PRIVACY MANAGEMENT PLAN

Contents

1. Introduction....2
2. About the University....3
3. Privacy by Design....5
4. Collecting personal and health information....6
5. Retention and security of personal information....7
6. Ensuring the accuracy of personal information....8
7. Limiting the use of personal information?....9
8. Disclosure of personal information....10
9. Dealing with sensitive personal information?....10
10. Health records linkage systems....11
11. Individual identifiers....11
12. Opportunity to remain anonymous....11
13. Accessing personal information....12
14. Amending personal information....13
15. Public registers....13
16. Is the University subject to any exemptions?....13
17. Mandatory Data Breach Notification Scheme....14
18. How to make a privacy complaint to the University....14
19. Key contacts....15

November 2023

Owner: UNSW Legal & Compliance Office
This plan is located on the UNSW Website www.unsw.edu.au/privacy (refer to the Legal & Compliance Privacy web page)

1. Introduction

1.1 Purpose

The purpose of this Privacy Management Plan (the **Plan**) is to explain how the University of New South Wales (the **University**) manages personal and health information in accordance with the University's Privacy Policy and following applicable privacy laws:

- *Privacy and Personal Information Protection Act 1998* (NSW) (the **PPIP Act**)
- *Health Records and Information Privacy Act 2002* (NSW) (the **HRIP Act**)

In particular, it deals with the Information Protection Principles (the **IPPs**) and Health Privacy Principles (the **HPPs**) contained in the above acts. These privacy principles regulate collection, storage, access and correction, use and disclosure of personal and health information in NSW. Section 33 of the PPIP Act requires agencies, including the University, to have a privacy management plan.

The plan also explains who to contact with questions about the information collected and stored by the University, how to access and amend personal information and how to make a complaint if the University may have breached the PPIP or HRIP Acts.

This plan is one of the tools used to train and inform University staff and affiliates about dealing with personal and health information. This helps to ensure that the University complies with the PPIP Act, the HRIP Act and the *Government Information (Public Access) Act 2009* (NSW) (the **GIPA Act**).

1.2 What the plan covers

This plan meets the requirements of s33(2) of the PPIP Act including:

- information about how the University develops policies and practices in line with the state's records, information access and privacy acts
- how the University disseminates these policies and practices within the organisation and trains its staff and affiliates in their use
- the University's internal review procedures
- anything else the University considers relevant to the plan in relation to privacy and the personal and health information it holds.

References to personal information in the plan should be read to include health information. Where there are matters specific to health information they will be so identified.

1.3 Scope

This Plan covers the activities of the University only and does not cover University controlled entities (which are required to develop privacy policies and plans consistent with the privacy obligations in the jurisdictions in which they operate).

This Plan also does not cover independent entities and bodies established to serve the interests of students, staff and others which are not under the direction or control of the University, including:

- Arc@UNSW Limited (including student clubs and societies)
- UNSW Fitness and Aquatic Centre
- UNSW Village, owned and operated by a third party contracted by the University
- independent residential colleges.

1.4 Definitions

Appendix A contains the meaning of key terms.

1.5 Review

This Plan will be reviewed on an annual basis.

2. About the University

2.1 The University's object and functions

The University collects, retains, uses and discloses personal information in the course of meeting its object and exercising its functions as set out in the *University of New South Wales Act 1989 (*NSW). The object of the University is the "promotion within the limits of the University's resources, of scholarship, research, including health research, free inquiry, the interaction of research and teaching, and academic excellence."

The principal functions of the University include:

- the provision of facilities for education and research of university standard,
- the encouragement of the dissemination, advancement, development and application of knowledge informed by free inquiry,
- the provision of courses of study or instruction across a range of fields, and the carrying out of research, including health research, to meet the needs of the community,
- the participation in public discourse,
- the conferring of degrees, including those of Bachelor, Master and Doctor, and the awarding of diplomas, certificates and other awards,
- the provision of teaching and learning that engage with advanced knowledge and inquiry,
- the development of governance, procedural rules, admission policies, financial arrangements and quality assurance processes that are underpinned by the values and goals referred to in the functions set out in this subsection, and that are sufficient to ensure the integrity of the University's academic programs.

