Privacy Management Plan

Section 1 - What is a Privacy Management Plan?

(1) Western Sydney University has legal obligations to individuals whose personal information (also known as personal data) it collects, uses, holds (that is, stores) discloses and destroys. These are obligations that arise at law under the Privacy and Personal Information Protection Act 1998 (NSW) (PPIPA), the Health Records and Information Privacy Act 2002 (NSW)(HRIPA); in some circumstances, the Privacy Act 1988 (Cth) (Federal Privacy Act) and foreign privacy regulations, such as the European Union General Data Protection Regulation 2016/679 (GDPR).

(2) Under the PPIPA, the University is required to have a Privacy Management Plan (PMP) and embraces this obligation as an exercise of good governance and transparency in the way in which the institution deals with the personal information of staff members, students, and other members of the University community.

(3) The Information Protection Principles (IPPs) are set out in the PPIPA as the guiding principles that regulate how the University can collect, use, hold, and disclose personal information of individuals. These are summarised in Section 21 – Annexure A to this PMP.

(4) Under the HRIPA, the Health Privacy Principles (HPPs) set out the obligations of the University when it manages health information. These are summarised in Section 22 - Annexure B to this PMP where these differ from the IPPs.

(5) There are some circumstances where the Federal Privacy Act applies to the University and these details are set out in clause (165). There are also some circumstances where foreign privacy regulations, such as the GDPR apply to the University and these are set out in Section 17. However, the University's primary obligations arise under the PPIPA, as detailed throughout this PMP.

(6) The University is also bound by other legislation that regulates collection, use, storage, disclosure or destruction of personal information. These include:

a. Criminal Records Act 1991 (NSW);
b. Data Sharing (Government Sector) Act 2015 (NSW);
c. Education Services for Overseas Students (ESOS) Act 2000 (Cth);
d. Government Information (Public Access) Act 2009 (NSW);
e. Higher Education Support Act 2003 (Cth);
f. State Records Act 1998 (NSW);
g. Telecommunications (Interception and Access) Act 1979 (Cth); and
h. Workplace Surveillance Act 2005 (NSW).

(7) In addition, some University professional staff are bound by professional codes of practice relating to confidentiality of personal information when providing services for staff or students (counselling services for example). University staff who undertake research involving human participants are required to comply with the 'National Statement on Ethical Conduct in Human Research' (updated 2018) jointly developed by the National Health and Medical Research Council, Australian Research Council and Universities Australia. In accordance with the National Statement, researchers are required to safeguard the privacy and confidentiality of research participants at all stages of the research including the collection, use, analysis, disclosure, storage, retention, disposal, sharing and re-use of

participant data or information.

Scope and Application

(8) This PMP applies to all personal information and records of staff, students and members of the public held by the entire University. All academic and business units of the University must collect, manage and use the personal information they hold in accordance with this PMP. All persons who handle personal information on behalf of the University (including officers, employees, volunteers and contractors) must also comply with the requirements in this PMP.

(9) This PMP also covers controlled entities of the University, which currently include Western Sydney University Enterprises Pty Ltd trading as Western Sydney University - The College (The College), Western Sydney University Early Learning Ltd, Whitlam Institute within Western Sydney University Ltd and Whitlam Institute within the Western Sydney University Trust.

(10) For the purpose of this document, a reference to a "student" includes a reference to a student enrolled in a program of study at the University and/or at The College, and a reference to University processes includes a reference to The College processes unless otherwise indicated.

Section 2 - Personal Information Defined

What is personal information?

(11) Personal information is defined in the PPIPA as:

> 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.

(12) The PPIPA also defines personal information to include an individual's fingerprints, retina prints, body samples, or genetic characteristics.

(13) The University assigns employees and students with a unique identifier in the form of a staff or student ID number. Staff and student ID numbers are considered to be personal information and will be handled in accordance with applicable privacy laws.

What is not personal information?

(14) Certain categories of information are often mistakenly classified as personal information, and the PPIPA also specifies classes of information that are not "personal information".

(15) The categories of information that are not personal information relevant to the University include:

a. information which relates to a person who has been dead for more than 30 years; or
b. information which is publicly available; or
c. information about an individual that is contained in a public interest disclosure within the meaning of the Public Interest Disclosures Act 1994, or that has been collected in the course of an investigation arising out of a public interest disclosure; or
d. information which relates to a person's suitability for employment as a public sector official; or
e. information that is de-identified information, for which identifiers have been permanently removed or never included; or

f. information about University graduates, including a graduate's name, academic award, and year of conferral, which is made publicly available through the University's Award Verification Service.

What is health information?

(16) Health information is defined in the HRIPA as personal information that is information or any opinion about:

a. the physical or mental health or a disability (at any time) of an individual; or
b. an individual's express wishes about the future provision of health services to them; or
c. a health service provided, or to be provided, to an individual.

(17) It is further defined as personal information:

a. collected to provide, or in providing, a health service; or
b. 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
c. collected in connection with the donation, or intended donation, of an individual's body parts, organs or body substances; or
d. health care identifiers (numbers assigned to an individual used in connection with health information).

Section 3 - Why Does the University Collect Personal Information?

Rationale

(18) The University is a public institution participating in teaching, research, community service, and engagement activities. It collects and holds a wide range of personal information about students, alumni, staff, and members of the external University community. The University comes into contact with these individuals in carrying out its functions and activities, and it cannot function without collecting and holding information with regard to individuals.

(19) It is essential that the University collects, holds, and uses the above information for the ongoing conduct of its activities.

Purposes for which Information is Collected

(20) Personal information may be collected for the performance of the University's key functions, including:

a. managing and improving the experience of students, including recruitment, enrolment, registration, assessment, graduation, safety and wellbeing;
b. managing and improving the experience of employees, volunteers and affiliated individuals (such as visiting, adjunct, conjoint, honorary and others) including recruitment, performance, remuneration, safety and wellbeing;
c. learning and teaching;
d. research and development;
e. administrative functions, including receipt, management and payment of funds, and safety and security of individuals and property;
f. provision of welfare, community and other services and advocacy;
g. development and engagement with various groups including employees, students, prospestive students,

alumni, donors, community groups, other educational institutions, industry and government;

h. reporting obligations with which the University is legally bound to comply.

