Privacy Management Plan

Table of Contents

1. INTRODUCTION

This Privacy Management Plan (Plan) details the University of Newcastle's approach to managing personal information of staff, students and the general public in their dealings with the University.

This Plan supports the University's compliance obligations under the Privacy and Personal Information Protection Act 1998 (NSW) (the PPIP Act) and the Health Records and Information Privacy Act 2002 (the HRIP Act) by:

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

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

2. AUDIENCE

This policy is relevant to University staff, contractors, controlled entities, conjoints, volunteers, affiliates, students and the general public.

2.1. Controlled Entities

The University requires controlled entities to manage personal and health information in accordance with this Plan. Controlled entities may also have other requirements under the Australian Protection Principles and/or other legislation.

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

3. INFORMATION ABOUT PUBLIC REGISTERS

3.1. UON Graduation Book

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

3.2. Contracts Register

The University maintains and publishes a Contracts Register as required by the Government Information (Public Access) Act 2009 (NSW) (the GIPA Act) with the information required to be contained in the Contracts Register set out in s29 of the GIPA Act. It is unlikely the register will include personal or health information.

The Complaints, Compliance and Policy Officer may be contacted regarding any concerns about information published, as it relates to their personal or health information, via email at privacy@newcastle.edu.au.

4. PROTECTION / PRIVACY PRINCIPLES

This Plan is prepared in consideration of the 12 Information Protection Principles (IPPs) and 15 Health Privacy Principles (HPPs) as outlined in the PPIPA Act and HRIP Act respectively.

The IPPs are summarised using information produced by the NSW Information and Privacy Commission in Appendix 1. The HPPs are summarised using information produced by the NSW Information and Privacy Commission in Appendix 2.

The University continues to be governed by NSW privacy legislation. Certain information (such as Tax File Numbers) is expressly governed by the Privacy Act 1988 (Privacy Act). In particular functions or Commonwealth funded research projects the University may also have obligations under the Australian Privacy Principles (APPs) which are outlined in the Privacy Act. The APPs are not outlined in full in this Plan, however, reference is made to relevant APPs for guidance.

5. COLLECTION

5.1. Lawful Collection

The University may only collect personal and health information for a lawful purpose which is needed for and directly relates to the University's activities.

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

i. provision of courses of study;
ii. conferring of degrees and other awards;
iii. research;
iv. exercising commercial functions;
v. fundraising;
vi. promotion of events and students;
vii. surveys and competitions;
viii. news and updates;
ix. selection, employment, appraisal and remuneration of staff;
x. providing accommodation for students;
xi. providing support services such as counselling/disability services or advocacy services;
xii. managing complaints or disputes;
xiii. managing or facilitating scholarships; and/or
xiv. managing requests for academic consideration.

Refer Appendix 4 for examples of University functions for which the University may collect personal or health information.

5.2. Direct Collection

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

i. the individual has authorised collection of the personal information from someone else;
ii. the personal information is provided by a parent or guardian of a person who is under the age of 16 years; or,
iii. for health information, if it is unreasonable or impracticable to do so.

Where the University collects personal or health information from another individual, agency or party, consent may be obtained with the individual:

i. accepting terms and conditions; or
ii. entering into a contract; or
iii. providing valid and express consent.

Personal or health information may be authorised and the consent managed by another party, prior to the information being provided to the University. This may include where a student authorises information to be provided by another tertiary institution.

5.3. Open Collection

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

i. why it is collecting it;
ii. the use;
iii. who else might see it;
iv. how they can view and correct their personal information;
v. whether the information is required by law or is voluntary; and
vi. any consequences if they decide not to provide the information.

This advice may be provided by way of:

i. terms and conditions;
ii. a collection notice on a form or agreement;
iii. a published privacy notice;
iv. correspondence (i.e. e-mail communication or file note).

5.4. Relevance of Collection

The University aims to ensure that personal and health information is relevant, accurate, complete, up-to-date, not excessive and that the collection does not unreasonably intrude into the personal affairs of the individual.