The University has other functions including:

- the exercise of commercial functions comprising the commercial exploitation or development, for the University's benefit, of any facility, resource or property of the University or in which the University has a right or interest
- generating revenue for the purpose of funding the promotion of its object and the carrying out of its principal functions
- developing and providing cultural, sporting, professional, technical and vocational services to the community
- general and ancillary functions as may be necessary or convenient for enabling or assisting the University to promote the object and interests of the University, or as may complement or be incidental to the promotion of the object and interests of the University,

The functions of the University may be exercised within or outside NSW, including outside Australia.

2.2 University records containing personal information

In exercising its functions, the following records of the University may contain personal information:

- student administration records relating to admission, identification, enrolment, academic progression, assessment, learning management systems, misconduct and discipline, learning analytics, results, special consideration, academic appeals, graduation and contact lists

- student services records including health, counselling, disability support and wellbeing services
- staff related records including recruitment, identification, superannuation, remuneration, leave, misconduct, performance management and declarations of external interests
- affiliate related records including nomination, appointment and conditions
- administrative records dealing with governance, finance, property (land and buildings), security (including Closed Circuit Television (**CCTV**)), procurement
- alumni and donor records
- research related records such as ethics committee minutes, participant consent and information forms, research data, intellectual property agreements and licences, and grant applications
- marketing and subscriber databases for the promotion of University programs, courses, events and commercial activities
- libraries, museum and archive records of donors and users of these services
- information and communication technologies (ICT) records such as email and other account information, web sites and cookies.

Many of the functions described above specifically require the collection of health information in addition to personal information. However, there are University functions that are based on the collection of health information. These are:

- Research involving humans in the medical, health and allied sciences.
- Teaching using health clinics operated by the University for teaching and research.
- Human resources and Safety – staff leave, work health safety, injury reporting and management, workplace adjustments, support services, medical services.
- Student services – special considerations, disability, health and psychological support and services.

Health information may be collected:

- Direct from the individual, in person, by forms, or online.
- From third parties with consent or in accordance with statutory guidelines under the HRIP Act.

For detailed information about the University's governance and structure, see the University's website.

2.3 Privacy-related policies, procedures and statements

The University states its commitment to protecting personal information in compliance with applicable privacy laws through its Privacy Policy.

Other key University policies and procedures that support compliance with applicable privacy laws and the University's commitment to protecting personal information include:

- Cyber Security Policy
- Data Breach Policy and Procedure
- Data Classification Standard
- Data Governance Policy
- Data Retention Procedure – Home Drives, Office 365 and OneDrive
- Recordkeeping Policy and Standard
- zID Usage Guideline

A full list of University policies is available to the public here.

The University also maintains the following privacy collection statements:

- Student Privacy Statement
- Employee Privacy Statement
- Alumni Privacy Statement
- Website Privacy Statement

2.4 Training and awareness

All staff and affiliates that handle personal information in the course of their work functions must:

- be familiar with this Plan, the Privacy Policy and other applicable policies and privacy collection statements
- complete the online training module – *Foundations of Privacy* – available on Moodle (registration via the Training and Development tab within *myUNSW*) and repeat this training every two years.

The Legal & Compliance team provides customised privacy training and workshops to specific business units on request.

3. Privacy by Design

Across all stages of the personal information lifecycle, the following principles must underpin the University's approach to the management of personal information (as adapted from the NSW Information and Privacy Commission's Privacy by Design Fact Sheet):

- take a proactive approach, anticipating risks and preventing privacy-invasive events before they occur
- automatically protect personal information in IT systems and University practices as the default
- embed privacy into the design of all systems, services and University practices, ensuring that privacy becomes one of the core functions of any system or service
- incorporate all legitimate interests and objectives in a "win-win" manner, avoiding unnecessary trade-offs, such as between privacy and security
- put in place strong security measures throughout the personal information lifecycle, processing personal information securely, documenting maximum period of retention, and destroying personal information securely once the information is no longer required
- ensure that whatever practice or technology used by the University to handle personal information operates according to the stated promises and objectives and is independently verifiable
- actively seek methods to be transparent and make information available to individuals whose personal information is held by the University that is clear, easy to understand and accessible
- keep the interest of individuals paramount in the design and implementation of any system or service, by offering strong privacy defaults and user-friendly options, and ensuring appropriate notice is given
- ensure that any system that holds personal information will have a Privacy Impact Assessment (PIA) undertaken by the UNSW Privacy Officer before the system design is finalised.