(21) Personal information may also be collected from third parties as part of a formal investigation taken under a legislative requirement or pursuant to any rules, codes of conduct or policies of the University, including carrying out due diligence inquiries and investigations relating to alleged staff or student misconduct.

(22) Health information may be collected for the University's functions including student engagement, health and welfare services, recruitment, human resources and complaint handling.

(23) There is no finite list of personal information and/or health information that the University collects about individuals. However, Section 23 – Annexure C sets out examples of personal information and health information that may be collected by the University in undertaking its functions and activities.

Only Relevant Information is Collected

(24) The University ensures that the personal information and health information it collects from individuals is relevant to its functions. It collects the information that is required depending on who the individual is and what their relationship is with the University. For example, different information is collected from students than from staff, which is again different to information collected from donors to the University.

(25) The University takes steps to minimise unreasonable intrusion to an individual and not to collect excessive information by, for example:

a. reviewing and updating processes that always require collection of personal information, such as recruitment and enrolment;
b. undertaking a fresh collection of personal information and health information for different processes within the University, for example during complaint-handling or a workers' compensation matter;
c. in the case of students in contact with Equity, Safety and Wellbeing, requesting updated health information on a bi-annual basis or when circumstances change.

Section 4 - Holding Information

Overview

(26) Under the PPIPA, the University must ensure that it does not hold personal information for longer than it needs to use the information. The University must also retain personal information records as required by the general retention and disposal authorities issued by the State Records Authority. The period in which records are retained depends on the type of record.

(27) The ways in which the University holds, uses, discloses and destroys personal information is discussed below.

(28) The University holds information for the purposes of privacy obligations if the information is:

a. in its possession or control; or
b. in the possession or control of a person employed by or engaged by the University; or
c. contained in a state record under the State Records Act 1998 (NSW).

(29) The University holds personal information in a variety of media, including in hardcopy form, but primarily in data management systems and the University's records management system. Different parts of the University hold different information in different databases and systems.

Examples of Information Held

(30) Below are some examples of where the University holds personal information:

a. staff calendars;
b. annual reports;
c. staff and case management files including records of professional performance and conduct of an employee at the University;
d. books, articles, papers or other publications by members of staff;
e. information technology records, including email, internet access and usage, WesternNow, SMS and live chat functions;
f. the University's electronic recordkeeping system, Content Manager (TRIM) which contains, among other things, all staff personal files;
g. electronic or hard copy files of student records, employee records or records containing information about third parties;
h. the University's student management system;
i. records and information management systems;
j. the University's human resources and recruitment management systems;
k. career development and management system;
l. welfare and counselling services records;
m. complaints handling system;
n. the business and finance system;
o. library systems;
p. University electoral rolls;
q. student/staff evaluation records;
r. conflicts of interest registers and forms;
s. debtor records; and
t. library loan records.

Section 5 - Storage and Maintenance of Information

(31) The University is legally obliged to protect the personal and health information it stores, including preventing unauthorised use or disclosure, and disposing of the information securely and in accordance with any other retention and destruction laws. In addition to the requirements under the PPIPA and the HRIPA, the University is bound by specific provisions in the State Records Act 1998 (NSW) and the Government Information (Public Access) Act 2009 (GIPAA).

(32) Schools and organisational units must adopt processes to secure employee and student personal information and enable access to that information only in accordance with this PMP. Staff must only have access to information systems for legitimate purposes to enable them to perform the requirements of their position at the University.

(33) The University's Records and Archives Management Policy also sets out the standards for creating, maintaining, and legally destroying University records and archives.

Storage of Personal Information Outside the University

(34) The University may need to store information or data outside the University (including outside New South Wales),

for example by using an off-site commercial storage facility to store paper records, or by engaging a third party to host and manage electronic records or data (including by means of cloud storage).

(35) In these cases, the area of the University responsible for managing these activities or contract must complete a Privacy Impact Assessment (PIA) beforehand to ensure the activity meets privacy obligations. For Information Technology and Digital Services related systems, this includes undertaking a Risk and Compliance Review (refer to the Digital Services Implementation Policy).

(36) In addition, the University will ensure that third party contracts incorporate appropriate obligations to ensure compliance with the PPIPA (and, to the extent applicable, any other privacy laws) and this PMP.

(37) Refer also to the section headed Transborder Data Flow of Personal Information regarding data that may contain personal information that is transferred outside of New South Wales.

Student Records

(38) Student records about admissions and enrolment are the responsibility of the University's Data Integrity, Quality and Operations unit. Each individual student of the University has an electronic file within TRIM, the University's recordkeeping system.

(39) Student records about health and welfare services are the responsibility of the University organisational unit responsible for the provision of those health and welfare services. Such records are held in a separate secure database only accessible to authorised staff.

(40) TRIM restricts access and controls input to student records by granting various levels of access rights to University staff. Only authorised staff can create, access, or amend student records.

(41) All University staff that access student records within TRIM must ensure that the records are kept secure, treated confidentially, and protected from unauthorised access or misuse. Staff who are required to use TRIM are trained and given explicit warnings that all information is confidential and must only be collected, accessed, used, disclosed, amended, or deleted by staff authorised to do so and only for the official business of the University and not for any personal or other use.

(42) The University also creates, stores and uses digital images of students for legitimate University identification purposes. The use of student images for other University purposes (such as publicity) is only permissible upon the receipt of a student’s signed consent form authorising the particular purpose and for a specified period of time. The consent form must be stored and linked to the image. Model release forms are available from the Office of General Counsel (OGC). The image must be deleted or destroyed when the authorised time period has lapsed.

Employee Records

(43) Employee records are the responsibility of the Office of People. Electronic personal or confidential information about staff should only be held in TRIM or formal University systems, such as Acentre, and should never be held in collaborative areas, such as share drives and Sharepoint.

(44) Staff in Office of People have access to employee records in the course of their official University duties and for no other purposes.

(45) Records relating to staff grievances, disciplinary matters or other sensitive information are held in a separate Office of People TRIM file. The exceptions to this include proven cases of misconduct and unsatisfactory performance. In these instances investigation reports, allegations, employee response to allegations and letters of outcome are placed on the employee’s personal file.