The University aims to ensure that information is not collected or unnecessarily duplicated and that databases and systems are maintained and reviewed to ensure information is accurate; processes are in place and are easily identifiable for individuals to update or amend their information; and only information required is sought (this will depend on the purpose for which the information is collected).

6. STORAGE

6.1. Security

The University protects personal or health information by:

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

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

7. ACCESS AND ACCURACY

7.1. Transparency

An individual may obtain details to outline:

i. how their personal or health information is being stored;
ii. why it is being used; and
iii. any rights they have to access it.

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

7.2. Accessibility and Accuracy

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

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

i. a Human Resource Services Support staff, for requests from staff; or
ii. Student services, for requests from students.

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

Requests for correction or amendment of personal or health information may also be referred or made to the Complaints, Compliance and Policy Officer for advice or action as appropriate. In certain cases, requests may be referred for action under the GIPA application process. Such cases include where the information:

i. contains personal or health information about another individual;
ii. may require further consideration and advice; or
iii. is held across several different units.

8. USE

8.1. Accuracy

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

8.2. Limitation

The use of personal or health information primarily refers to its use within the University. Where personal or health information is to be used for a directly related purpose that is not the original purpose, staff should take reasonable steps to identify and document as appropriate why they have considered that use to be directly related to the original purpose.

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

9. DISCLOSURE

9.1. Restricted and Limited Disclosure

Disclosure primarily refers to the sharing of information held by the University with another agency or individual outside of the University. Staff should undertake reasonable actions to ensure that personal or health information is not disclosed, either routinely or on a single occasion, without the knowledge of the individual, unless an exemption applies.

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

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

9.2. Safeguarded

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

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

10. IDENTIFIERS AND ANONYMITY

Individuals may be identified by using unique identifiers if it is reasonably necessary to carry out University functions efficiently. Services may be provided anonymously, where lawful and practicable.

The University will generally require information about an individual's identity in order to deliver a service however, anonymity may be allowed wherever possible.

11. TRANSFERRALS AND LINKAGES

Health information may be transferred outside of New South Wales if:

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

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

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

12. LAW ENFORCEMENT AGENCIES

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

The University may exercise discretion and provide personal or health information to a law enforcement agency if it is permitted to do so under the legislation in the particular circumstances.

This discretion may be exercised by:

- the Vice-Chancellor;
- the Deputy Vice-Chancellor (Academic), where the information relates to a student or former student; or
- the Director, People and Workforce Strategy, where the information relates to a staff member or former staff member.

13. SYSTEM DESIGN AND REVIEW

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

14. TRAINING AND AWARENESS

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

15. COMPLAINTS OR REVIEW

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

An individual may also request that the University undertake an internal review of the University's handling of their person or health information which can be initiated by completing the internal review form.

Individuals may lodge a complaint with the NSW Information and Privacy Commission or seek an external review with the NSW Civil and Administrative Tribunal, whose details are set out below.

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

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

16. BREACH OF A PRINCIPLE

Where the University becomes aware of a breach, appropriate steps will be taken to identify and address the breach. Breaches or potential breaches are to be reported to Council Services & Chancellery at privacy@newcastle.edu.au who will advise the Vice-Chancellor accordingly.

17. ADMINISTRATION

An issues register is maintained by Council Services and Chancellery to support the review process, and issues or feedback may be e-mailed to privacy@newcastle.edu.au

Document number	TRIM: D12/12482P
Document owner	Director, Council Services and Chancellery