4. Collecting personal and health information

4.1 Prior to collection of personal and health information:

Before the University collects personal and health information it must:

- consider alternatives to collecting the information so that data minimisations is prioritised (only collect information that is necessary for the purpose it is being collected and which does not unreasonably intrude into the personal affairs of the individuals concerned)
- for any new project or activity of the University that will involve the collection of such information not previously collected by the University, assess the project or activity to ensure the collection is lawful, fair, necessary and proportionate (via a PIA which is conducted by the Privacy Officer)
- only proceed with new collections of personal and health information where the PIA determines that the collection is lawful, fair, necessary and proportionate
- when collecting personal and health information from students, ensure that such collection is consistent with the purposes set out in the Student Privacy Statement
- when collecting personal and health information from staff, ensure that such collection is consistent with the purposes set out in the Employee Privacy Statement
- when collecting personal and health information from alumni, ensure that such collection is consistent with the purposes set out in the Alumni Privacy Statement

4.2 Collection of personal information – privacy notices and statements

At the time of collection, the University aims to tell students, staff, affiliates and members of the community how it will manage their personal and health information. At the time of collection, the University must:

- collect the personal or health information directly from the individual to whom it relates, unless the individual concerned authorises the collection from someone else (or an exemption in the PPIP Act or HRIP Act applies) – see section 4.3 for more details
- where the collection is from students, staff or alumni, ensure that access to the applicable Privacy Statement is available at the time of collection
- where an existing Privacy Statement is not applicable, a privacy notice must be provided to the individual at the time of collection that sets out:
    - the fact that it is the University collecting the information
    - the purpose for the collection of the information
    - whether the supply of information is required by law or is voluntary, and the consequences of not providing the information.
    - the manner in which the individual can request access to and correction of the information

4.3 Collection of personal information – from third parties

Generally, the University collects personal and health information directly from the individual concerned unless it is lawful and reasonable to do otherwise. Specific collections of personal information from third parties, where the individual concerned has authorised, include information received from:

- the NSW Universities Admissions Centre (the UAC) and similar bodies in other states about individuals seeking to study at the University

- education providers delivering preparation programs which provide a pathway to the University
- authorised agents on behalf of their prospective international student clients
- organisations where students undertake work integrated learning (including clinical placements, field work, practicums, professional experience programs or internships)
- accommodation providers contracted to the University who provide reports to the University relating to discipline and pastoral care of students in residence
- other institutions where students of the University are studying as part of their degree program.

Research

Where personal or health information is collected via a third party as part of research, it must be done in accordance with the Statutory Guidelines on Research issued by the NSW Privacy Commissioner. These require research proposals to be submitted and reviewed by a Human Research Ethics Committee (HREC) registered by the National Health and Medical Research Council (NHMRC).

4.4 Collection of personal and health information – ensure relevance, not excessive and is not an unreasonable intrusion

The University collects most personal and health information required for administrative functions through its business systems. The framework of data and information governance contributes to ensuring the collection of personal and health information by the University is relevant, not excessive and is not an unreasonable intrusion into the personal affairs of individuals.

- Expert staff

The University employs staff with expertise in recordkeeping, privacy and information security, including lawyers and a dedicated Privacy Officer, who are regularly members of project teams, or consulted as subject matter experts, where the personal or health information is a consideration in the University business system.

- Routine collections

For routine or ad hoc collections of personal or health information the Privacy Officer and other expert staff provide advice and assistance to business units. In addition to the training referred to in section 2.4 above, the Privacy Officer also provides custom training for units on request. Lawyers with privacy expertise from the University's Legal Office provide legal advice when it is required.

5. Retention and security of personal information

5.1 General requirements

To ensure personal and health information is stored securely, and kept for no longer than necessary, disposed of appropriately, protected from misuse and unauthorised access, use, modification or disclosure:

- Storage systems (both physical and technological) must be assessed to ensure they provide an appropriate level of protection for the personal and health information being stored (noting that sensitive personal information requires more stringent protections)
- where personal and health information is stored and managed by third parties on behalf of the University, that such parties are bound by a legally binding agreement that commits the third party to the University's retention and security requirements
- access must be restricted (using organisational and technical measures) to only those staff and affiliates that require access to the information to perform their legitimate work functions

- monitoring and auditing of access rights must be undertaken on a regular basis and at a minimum every 3 months
- retention periods must be determined and documented for all personal and health information that is held, such retention periods being consistent with the notice provided to the individuals concerned and any statutory retention obligations
- plans for the secure destruction of personal and health information must be documented and implemented without delay at the end of the retention period.