(46) Some information contained in employee records may not be covered by the PPIPA, particularly information about a person's suitability for employment with the University. This may include a selection panel report, a referee's report, a job application or records relating to misconduct. This information is treated by the University as confidential and access to those records is restricted. However, this information may be requested for release under the GIPAA or the University may be required to produce it by law to a court, tribunal or government agency (for example, a subpoena).

(47) The University also creates, stores and uses digital images of staff for legitimate University identification purposes. The use of staff images for other University purposes (such as publicity) is only permissible upon the receipt of the staff member's written consent form authorising the particular purpose and for a specified period of time. The consent form must be stored and linked to the image. Model release forms are available from the Office of General Counsel (OGC). The image must be deleted or destroyed when the authorised time period has lapsed.

Research Records

(48) Under s.27B of the PPIPA, there is an exemption that applies to the collection, use or disclosure of personal information used for research purposes, or the compilation or analysis of statistics in the public interest, provided that specific conditions are met. Staff engaged in research that wish to access personal information held by the University for research purposes should refer to the NSW Information and Privacy Commissioner's Statutory Guidelines on Research – Section 27B for more information and consult with the University's Privacy Officer or the Office of General Counsel. Approval from the University's authorised delegate is required before any information can be provided.

(49) Research records are the responsibility of the staff and students conducting that research. The University does not have a central repository for research records within TRIM. The University's Research Data Management Policy specifies the responsibilities of the University, its researchers and research students regarding the management of research data.

(50) The University's Research Code of Practice details the compliance requirements relating to research records in accordance with the Australian Code for the Responsible Conduct of Research, 2018.

(51) The University manages and stores its research data as detailed in the University's Research Data Management Policy to ensure compliance with relevant legislation covering data retention, accessibility, storage and security, that the validity of the data can be demonstrated as required and also to meet its PPIPA obligations. Individual researchers should not hold the only copy of the data and must ensure that a copy of the original data is retained in the academic unit, school, or research unit in the University where the chief investigator(s) is normally employed or is based for the purposes of that research project.

University Community Engagement and Public Events

(52) The University holds or hosts public or publicly accessible events for the purposes of community engagement, including lectures, seminars and performances at University venues or by electronic means such as videoconferencing and live streaming. The University also regularly holds graduation ceremonies both at its Australian campuses and at overseas venues (for the benefit of graduating international students) or by using live streaming or audio or other electronic means.

(53) While most information and data collected through these activities (including filming or photographing these events for broadcast, including by means of live streaming on the University's website) are in the public domain, there is some information collected and maintained on a continuing basis, but which is not public and is protected by the PPIPA. This includes:

a. records of prospective students, collected, held and used by the Office of the Pro Vice-Chancellor, Engagement and Advancement;
b. a University alumni database generated from the University's graduation records and which includes contact

details;

c. donor records containing contact details and other personal information about individual donors as well as details of donations (including gifts and bequests) made; and
d. University collections record containing contact details and records of visits and access to University collections by individuals.

Section 6 - How does the University Collect Personal Information?

Requirements

(54) The University must only collect personal information and health information that is necessary for a function or activity of the University. The University's functions include learning and teaching, research, administration, welfare and community advocacy, development and engagement. However, there are other functions of the University that require the collection of personal information and health information, as detailed elsewhere in this PMP.

(55) The University collects information from individuals directly, unless they have authorised collection of the information from someone else, that is, it is provided by a parent or guardian for a person under the age of 16, or the individual lacks capacity (including temporarily) to provide that information directly (for instance, if the person is involved in an accident).

Examples of Information Collected

(56) Some ways in which the University may ask an individual to provide personal information or health information include:

a. in meetings or interviews held in person or via electronic means, phone conversations, lectures or tutorials held in person or via electronic means where information is recorded about a person and either directly or at a later time uploaded onto a storage system operated by the University;
b. as written data either in an electronic (including online) or hard copy form, such as application forms, enrolment forms, tender documents, student/staff evaluation forms, competitions and surveys;
c. in the ordinary course of teaching functions carried out within the Schools and organisational units of the University, including participation in recorded lectures and tutorials, online forums, submission of assessment work, student placements and presentations;
d. in the course of providing digital (including online or mobile) services, for example, participation in a competition, or live chat forum;
e. in the ordinary course of commercial business undertaken by the University when engaging with external organisations or third party contractors;
f. pursuant to a statutory or other legal obligation.

(57) Individuals may also volunteer solicited or unsolicited information, for example, via student surveys that the University undertakes to improve its services or students' experiences at University, or that give individuals more choices with the type or of services or activities they can access.

Information Provided to Individuals

(58) When collecting personal information, the University will take all reasonable steps to ensure the individual understands how and why their information is being collected. Where applicable, individuals will be told of any consequences if they do not provide the information, for instance, that a service is unavailable or limited or an

application may be refused.

(59) The Student Declaration sets out how personal information is collected, used, disclosed and destroyed by the University.

(60) Health information is usually collected from students directly by the University's Equity, Safety and Wellbeing staff and students must complete a separate consent form prior to that collection. Health information is usually collected by staff on an as needs basis, such as when processing sick leave applications.

(61) The University generates some personal or health information itself – for example, academic transcripts and records, and applications or requests related to students' academic progress (disruption to studies, academic withdrawal without penalty for example). The University treats such information as personal or health information and complies with the rules regarding the use and disclosure of that information in accordance with, as the case may be, the PPIPA and the IPPs or the HRIPA and the HPPs.

Information Received from Third Parties

(62) The University may receive information from third parties, including through third party suppliers or service providers. The University handles that information as it does information collected directly from individuals in accordance with this PMP.

(63) There are some circumstances where the University is exempt from aspects of the collection principle and may collect information from third parties, including:

a. the Universities Admissions Centre (UAC), as part of a student's application process. Applicants provide authority for UAC to liaise with the University as part of the application process, which in turn requires information to move between the University and UAC to process an application;
b. contractors or agents engaged by the University to provide services or conduct activities on behalf of the University, for example, to recruit overseas students;
c. schools, hospitals and other organisations involved with supervising University students who undertake placements and other work integrated learning experiences. This forms part of individual program requirements and relevant consents are provided during the enrolment, registration or placement process;
d. other education providers and professional registration bodies for the purpose of verifying qualifications. The University may verify where a prospective student or staff member claims qualifications or has indicated previous study;
e. health care providers, where professional authority (including verification or confirmation of issue of a medical certificate or opinion) is required in support of a disruption to studies application by a student;
f. next of kin or attorney appointed under a power of attorney in relation to a deceased individual or an individual who lacks capacity (including temporarily) for any reason (for instance, if the individual is involved in an accident);
g. parents and legal guardians for individuals who are under 16 years of age.