Effective Date	Approved by	Amendment
10/10/2016	Vice-Chancellor	Review and minor amendments to improve clarity
24/092015	Noms & Legis Cttee	Complete Review conducted. Approved by Nominations and Legislation Committee (Item 4:08-3 D15/26538). The Agency Information Guide has been repositioned as a supporting document to Privacy and Information Access Policy.
23/04/2014	Vice-Chancellor	Administrative Update amend definitions and clause 6.2 replacing DVC(A) with Director Complaints and Information Management as the University's Privacy Officer, update title of Deputy University Complaints Manager
23/01/2014	University Council	Full revision of principles and commitment of the University
15/11/2012	Vice-Chancellor	Administrative Update amend clause 6.2 to change DVC(A&GR) to DVC(R) pending arrival of new DVC(A), update policy owner from DVC (A&GR) to DVC(A)
29/05/2012	Privacy	Administrative Update GIPA Act to GIPA Act 2009 and update to title of the Deputy Vice-Chancellor (Academic and Global Relations)
21/02/2012	Privacy	Administrative Update FOI reference in Principle 6 and 8 to refer to GIPA and working altered in principle 7
28/10/2010	Privacy	Administrative Update FOI to GIPA provisions
15/05/2009	Vice-Chancellor	Insert new clause 1.2 re FOI
21/10/2008	University Council	First version
Document approver	Vice Chancellor	
Other stakeholders		
Date of this version	10 October 2016	
Review date	10 October 2018	
Previous versions		
Legislation	Privacy and Personal Information Protection Act 1998 (NSW) Health Records and Information Protection Act 2002 (NSW) Privacy Act 1988	
Supporting documents	Privacy and Information Access Policy Internal Review Form	
Further information	privacy@newcastle.edu.au	

APPENDIX 1 - INFORMATION PROTECTION PRINCIPLES (IPPs)

The 12 Information Protection Principles (IPPs) are detailed in Sections 8 to 12 of the PPIP Act. To support these principles, an agency must:

Collection		
Lawful	1	Only collect an individual's personal information for a lawful purpose. It must be needed for the agency's activities.
Direct	2	Collect the information from only the individual, unless exemptions apply.
Open	3	Tell the individual that the information is being collected, why and who will be using it and storing it. The individual must be told how to access it and make sure it's correct.
Relevant	4	Make sure that an individual's personal information is relevant, accurate, current and non-excessive.
Storage		
Secure	5	Store your personal information securely. It should not kept longer than needed, and disposed of properly.
Access and Accuracy		
Transparent	6	Provide you with details about the personal information they are storing, reasons why they are storing it and how you can access it if you wish to make sure it's correct.
Accessible	7	Allow you to access your personal information in a reasonable time frame and without being costly.
Correct	8	Allow you to update, correct or amend your personal information when needed.
Use		
Accurate	9	Make sure that your personal information is correct and relevant before using it.
Limited	10	Only use your personal information for the reason they collected it.
Disclosure		
Restricted	11	Only release your information if you consented. An agency, however, may also release your information if it's for a related reason and can be reasonably assumed that you would not object. Or your information is needed to deal with a serious and impending threat to someone's health and safety including your own.
Safeguarded	12	Not disclose your sensitive information without your consent. Such information includes: racial, ethnic information, political, religious and philosophical beliefs, sexual activity and trade union membership. Your information may only be released without consent to deal with a serious and impending threat to someone's health and safety.

APPENDIX 2 – HEALTH PRIVACY PRINCIPLES (HPPs)

The 15 Health Privacy Protection Principles (HPPs) are detailed in Schedule 1 to the HRIP Act.

To support these principles, an agency must:

Collection		
Lawful	1	Only collect an individual's health information for a lawful purpose. It must also relate directly to the agency's activities.
Relevant	2	Make sure that an individual's health information is relevant, accurate, current and non-excessive.
Direct	3	Collect your health information from only the individual, unless exemptions apply.
Open	4	Tell the individual that the information is being collected, why and who will be using it and storing it. The individual must be told how to access it if they wish to make sure it's correct.
Storage		
Secure	5	Store an individual's health information securely. It should not kept longer than needed, and disposed of properly.
Access and Accuracy		
Transparent	6	Provide an individual with details about the health information they are storing, why and how the individual can access it.
Accessible	7	Allow an individual to access their health information in a reasonable timeframe and without being costly.
Correct	8	Allow an individual to update, correct or amend their health information when needed. (Note: private sector organisations should also refer to s33-37 of the HRIP Act for further provisions).
Accurate	9	Make sure that an individual's health information is correct and relevant before using it.
Use		
Limited	10	Only use an individual's health information for the reason that is was collected, unless exemptions apply.
Disclosure		
Limited	11	Only disclose an individual's health information for the reason that is was collected otherwise separate consent is needed from the individual.
Identifiers and anonymity		
Not identified	12	Can only give an individual an ID number if it is reasonably necessary.
Anonymous	13	Give an individual the option of receiving information from them anonymously, where practicable.
Transferrals and linkage		
Controlled	14	Only transfer health information outside NSW in accordance with the HPP 14.
Authorised	15	Only use health records linkage systems if the individual has provided consent.