5.2 Third party service providers

Personal information collected in the course of performing University functions should only ever be stored in University-approved systems. Where such systems are provided by a third party, the provision of such systems must be subject to a legally binding contract between the University and the service provider that contains provisions for the security and handling of personal information. **Third party systems where no such contract exists (e.g. personal cloud storage solutions) should never be used to store personal information collected by the University.**

A typical contract for a service in which the University provides personal information to the service provider will require that the personal information be used only for the purpose of performing the services and that the service provider must observe any directions by the University concerning the use, storage or security of that personal information. In addition, the contract must require that personal information from the University may only be accessed by the service providers employees who have a need to know for the purposes of the contract and who have been directed by the service provider to keep that personal information confidential. Service providers must not by act or omission cause the University to breach its obligations in relation to, or expose the University to any liability in connection with, personal information.

5.3 Retention and disposal of personal information

University records

Personal information in University records must be disposed of in accordance with the retention periods and disposal authorities required under the *State Records Act 1998* (NSW). Retention and disposal of records is managed by Records and Archives.

The advice of the Records and Archives team must be obtained in determining the retention period for personal information being collected, as well as the method and timing of disposal.

Research data

Research data has requirements for data retention over the course of the research project and afterwards. The periods of retention are determined by the *State Records Act 1998* (NSW) and the *Australian Code for the Responsible Conduct of Research*. Where there is a conflict between these two, the longer retention period applies.

The advice of the Research Data Management team must be obtained in determining the retention period for personal information being collected as part of research data, as well as the method and timing of disposal.

6. Ensuring the accuracy of personal information

The majority of personal information used by the University is collected as part of its functions and is then held in business systems to be available for authorised use. Verification at the time of collection is an important step in ensuring the accuracy of personal information. Major business systems are

the “single source of truth” for the respective functions of the University.

To ensure the accuracy of personal information before it is used, the University must:

- subject to notifying the individual concerned that such verification will occur, ensure that documents provided by individuals are verified with the issuer of the document (e.g. academic transcripts from other institutions provided for admissions purposes are verified with the institution that issued the transcript)
- ensure that individuals are aware of the processes and systems available to them to update their own personal information held by the University (e.g. students and staff can update certain personal information via myUNSW)
- use the unique identifier that is assigned to staff and students (the zID) in business systems and transactions in preference to any other form of identification.

7. Limiting the use of personal information?

7.1 General requirements

Access to personal information contained within University business systems is not automatic and must be made by application, with approval required depending on the nature of the information in each system. Where necessary, different levels of users access and functionality must be utilised to ensure that staff only have access to personal information where required for legitimate work functions.

All University business systems containing personal information must have data governance roles as prescribed by the Data Governance Policy. This includes a Data Controller who is accountable for oversight and management of data within that system. The Data Controller is responsible for day-to-day decision making regarding data in that system, including approving and determining any conditions for the use of that data.

7.2 Students

Personal information of students must only be used for the purposes set out in the Student Privacy Statement. Students acknowledge this Statement when they enrol and each time they re-enrol. The University must seek the student’s consent prior to the use of their personal information for any other purpose, except where that other use is authorised or required by law. Students who provide such consent may withdraw their consent in writing at any time.

7.3 Staff

Personal information of employees must only be used for the purposes set out in the Employee Privacy Statement. Staff acknowledge this Statement when they accept their offer of employment. The University must seek the employee’s consent prior to the use of their personal information for any other purpose, except where that other use is authorised or required by law. Employees who provide such consent may withdraw their consent in writing at any time.

7.4 Alumni

Personal information of alumni must only be used for the purposes set out in the Alumni Privacy Statement. Alumni acknowledge this Statement when they graduate from the University. The University must seek the alumni’s consent prior to the use of their personal information for any other purpose, except where that other use is authorised or required by law. Alumni who provide such consent may withdraw their consent in writing at any time.