(64) From time to time, the University may receive personal information about a member of the University community that it has not actively collected or sought, from third parties such as law enforcement agencies and other government departments. The University treats this as unsolicited information and does not have to comply with the IPPs or HPPs in relation to its collection. However, the requirements of this Plan apply to the storage, use or disclosure of unsolicited information containing personal information.

Automated Collection

(65) The University also collects information by automated means including:

a. security cameras located throughout and across all University campuses;
b. video recordings used for assessment purposes, including assessment of clinical and other placements;
c. digital and online means (including the University's website or mobile services). This includes information gathered to monitor access to and use of, or gather feedback about the accessibility and quality of, University infrastructure and services;
d. the University's network and other technology and communications systems (such as WiFi) that records login and other identifiers of users or their devices;
e. audio, video or images taken or live streaming of learning and teaching activities and events (including graduation ceremonies, lectures and tutorials).

(66) Information collected using automated means is collected from individuals through their participation in an activity or use of a system. Where possible, the University will take steps to ensure that automatic collections are open and transparent through relevant notices or signage, terms and conditions or other methods of communication.

Section 7 - How does the University Use Personal Information it Collects?

Limits on Use

(67) The University limits use of personal information and health information as required under the PPIPA to one or more of the following circumstances:

a. it is used for the primary purpose for which it was first collected;
b. the proposed use is directly related to the purpose for which the information was collected;
c. the individual concerned has consented to the use of the personal information.

(68) There are specific use and disclosure exceptions permitted under the PPIPA, discussed below. Additional obligations relating to the use of health information are discussed in Section 22 – Annexure B.

(69) Surveillance information or records relating to University staff, as defined in the Workplace Surveillance Act 2005 may only be accessed or used in accordance with the University's Workplace Surveillance Policy or where a covert surveillance order has first been obtained under the Workplace Surveillance Act 2005.

Consent

(70) The University obtains consent from individuals at the first point of contact the individual makes with the University and then from time to time as necessary. Examples of consents obtained can be found in the Student Declaration and enrolment forms and at the time of staff engagement through employment.

(71) “Bundled consent” is not a legitimate form of consent and must not be used. Bundled consent refers to the practice of an organisation ‘bundling’ together multiple requests for an individual’s consent to a wide range of collections, uses and disclosures of personal information, without giving the individual the opportunity to choose which collections, uses and disclosure they agree to and which they do not.

Accuracy of Information Held by the University

(72) The University must take steps to ensure the accuracy of the personal information it uses and that the information is relevant, accurate, up to date, complete and not misleading. The University relies on the individuals providing the personal information to provide information that is accurate and to notify the University of any changes, for example changes of names, addresses and other contact details. Individuals are usually informed of their

obligations at the time the information is collected, as set out in documents such as the Student Declaration.

Section 8 - How does the University Disclose Personal Information to Others?

Limits on Disclosing Information

(73) The University limits disclosure of personal information as set out under the PPIPA to another person or body in one or more of the following circumstances:

a. the disclosure is directly related to the purpose of collection and the University does not believe the individual concerned would object;
b. the individual concerned is reasonably likely to be aware of the disclosure;
c. disclosure is necessary to prevent or lessen a serious and imminent threat to the life or health of the individual concerned or another person; or disclosure of the information is reasonably necessary to assist in a state of emergency.

(74) There are specific use and disclosure exceptions permitted under the PPIPA, discussed below. Additional obligations relating to the use of health information are discussed in Section 22 - Annexure B.

Public Registers

(75) The University maintains an Award Verification Service which is a database that can be accessed by members of the public and searched via the University's website. The Service allows searches of graduates' names, awards conferred and conferral dates.

(76) This is a public register for the purposes of the PPIPA and its purpose is to protect the value and integrity of qualifications conferred by the University and its antecedent institutions.

Other Information that can be Accessed by Third Parties

(77) The University makes some information available through its website and publications, including publications that are publicly accessible, for example graduation booklets.

(78) The University will also confirm to third parties the existence of a qualification (see clause 132) or authenticity of a University document, including a transcript, testamur or other academic record provided by the University or any of its antecedent institutions. This is a matter of public interest and is considered vital to protect the value and integrity of qualifications conferred by the University and its antecedent institutions.

Use of Social Media and Livestreaming

(79) The University uses public social media platforms increasingly as a means of communicating with current and potential students. Images of students, staff and others posted to public social media domains are limited to those images for which a consent form can be matched, as per clauses (42) and (47) of this Plan.

(80) The University uses Yammer as an internal organisational social network that can be accessed by University staff.

(81) When using social media, users are expected to not use it to collect or disclose any personal information. Any communications made to University students or staff must comply with the PPIPA and this PMP.

(82) The University also broadcasts (including by livestreaming) public events and activities through its website, including graduation ceremonies.

Transborder Data Flow of Personal Information

(83) There are special restrictions regarding the transborder (outside of New South Wales) data flow of personal information under PPIPA. These align with the requirements of transborder data flow under the HRIPA.

(84) In the course of its business, the University may provide or receive personal information to or from organisations outside New South Wales (including outside Australia). This includes information regarding overseas students. The University will only provide this information to those organisations:

a. where it believes the recipient is subject to a law, binding scheme or contract that uphold principles for fair handling of the information that are substantially similar to the information principles under the PPIPA or the HRIPA;
b. where an individual expressly consents to the transfer of the information;
c. where the transfer is necessary for the performance of a contract between the individual and the University including implementation of pre-contractual measures at the individual's request;
d. where the transfer is necessary for the performance of a contract in the interests of an individual between the University and a third party;
e. where the transfer is otherwise required or permitted by law.