APPENDIX 3 - POLICY AND PROCESS TO SUPPORT COMPLIANCE WITH THIS PLAN

The University has a number of policies, procedures and processes that refer to or affect how personal and health information are managed by the University. This table will be reviewed and updated as necessary to support staff to comply with the Principles outlined in this Plan.

PRINCIPLE	DOCUMENTS
Communication	The following documents support compliance with the principles outlined in this Plan: • Code of Conduct Policy • Electronic Mail Policy and Guidelines • University Computing and Communications Facilities Conditions of Use Policy • Social Media Communication Policy and Procedure
Systems and Security	The following documents support compliance with the principles outlined in this Plan: • Network Security Policy • University Computing and Communications Facilities Conditions of Use Policy • Records Management Policy • CCTV Policy and Procedure
Student Information	The following documents support compliance with the principles outlined in this Plan: • Admissions and Enrolments process and procedures • Student Amendment of Details Form
Staff Information	The following documents support compliance with the principles outlined in this Plan: • Respectful and Collaborative Workplace Policy • Work Health and Safety Procedure
Access to Information	The following documents support compliance with the principles outlined in this Plan: • Agency Information Guide
Complaints and Investigations	The following documents support compliance with the principles outlined in this Plan: • Complaints Policy and Procedures • Public Interest Disclosures Policy • Student Academic Integrity Policy • Student Conduct Rule and Policies
Research	The following documents support compliance with the principles outlined in this Plan: • Research Institutes Guidelines and Procedures • Responsible Conduct of Research Policy and Procedures • Ethics approval process and procedures

APPENDIX 4 - EXAMPLES OF PURPOSES FOR WHICH INFORMATION MAY BE COLLECTED, USED OR DISCLOSED

This information provides an overview of functions of the University for which personal information may be collected, used or disclosed. It does not replace privacy statements or collection notices.

GENERAL FUNCTION	SPECIFIC FUNCTION/PURPOSE
Student Recruitment, Teaching & Learning and Administration Information collected and used for the purpose of student administration may include addresses and telephone numbers, academic details, sensitive information and/or health information.	• Provision of information to prospective students • Admission and enrolment (including cross institutional programs) • Set up of accounts and systems (i.e. email account) • Communication with students (including via email) • Academic progression • Conferral of degrees • Delivery of programs • Teaching and assessment • Record of attendance • Scholarships • Administration of student placements • Career development • Financial administration • Student retention • Special events i.e. graduation • Special/adverse circumstances information • Disability services information • Student advocacy • Support services • Complaints or investigations • Student misconduct information • Misconduct information • Incident/emergency information • Mandatory reporting or notification, for example to a government agency • Surveys and statistical reporting
Staff Administration Information collected for employee administration may include biographical detail, sensitive personal information and/or health personal information.	• Recruitment, appointment and termination • Absence management • Administration of salary • Administration of leave • Promotion and or professional development • Performance review • Disputes or complaints • Work, Health & Safety • Equity and Diversity • Statistical purposes for reporting • Mandatory reporting or notification, for example to a government agency • Surveys and statistical reporting

GENERAL FUNCTION	SPECIFIC FUNCTION/PURPOSE
Research Information collected for research purposes may include biographical detail, sensitive personal information and/or health personal information.	• Collation and assessment of data (i.e. surveys)
Campus and Community Information collected for campus and community purposes may include biographical detail, sensitive personal information and/or health personal information.	• Gifts and Donations • Maintaining and Alumni database • Communication about the University, University events or news • Requests for information • Requests for or use of a service • Community programs and events • Recording and promotion of activities and events • Administration of volunteers • Security and Safety • CCTV
Assurance, Reporting and Marketing Personal information may be collected or used for the purpose of assurance, reporting and or marketing.	• Surveys • As part of a request for service or support