7.5 Data sharing

Where there is a requirement to use data, including personal information, from one system in another system (including systems provided by third parties), it is a requirement for a data sharing agreement approved by the Data Controller for the source system and agreed by the Data User (being the head of the University business unit that intends to use the data).

The Data Sharing Agreement documents the formal approval given by the relevant Data Controller to a Data User for data to be used in a specified way. It must specify:

- data fields to be shared
- who has permission to access/use the data
- how the data will be accessed/transferred, used, stored, and disposed of when no longer required
- the security arrangements for that data in its target location
- whether the data includes personal information and how that data will be managed and protected
- any caveats that may apply.

8. Disclosure of personal information

8.1 General requirements

Disclosure of personal information outside of the University must only occur where necessary to support the uses outlined in the applicable privacy collection statement, or where the disclosure is authorised or required by law. The University must seek the consent of the individual concerned prior to the disclosure of personal information for any other purpose.

8.2 Disclosure of health information

Disclosure of health information outside of the University must only occur where necessary to support the purpose for which it was collected. Disclosure of health information for any secondary purpose must only occur with the consent of the individual concerned or where the disclosure is authorised or required by law. The disclosure of health information must also be made in accordance with any statutory guidelines issued by the NSW Privacy Commissioner.

8.3 Disclosure under the GIPA Act

Under the GIPA Act individuals may seek access to government information. Where an access application concerns the personal information of a third party the Act requires that they be consulted as part of the public interest test to balance the public interest considerations for and against the disclosure. The consulted persons are informed of their rights of review over any decision to release their personal information.

9. Dealing with sensitive personal information?

Sensitive personal information includes information which relates to an individual's ethnic or racial origin, political opinions, religious or philosophical beliefs, trade union membership, or sexual activities. It also includes health information about an individual (as defined by the HRIP Act), genetic information and biometric information.

Sensitive personal information is collected where it is required by law, where necessary to exercise University functions, and for planning purposes. For example, the University is required to report

detailed statistical information to the Commonwealth. This necessitates the collection of student ethnic or racial origin, which is also used for planning purposes in the University. Similarly, some such information about staff may be required to comply with employment related laws.

Examples of circumstances when sensitive information may be collected:

- initiatives to assist Aboriginal and Torres Strait Island peoples wishing to study, including admission pathways, scholarships and other financial support
- from participants in research projects, where such participants have been provided with a Participant Information Statement and have consented to providing the sensitive information, and the project has received approval from a HREC
- trade union membership fees may be deducted from a staff member's pay, and so this sensitive information may be held by the University for some staff.

The information is retained in the University's secure business systems. Disclosure of sensitive information is only made with the consent of the relevant individual.

10. Health records linkage systems

The University health clinics collect health information and use health records linkage systems.

Linkage systems are used for health information collected during research projects, in some clinical trials as well as University biobanks with health information held by the relevant health departments.

11. Individual identifiers

The University assigns a unique identifier to all students and staff (their zID). Where a student is also a staff member (and vice versa), the same unique identifier will be used. The zID is used to identify the individual in University business systems and is required to be provided by the individual when they interact with the University in their capacity as a student or staff member.

12. Opportunity to remain anonymous

Generally, the University's functions are unable to be fulfilled where an individual remains anonymous. The University is required by law to collect identifiable information from individuals when they enrol in a course of study or are employed by the University.

However, individuals can remain anonymous when:

- making general inquiries to the University
- completing surveys
- participating in some research projects
- making a report through the University's Gendered Violence Portal
- the individual is an Eligible Discloser when making a public interest disclosure under the University's Report Wrongdoing Policy and Procedure.

13. Accessing personal information

13.1 General requirements

A request for access to personal information can only be made by the person to whom the personal information relates or with their express authority. The University will provide access to requested personal information as soon as practicable, usually within 20 working days of the date of the request. Reasonable processing charges may apply to the request but the University will endeavour to provide access where possible at little or no expense.

The Privacy Officer is able to help a person find out if the University holds information about them and the nature of that information and the main purpose for its collection.

Requests for access to personal information are subject to any conditions or limitations that would apply to information access applications under the GIPA Act. In particular, the public interest considerations against disclosure may be relevant in determining a request to access personal information. The restrictions on access imposed by the GIPA Act will override the access rights provided by the PPIP Act and HRIP Act.