(85) Examples of contracts referred to in clause (84)d. include arrangements with third party providers of cloud-based technologies, data storage facilities or digital services (including online and mobile services, such as "live chat"). See clause (36) of this PMP.

(86) The University does not transfer personal information or health information to organisations outside New South Wales except as permitted under the PPIPA or the HRIPA, and the circumstances referred to in clause (84).

Section 9 - Exemptions

Overview of PPIPA Exemptions

(87) Division 3 of PPIPA sets out the exceptions to compliance with IPPs. The exemptions relevant to University operations are set out below.

(88) These should not be read as an exhaustive list of exemptions and any University officer unsure whether an exemption applies when handling personal information in their role should discuss the matter with their supervisor or contact the Privacy Officer.

Serious and Imminent Threat

(89) The University may use personal information and disclose it for the purpose of preventing or lessening a serious and imminent threat to the life or health of a person.

(90) This exception has been determined by the NSW Civil and Administrative Tribunal (NCAT) to be permitted in very limited circumstances. The threat must be both serious and imminent: imminent meaning likely to occur at any moment, or impending. There must also be a belief held on reasonable grounds about the serious and imminent threat by the officer of the University when this exception is relied on.

(91) Staff involved in assessing any threat should speak to their supervisor and also contact the University's Privacy Officer and/or the Office of General Counsel for advice.

Investigations

(92) The University is not required to comply with the privacy obligations under the PPIPA if:

a. it is investigating or otherwise handling a complaint and compliance might detrimentally affect the proper handling of its investigative function; or
b. non-compliance is reasonably necessary to enable the University to exercise its complaint handling functions; or
c. the information is disclosed to an investigative agency.

Law Enforcement Purposes or Otherwise Lawfully Authorised

(93) The University is not required to comply with the obligations under the PPIPA if:

a. the information is collected for law enforcement purposes; or
b. the information is collected in connection with any proceedings (whether or not actually commenced) before any court or tribunal; or
c. use of the information is reasonably necessary for law enforcement purposes or the protection of public revenue; or
d. disclosure of the information is:
    i. made in connection with proceedings for an offence or for law enforcement purposes; or
    ii. to a law enforcement agency for the purposes or ascertaining the whereabouts of a missing person; or
    iii. authorised or required by subpoena or by search warrant or other statutory instrument; or
    iv. reasonably necessary for the protection of public revenue or to investigate an offence where there are reasonable grounds to believe an offence may have been committed; or
e. disclosure of the information is reasonably necessary to assist in a state of emergency; or
f. the University is otherwise lawfully authorised or required not to comply with the PPIPA, or non-compliance is permitted under any Act or law.

(94) A reference to “law enforcement purposes” includes law enforcement purposes of any state or territory, or the Commonwealth, of Australia.

(95) Examples of other legislation which may authorise non-compliance include the GIPAA, the State Records Act 1998 (NSW) and the Data Sharing (Government Sector) Act 2015. The operation of this and any other legislation that permits non-compliance with the PPIPA does not affect the University's handling of the personal information and health information, other than for the purpose of the exempt conduct.

Other Exemptions

(96) The University is also exempt from various provisions of the PPIPA where:

a. the individual concerned has expressly consented to non-compliance with particular provisions;
b. it discloses to or receives from another agency information about an individual in any of the circumstances described in section 27A of the PPIPA, including for the purpose of enabling inquiries to be referred between the University and that other agency;
c. the collection, use or disclosure of the information is reasonably necessary for research and the matters in section 27B of the PPIPA apply.

(97) The University may also have mandatory reporting obligations to regulatory bodies, such as the NSW Independent Commission Against Corruption (ICAC), and other government agencies.

Disclosure of “Sensitive” Personal Information

(98) The PPIPA provides a restriction on disclosure for “sensitive” types of information, which are defined as an individual’s ethnic or racial origin, political opinions, religious or philosophical beliefs, trade union membership, or sexual activities. The University will not disclose this type of information unless it is necessary to prevent a serious and imminent threat to the life or health of an individual.

(99) It should be remembered that sensitive personal information may be contained in identification documents, such as passports and drivers’ licences. For example, photos might establish racial origin or religion and a document evidencing an individual’s marital status may disclose their sexual orientation.

Section 10 - How does the University Destroy Personal Information?

Requirements

(100) Destruction of personal information by the University will always be undertaken in accordance with University policy and its obligations under the State Records Act 1998 (NSW). If there is a contract in place between the party who has provided the personal information and the University, any destruction obligations contained in that contract must also be complied with, subject always to the requirements of the State Records Act 1998 (NSW).

(101) The University cannot destroy records that are, or may be, the subject of a request under the GIPAA, subpoena or other formal request for access, or relate to any ongoing action, such as an appeal, regardless of whether the minimum statutory retention period has expired.

Section 11 - How does Privacy Interact with Changes to Technology or Projects that Involve Handling Personal Information?

Changes to Technology and Projects Handling Personal Information

(102) The University acknowledges that technology is constantly changing and seeks to embrace those changes while at the same time maintaining legislative compliance. The University aims to utilise the most up-to-date technology to meet its key functions and to enhance the student experience. The University is working to adopt new technologies to enhance the student experience and allow staff and community members to best utilise technology in their practices to meet the key functions of the University.

(103) The University has in place policies regarding data storage, information technology security, and systems approval and implementation to ensure that the University complies with all relevant laws and industry standards regarding data security.

(104) In embracing new technology, the University will ensure that its information technology contractors are able to meet these standards and the requirements in this PMP. The University cannot abrogate its statutory obligations when it contracts with technology providers, and business units are responsible for ensuring that contractual arrangements include terms and conditions that comply with the University's policies related to procurement and implementation of systems handling personal information.

(105) Users of University information technology are informed if they are using software or services that operate

outside or independently of systems or services operated by or on behalf of the University. When using these systems, students and employees should be aware that the PPIPA may not apply and they should check the relevant privacy policy of any third party software or service provider before providing their personal information. This is particularly important when providing personal information that may be stored overseas and/or in systems utilising cloud-based technology.

(106) University staff using personal devices for business purposes must also ensure that they comply with the relevant University policy in relation to storage and disclosure of personal or health information. At a minimum, staff using personal devices should always ensure their device is protected or secured in accordance with University policies relating to the acceptable use, and security, of devices including by using a security password or passcode to prevent unauthorised access. For more information on the acceptable use of personal devices, refer to the Acceptable Use of Digital Services Policy.