APPENDIX 5 - EXAMPLES OF SYSTEMS USED BY THE UNIVERSITY TO HOLD OR MANAGE PERSONAL INFORMATION

CATEGORY	SYSTEM	OTHER
Primary Systems		
Human Resources	Alesco HR online Cognology (PRD On-line) Incident Management System Discover	
Finance (Financial Information)	Technology1 Fraedom	
Research Information	NURO RIMS (Research Data)	
Student Administration	NuStar (Student Information) Student Portal - MyHub UONLine and Blackboard OASIS JAMS Databases and CRMs SONIA BMED Admissions System	
Records Management	TRIM (Records Management)	
Communication	Microsoft Outlook email system	Externally hosted in the USA
Other Systems		
Travel Information	ISOS Travel System	Externally Hosted
Student Identification	NuCard	
Recruitment	Staff Appointments Online (SAO)	
Library	Library Systems	
Management	Alumni CRM Student Recruitment CRM Foundation CRM Other	
	LANDesk and ZenDesk Maximo UONService Now	
	Magento	

APPENDIX 6 - COMPLAINTS AND REVIEW

Where an individual has a concern regarding the way the University has managed their personal or health information, they have a right to make a complaint or seek a review of the conduct they are concerned about.

Guidance for raising concerns is outlined below:

Step 1: Individuals should first inform the University of their concerns, so that any available steps may be taken to remedy a privacy issue. Where the University is made aware of a breach, appropriate steps will be taken to address the situation.

Step 2: Individuals may raise a complaint about the potential privacy by contacting the Complaints, Compliance and Policy Officer via email at privacy@newcastle.edu.au.

Step 3: Individuals may also seek an Internal Review by the NSW Privacy Commissioner (the Commissioner) as outlined below.

Internal Reviews

Internal reviews are conducted in accordance with the requirements of Part 5 of the PPIP Act and with regard to guidance produced by the Commissioner.

Role of the Commissioner

The Commissioner will be advised:

- that an Internal Review has been received;
- of the progress of the review;
- of the draft findings; and
- of the final determination.

The Commissioner may wish to make a submission on the subject matter of the review and the University must consider any submissions received in making the final determination.

Who will undertake the review?

A staff member, who has no conflict of interest or involvement in the conduct concerned, will undertake the review. The applicant will be notified when their application is formally acknowledged of the name and contact details of the reviewing officer.

How the applicant is advised of the findings

The applicant will be advised of:

- the findings of the Internal Review and the reasons for those findings;
- the action proposed and the reasons for these actions; and
- their right to seek a review of the University's decision.

Possible actions arising from an internal review include:

- taking no further action;
- making a formal apology;
- taking appropriate remedial action;
- providing an undertaking that the conduct will not occur again; and/or
- the implementation of administrative measures to ensure the conduct is not repeated.

External Review

An applicant may seek an external review by the NSW Civil and Administrative Tribunal if:

- the Internal Review is not finalised within the required period;
- the applicant is not satisfied with the findings; or

- the applicant is not satisfied with the actions proposed.

Reporting
The University will continue to report on any Internal Reviews conducted in the Annual Report.

Further Information
- University of Newcastle – Complaints, Compliance and Policy Officer contact privacy@newcastle.edu.au
- The Information and Privacy Commission NSW (IPC) – refer ipc.nsw.gov.au
- NSW Civil and Administrative Tribunal – refer ncat.nsw.gov.au

APPENDIX 7 - TRAINING AND AWARENESS

Training is available as follows:

- Privacy training sessions for new and continuing staff are available in the staff learning and development portal 'Discover'. This session is an induction requirement.
- Privacy training sessions, both general and tailored to a specific area, are available on request of the Complaints, Compliance and Policy Officer.

Suggestions for training or awareness campaigns or requests for training should be sent to privacy@newcastle.edu.au.

The University continues to participate in Privacy Awareness Week.

end of document