13.2 Access by students

University students are able to access information relating to their enrolment at the University through the myUNSW self-service portal. This includes their current enrolment, academic record and current personal contact details. Current and former students can also order a copy of their academic transcript at www.student.unsw.edu.au/transcript (fees apply).

13.3 Access by staff

University staff are able to access information relating to their employment through the myUNSW self-service portal. This includes pay slips, payment summaries and their current personal contact details. Staff can request access to their Personnel File by contacting Human Resources.

13.4 Requesting access to personal information

Members of the public and students or staff and affiliates may request access to their personal information by contacting the relevant business unit of the University that holds the information. The individual may also make the request to the University Privacy Officer if they are not certain which part of the University to contact. There is no application fee, but processing charges may apply.

Requests for personal information will usually be processed in 20 working days, subject to the complexity of the request and the volume of information involved.

If the individual is not satisfied with the outcome of their request, they may apply to the University for an internal review – see section 18.

13.5 Applying for access to personal and non-personal information

Members of the public and students or staff may apply under the GIPA Act for access to any information held by the University, including information about themselves. There is a statutory application fee of $30 plus processing charges may also apply. Further information and an application form are at www.legal.unsw.edu.au/compliance/gipa/requestinfo.

14. Amending personal information

14.1 Amendment by students

University students are able to amend some of their personal information through the myUNSW self-service portal, including address, phone, personal email, emergency contact and personal statistics. Students cannot change their formal name, date of birth, gender or residency status via myUNSW, and must instead use the forms provided at www.student.unsw.edu.au/change-personal-details. Appropriate supporting documentation is required to be provided.

14.2 Amendment by staff

University staff are able to amend some of their personal information through the myUNSW self-service portal, including name, contact details, emergency contacts and personal statistical profile. Appropriate supporting documentation is required to be provided for some changes.

14.3 Amendment by staff

Alumni are able to update their personal contact details through the Alumni website.

14.4 Other options to amend personal information

A person who believes the University holds personal information about them not covered by the routine processes above, may request amendments by contacting the University Privacy Officer.

The University may agree to amend the information and, if so, will inform the individual accordingly. If the University decides not to amend the information, reasons will be provided to the applicant, along with details of the right to seek an internal review of the decision – see section 18. If requested, the University will attach any statement provided by an applicant to the relevant file or information.

If the University changes information as the result of an application, the person to whom the information relates is also entitled, providing it is practicable, to have any recipients of the inaccurate or misleading information notified of an amendment made by the University.

15. Public registers

The University has no public registers under Part 6 of the PPIP Act.

16. Is the University subject to any exemptions?

The University is not covered by any:

- privacy code of practice or public interest direction
- legislation allowing it not to comply with any of the IPPs or HPPs
- memorandums of understanding or referral arrangements with other agencies that relate to personal information other than for research.

17. Mandatory Data Breach Notification Scheme

17.1 Overview

The Mandatory Data Breach Notification Scheme (the **MDBN Scheme**) requires the University, in the event of a suspected data breach, to contain the breach and assess the likely severity of harm to the individuals concerned. The assessment must be completed within 30 days of the University becoming aware of the breach.

Where the breach is likely to result in serious harm to an individual (an **eligible data breach**), the University is required to notify the NSW Privacy Commissioner as well as impacted individuals, and to issue a public notification in certain circumstances. Some exemptions from making a notification are available including where the University takes action to mitigate the breach such that serious harm to an individual is unlikely to occur, if notification would create a serious risk of harm to an individual's health or safety, and where notification would worsen the University's cyber security or lead to further data breaches.

17.2 Reporting data breaches

Effective mitigation of actual data breaches or prevention of potential data breaches is reliant on timely reporting of such matters. University staff who become aware of an actual or potential data breach (irrespective of the severity of the breach) must immediately report the matter in accordance with the requirements of the University's Data Breach Policy.

17.3 Managing and reporting data breaches

All reported data breaches must be managed in accordance with the University's Data Breach Management Procedure.

18. How to make a privacy complaint to the University

18.1 Informal

Individuals are encouraged to try and resolve their privacy complaint informally where possible. The University has internal complaint-handling procedures for students, staff and members of the community to facilitate resolution of complaints informally.