Privacy Impact Assessments (PIAs)

(107) A Privacy Impact Assessment (PIA) is a risk assessment tool designed to identify the impact that the technology or project may have on the privacy of individuals and for identifying and evaluating solutions to mitigate privacy risks. PIAs must be undertaken for any new or revised project or process which has the potential to impact on the collection, storage, access to, use or destruction of personal information, or when making changes to existing ways of handling personal information. Some examples include:

a. collecting personal information in a new way, or from a new demographic (e.g. a new digital service, a new form to collect personal information, international student recruitment processes, digital marketing, or creating and implementing a new University digital service);
b. collecting personal information in a way that might be perceived as being intrusive (e.g. quantity or type of data, marketing purposes, images of personal spaces, University clinics);
c. disclosing personal information to a third party (in both the public and private sectors) such as a company, government agency, or a contractor where the University is either legally required to disclose personal information (such as for taxation purposes), or when disclosure is necessary in order to receive a service or meet the conditions of an agreement (such as providing information to a travel agent or to a student placement provider);
d. sharing personal information which has previously been collected by the University for a specific purpose, with another University digital service or department for a new or secondary purpose (e.g. new integration to transfer personal data from one digital service to another, including the Data Warehouse; or where the University wishes to use information collected from a student on enrolment for another purpose, such as a marketing purpose, or where the University wishes to later contact people who have previously attended an unrelated University event for fundraising purposes). This requirement also applies where personal information of a sensitive nature (eg, health-related information) is collected in the course of a confidential internal process or service (such as counselling). “Bundled consent” (meaning, assuming that if a person consents to one form of use it means they have also consented to any other form of use) is not a legitimate form of consent and must not be used;
e. there is a change in the way personal information is stored or secured (e.g. change to hosting vendor, change to data centre hosting location, or change to security controls) and paper formats (e.g. paper stored in a locked filing cabinet, paper transferred to digital via scanning processes, paper stored in an off-site records retention facility, microfiche converted to digital images and stored in a new/existing digital service).

(108) PIA’s should also be completed for any activities to which the foreign privacy legislation, such as the GDPR, may apply.(Refer to Section 17).

Section 12 - How can an Individual Access and/or Amend their Personal or Health Information held by the University?

Access

(109) The University must, when requested to do so, provide an individual with access to their personal information or health information it holds.

(110) The process to request access to personal or health information under the PPIPA or the HRIPA held by the University will depend on whether the individual is a student, staff member, member of the general public or a third party organisation.

(111) The University must be able to verify the identity of an individual when requests are made to access or amend personal or health information. The University may refuse access or amendment of personal or health information if it is unable to confirm the individual's identity through the appropriate verification process.

Amendment

(112) The University will amend personal and health information it holds about an individual at the request of the individual to ensure it is accurate and, taking into account the purpose for which that information was collected, is relevant, up to date, complete and not misleading.

(113) The University may refuse to amend information in certain circumstances, for example:

a. the change cannot be made due to system limitations or design;
b. the amendment is contentious (for instance, where an employee or a student seeks a change in a University decision that they disagree with);
c. the change conflicts with any laws, or with University requirements with respect to governance and record keeping;
d. the change would result in the information being out of date, inaccurate or misleading.

(114) If the University refuses a request to amend information, the individual will be advised of the decisions and reasons why, as well as any right to have that decision reviewed. For more information, refer to Section 13 of this PMP.

Requests by University Students

(115) My Student Records (MySR) is where students can view and manage their student record online. A student may amend certain personal information, such as their address, personal and emergency contacts, through MySR.

(116) For information not available through MySR, a student may apply to inspect and/or amend their student records (excluding records held in Equity, Safety and Wellbeing) either:

a. in writing to the Senior Manager, Completion, Enrolment and Load Data by email from the student's University student email account; or
b. in person or at Student Central (which are the University's face-to-face contact service points for students).

(117) A student seeking access to their student records (those records not available through MySR) must put their request in writing. An appointment will be arranged for the student to view their file in the presence of a staff member familiar with the student. A student may receive a copy of their records but must provide a signed release form or

other form of identity verification.

(118) University staff will require students to identify themselves on the basis of information held by the University, and may either request photo identification, or to undertake additional verification steps to verify the student's identity.

(119) Parents and guardians of students do not have an automatic right of access to any personal information held by the University about their child or ward. The written consent of the student will be required before student information is released. Students should complete the Consent to Release Personal or Health Information To Third Parties (Students) Form and provide it to the University via their student email account or in person at a Student Central.

(120) There may be situations where a student is granted access to only part, or a redacted form, of their student record if, for example, release of the complete record would breach another person's privacy.

Requests by University Employees

(121) An employee must apply to Office of People in order to inspect those electronic employee records that are not available to them already. An employee can view their electronic personal information in the presence of an Office of People staff member.

(122) An employee may amend certain personal information, such as their address, personal and emergency contacts through the University's Staff Online portal, or via the University's service and knowledge portal, WesternNow. Other personal information can only be amended by contacting Office of People directly, such as a staff member's name, tax file number, date of birth and qualifications.

(123) An employee may request to amend personal information on their record. In the case of a disagreement between the University and the employee about the amendment, the employee is entitled to put a statement on their record of the amendment sought.

(124) Any employee who requires assistance with a request should contact their Senior HR Partner.

Request by Third Parties

(125) An application to inspect and/or amend personal information held by the University about a member of the general public may be made to the University's Right to Information Officer.

(126) Disclosure of personal information of a student, staff member or any other individual in the University community can only be made in accordance with the PPIPA and the disclosure principles referred to in this document, or as otherwise permitted by law.

(127) The PPIPA provides an emergency exception to disclosure of personal information where necessary "to prevent or lessen a serious and imminent threat to the life or health of the individual to whom the information relates or to another person." Any University staff approached for information on this basis should, in consultation with their manager:

a. if practicable, seek to have the request in writing;
b. record the details of the person making the request;
c. establish the nature of the "serious and imminent threat" to life or health;
d. contact the student concerned and notify them of the request if uncertain about whether a serious and imminent threat exists;
e. if practicable, seek advice from the University's Privacy Officer and/or Office of General Counsel;
f. provide only such information that is necessary to mitigate the serious and imminent threat; and

g. make a formal record of the request and the action taken and forward it to their unit head and to the University's Privacy Officer.

