted access to our systems have an obligation to ensure they only access information that is reasonably required for, and consistent with, the performance of their role.

(58) The Privacy and Right to Information Manager is responsible for the:

a. oversight of the implementation and review of this Policy, the Privacy Management Plan and the Agency Information Guide;
b. management of systems and processes relating to personal information access applications, privacy complaints and privacy internal reviews;
c. training and awareness activities.

(59) The Vice-Chancellor as Principal Officer for privacy has overall responsibility for ensuring the promotion of the objectives of, and compliance by us with PPIP Act and HRIP Act and Privacy Act.

(60) The University Council receives management reports which enables it to have oversight of compliance with PPIP Act and HRIP Act and Privacy Act.

(61) Controlled entities may be requested to respond to requests from us for personal information access. Conrolled entities may be required to comply with other privacy related legislation, in their own right.

(62) Students have responsibilities when acting as a representative of the University in accordance with any special requirements of that function. In line with the Student Conduct Rule, students must respect the privacy and confidentiality of other students, staff and other members of our community.

Section 16 - Privacy Information available in other languages

(63) The Information Privacy Commissioner has Fact sheets available: A guide to privacy laws in NSW available in other languages.

Status and Details

Status	Historic
Effective Date	29th November 2023
Review Date	29th November 2024
Approval Authority	Vice-Chancellor
Approval Date	23rd October 2023
Expiry Date	23rd February 2025
Responsible Executive	Alex Zelinsky Vice-Chancellor alex.zelinsky@newcastle.edu.au
Enquiries Contact	Daniel Bell General Counsel and Chief Governance Officer Legal and Governance Services

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.

"Calendar days" - All days in a month including weekends and public holidays.

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

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

"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.