18.2 Application for internal review under PPIP Act

The PPIP Act also provides for individuals to make an application for internal review where such individual is "aggrieved" by the conduct of the University. A review can also be sought where the action taken by the University might only affect the personal information of other individuals. The request for internal review can only be made where it is alleged that the University has:

- breached any of the IPPs or HPPs; or
- breached any code made under the PPIP Act applying to the University; or
- disclosed personal information kept in a public register of the University.

An application for an internal review must:

- be in writing;
- be addressed to the University;

- specify an address in Australia to which the applicant is to be notified after the completion of the review; and
- be lodged with the University Privacy Officer within six months from the time the applicant first became aware of the conduct to be the subject of the review.

The request for internal review should be lodged with the University Privacy Officer using the application form available at www.legal.unsw.edu.au/compliance/privacy/complaints.

In accordance with the PPIP Act, the University will advise the NSW Privacy Commissioner of the name and the details of complainants and keep the Commissioner up to date with the progress of the internal review. The Commissioner also reviews and may make submissions on the findings and proposed actions prior to the University finalising the review. Complainants will be advised of the results of the internal review and any action that the University proposes to take in respect of the complaint.

Individuals who are dissatisfied with the outcome of an internal review can seek administrative review through the NSW Civil and Administrative Tribunal (NCAT).

Internal review findings and any proposed actions are required to be sent to the NSW Privacy Commissioner within 60 days of the date of receipt of the privacy complaint. Complainants are told of their rights to seek review of the University's decisions in response to the complaint.

18.3 Making a complaint to the Privacy Commissioner

The NSW Privacy Commissioner has the power to accept broad-based privacy complaints. Depending on the circumstances the Commissioner may not always be able to accept your complaint. However, the Commissioner can provide guidance regarding other options.

If the complaint is about conduct that can be the subject of an internal review – see above – the Commissioner must inform the complainant of the internal review process and the remedial action that may be available if the complainant decides to make an application for internal review.

18.4 Offences

Offences can be found in Part 8 of the PPIP Act and Part 8 of the HRIP Act.

It is an offence for the staff or affiliates of the University to:

- intentionally disclose or use personal or health information accessed as a part of their work for an unauthorised purpose
- offer to supply personal or health information that has been disclosed unlawfully.

19. Key contacts

19.1 The University

General inquiries

For further information about this Plan, please contact the **University Privacy Officer**.

Email: privacy@unsw.edu.au

Web: www.legal.unsw.edu.au/compliance/privacyhome

The Privacy Officer can provide information regarding:

- how the University manages personal and health information
- requests for access to and amendment of personal or health information

- requests to conduct internal reviews about possible breaches of the PPIP Act and HRIP Act.

Students

Students who have queries concerning their personal information held by the University should contact the **Nucleus Student Hub** in the first instance:

Web nucleus.unsw.edu.au/en/contact-us

Phone: +61 2 9385 8500

Staff

Staff who have queries concerning their personal information held by the University should contact **Human Resources** in the first instance:

Web unsw.sharepoint.com/sites/human-resources (Internal only)

19.2 The NSW Information and Privacy Commission

The NSW Information and Privacy Commission has a range of resources available to members of the public to inform them of their privacy rights.

Web www.ipc.nsw.gov.au/privacy/citizens

Email ipcinfo@ipc.nsw.gov.au

Phone 1800 472 679

19.3 NSW Civil and Administrative Tribunal

The NCAT contact details are set out below:

Web www.ncat.nsw.gov.au

Address: Level 9, John Maddison Tower, 86-90 Goulburn Street, Sydney NSW 2000

Phone 1300 006 228 or (02) 9377 5711

APPENDIX A - DEFINTIONS

Affiliates means conjoint and visiting appointees; consultants and contractors; agency staff; emeriti; members of University committees; and any other person appointed or engaged by the University to perform duties or functions for the University.

Health information is information or an opinion about a person's physical or mental health or disability, or a person's express wishes about the future provision of his or her health services or a health service provided or to be provided to a person (see the definition at section 6 HRIP Act).

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, including such things as an individual's fingerprints, retina prints, body samples, or genetic characteristics (see the definition and at section 4 of the PPIP Act).

Staff means all employees of the University, including casual employees.

DOCUMENT HISTORY

Review History				
Version	**Approved by**	**Approval date**	**Effective date**	**Sections modified**
1.0	General Counsel	November 2023	November 2023	New document