(128) The University must adhere to directions to produce information contained in legal documents, such as subpoenas, warrants, court orders, and other legally binding instruments. All documents of this kind must be directed to the Office of General Counsel for review and advice.

(129) The University may also be required to disclose personal information about individuals to external agencies or government bodies, such as the Universities Admissions Centre; Centrelink; Department of Education; Department of Employment and Workplace Relations; Department of Home Affairs; the Australian Taxation Office, and other bodies in accordance with any statutory or other legal obligations. All requests from Commonwealth or NSW government agencies or statutory bodies should also be reviewed by the Office of General Counsel.

(130) The University will usually only supply academic records in response to requests from other universities or educational institutions where the student provides express consent to transfer personal information contained in their student file.

(131) In the case of all other requests made by third parties (such as insurance companies), the University requires the written consent from the individual whose personal information is requested. The University must be satisfied that such request has the authorisation of that individual and for this purpose may take additional steps as necessary. For example, it may direct that the consent form be emailed from the person's University email account or require verification of the individual's identity or signature from documents held on file by the University, or by contacting that individual directly.

Information about University Graduates

(132) Information about University graduates, including a graduate's name, academic award and year of conferral, is made publicly available on the University's Award Verification Service which is treated as a public register (refer to the section in this PMP headed "Public Registers"). Any additional information sought about a University graduate must follow the processes required for any third party request.

Verification of Identity

(133) University staff will identify individuals on the basis of primary source information held by the University.

(134) Where information is sought by telephone, a formal verification process must be applied to ensure the identity of the caller is established beyond doubt.

(135) In all requests for access to personal or health information, the University may direct the individual to lodge a written request to be provided, as appropriate, from the student or staff email address or by providing an original consent form signed by the individual.

Who to Contact

(136) Any person, other than a current employee or student, who has an enquiry as to whether the University holds their personal information or health information, the nature of that information and the purpose for which it was collected should contact the Right to Information Officer at the University at rti@westernsydney.edu.au. An application to inspect University records may also be made under the GIPAA through the University's Office of Governance Services.

Section 13 - Complaints in Relation to Privacy Matters

Introduction

(137) Under the PPIPA, individuals who feel aggrieved by the University's conduct are entitled to an internal review if it is alleged that the University breached:

a. a privacy protection or health privacy principle; or
b. a privacy code of practice applying to the University; or
c. the public register provisions of the Act.

(138) If a matter does not fall into one of these categories, then it will be dealt with as a regular complaint. If it is unclear whether the matter should be an internal review or not, the Privacy Officer may write to the complainant seeking clarification of the nature of the complaint.

(139) A person aggrieved may also complain directly to the NSW Privacy Commissioner. More information on this process can be found on the NSW Information and Privacy Commission - Complaint webpage.

Internal Review Applications

(140) An internal review application must be:

a. in writing; and
b. made by the person whose personal information is said to have been the subject of the conduct of the University; and
c. addressed to the University's Privacy Officer.

(141) The University's Privacy Officer can be contacted through on (02) 4570 1428 or by email at privacy@westernsydney.edu.au.

(142) The University's internal review application form can be found on the University's Privacy website.

(143) Applications must be lodged within six months from the time the complainant first became aware of the conduct that is the subject of the application.

How is the Internal Review Conducted?

(144) In most cases, the University's Privacy Officer or the Associate Director, Complaints Management and Resolution will conduct the internal review on behalf of the University. However, if either of those persons is unable to conduct the review for any reason, the University's Privacy Officer may designate another appropriate person to do so.

(145) The person conducting the internal review must:

a. be an employee or officer of the University; and
b. have had no substantive involvement in matters that are the subject of the application; and
c. be suitably qualified to deal with the matters raised in the application.

(146) In accordance with the requirements of the PPIPA, the University must notify the NSW Privacy Commissioner of the internal review applications it receives, the progress made in dealing with applications, and any findings and actions taken. The NSW Privacy Commissioner may make submissions to the University with respect to applications

for internal review and the University will consider such submissions when finalising the internal review.

(147) The internal review must be completed by the University within 60 days from the day on which the application was received. Following the completion of the internal review, the University has 14 days in which to advise the applicant of the outcome. Once a review has been completed, the University may decide to do one or more of the following:

a. take no further action
b. make a formal apology
c. take appropriate remedial action, which could include payment of compensation
d. give an undertaking that the conduct will not recur; or
e. implement measures to prevent recurrence of the conduct.

Notification to the Complainant

(148) When notifying the complainant of the outcome of the request for internal review, the following information will be provided:

a. findings of the review;
b. the reasons for the finding;
c. the action(s) proposed to be taken;
d. the reasons for the proposed action(s); and
e. the applicant’s right to a review of the finding to the NSW Civil and Administrative Tribunal (NCAT).

(149) If a complainant is not satisfied with the outcome of an Internal Review, or if the University has not dealt with the matter within 60 days, they may make an application for review to NCAT.

(150) Alternatively, a complainant dissatisfied with an outcome may seek to resolve the matter informally through the University's Complaints Resolution Unit.

Assistance with Complaints

(151) The University cannot provide any legal advice in relation to an internal review. Some procedural assistance with applications may be provided by the University's Privacy Officer.

(152) The University will provide information via email upon request, and on the University's Privacy website.

Section 14 - How the University Handles Breaches of Privacy

Reporting

(153) A privacy breach occurs when there is unauthorised access to or collection, use or disclosure, loss or disposal of personal information held in the custody or control of the University (or a third party on behalf of the University) in contravention of the PPIPA or, where relevant, the Federal Privacy Act.

(154) Any University employee who becomes aware of an actual or potential privacy breach must immediately inform their unit head and the University's Privacy Officer. If the privacy breach involves any University systems (for example, suspected or actual hacking) that person should also report it to the Chief Information and Digital Officer.

(155) The University's Privacy Officer will, in consultation with the relevant unit head and, where applicable, the Chief Information and Digital Officer, decide the next steps taking into account the extent and seriousness of the alleged breach.

Containment and Risk Assessment

(156) The University's Privacy Officer is responsible for ensuring appropriate steps are taken to limit the extent and effect of any breach, which may include:

a. working with other units to secure or restrict access to systems or recover records;
b. notifying the police or other relevant statutory bodies if the breach involves criminal or corrupt activities;
c. mandatory notification where required by law (refer to the section of this PMP headed “University processes”).

(157) The University's Privacy Officer will, in conjunction with other University staff as necessary, assess risks associated with the breach, including:

a. cause and extent;
b. type and level of exposure (eg, risk to public health or safety, financial, reputational, etc);
c. risk of further exposure;
d. number and identity of individuals affected (including whether they are University staff, students, alumni or others);
e. notification to affected individuals;
f. and notification to the NSW Privacy Commissioner.

Prevention

(158) Following steps to mitigate risks associated with the breach, the University's Privacy Officer will investigate the cause of the breach, which may involve a security audit of physical, organisational and technological measures. Existing policies and processes will be reviewed to implement any lessons learned from that investigation including audit recommendations.

Section 15 - Law Enforcement and Litigation

Collection

(159) The University may collect information if it is in connection with court or tribunal proceedings in which the University is involved.

(160) The University may also collect information if it is for law enforcement purposes or it is to be provided to a law enforcement agency in accordance with the PPIPA.

Disclosure

(161) The University receives subpoenas or demands for the production of documents from time to time in legal claims and proceedings. There are a number of different ways in which courts, tribunals or others can legally demand information from the University. If a demand is made in this way, which has the force of law, the University may be compelled to disclose the personal information of others.

(162) The University may also disclose personal information of individuals as evidence in connection with any complaint, investigation or proceeding under the PPIPA or any other law (for instance, a claim for unlawful discrimination under a Commonwealth or a State Act) and to which the University and that individual are parties.

Section 16 - Federal Privacy Laws

(163) There is often confusion between the operation of the Privacy Act 1988 (Cth) (Federal Privacy Act) and the PPIPA and the HRIPA. The University is defined as a "public sector agency" under the PPIPA and the HRIPA and must comply with the privacy obligations arising under those laws, which are the University's primary privacy obligations.

(164) The Federal Privacy Act and the Australian Privacy Principles apply to private and public sector organisations that fall within the definition of an "APP entity". The University falls within the definition of a "State or Territory authority" for the purpose of the Federal Privacy Act.

(165) However, there are some circumstances in which the Federal Privacy Act applies to the University, for example in the handling of tax file numbers and in its contractual relations with the Australian Government and its agencies, including funding bodies such as the Australian Research Council. The University at all times complies with the terms of these obligations.

Section 17 - Privacy Regulation of Foreign Countries

Applicability

(166) Foreign privacy regulation, such as the GDPR, may apply to a variety of University activities including:

a. processing of personal information of individuals located in the countries or area covered by the regulation, in respect of the GDPR it covers countries within the European Economic Area (EEA) and the United Kingdom (UK). (In the GDPR, "processing" has a similar meaning to "handling" and "personal data" has a similar meaning to "personal information");
b. where the University offers goods or services in countries or areas covered by the legislation, such as the EEA or UK, irrespective of whether payment is required (for example, where the University actively promoting programs to residents in those countries or areas);
c. where the University enters into a contract with an entity located in that country or area, which involves the processing of personal information and disclosure of it out of that country or area to the University, and vice versa;
d. where the behaviour of individuals located in that country or area is being monitored or tracked, for example, by the use of cookies on the website; and
e. in research collaborations with entities in that country or are which include collecting and processing personal data.

(167) Under some foreign privacy regulations, such as the GDPR, it is a requirement where information is collected, used or disclosed as a result of express consent given by an individual, that consent may be withdrawn by that individual at any time. The individual may have the right to request the erasure, portability or restriction of processing of their personal data, and to object to the processing of their personal data.

(168) To access, correct or rectify personal information or for further enquiries, please contact the University's Privacy Officer on (02) 4570 1428 or email privacy@westernsydney.edu.au.

Section 18 - Notifiable Data Breaches

Description of Regime

(169) The Australian Government has established a Notifiable Data Breach Scheme ("NDB Scheme") under the Federal

Privacy Act to ensure that individuals are notified about serious data breaches of their personal or health information. The NDB Scheme took effect from 22 February 2018. At the time of approval of this Plan, there is no requirement for mandatory reporting under the PPIPA or the HRIPA.

(170) A notifiable data breach is a data breach that is likely to result in serious harm to an individual to whom the personal or health information relates. A data breach occurs when personal or health information held by an organisation becomes lost or if any unauthorised access, modification, disclosure or other misuse or interference occurs. Examples include where data systems are hacked or where personal information is provided to a third party in error.

(171) The NDB Scheme applies directly to the University in limited circumstances, including because it holds the tax file numbers of employees and students for the purposes of complying with its statutory obligations.

(172) The NDB Scheme also applies to the University in circumstances where it holds unsolicited personal information such as Individual Health Identifiers.

(173) In addition, the NDB Scheme applies to contractors and other organisations with which the University does business because they are subject to the Federal Privacy Act. Some of those contractors or organisations may have access to or store personal or health information on behalf of the University. A typical example is a third party engaged to provide cloud hosting services for the University (see clauses 34 and 84).

University Processes

(174) The University will establish processes for responding to data breaches and reporting notifiable data breaches in line with the requirements of the Federal Privacy Act and, as applicable, other Australian laws, such as the PPIPA and the HRIPA and, where applicable, foreign privacy laws such as the GDPR.

(175) The University will incorporate standard provisions for all contracts with contractors and other organisations who handle personal or health information on behalf of the University. These provisions will include, as a minimum, requirements to:

a. implement systems and controls that comply with relevant privacy laws, including any mandatory reporting regimes for data breaches;
b. allow the University to review or audit those systems and controls; and
c. notify the University and provide full details of any data breaches (including notifiable data breaches) in respect of any personal information held by that contractor or service provider as this relates to personal or health information held on behalf of the University.

Section 19 - Implementation of this Privacy Management Plan

Processes and Procedures

(176) The processes and procedures set out in this PMP are correct as of [19 April 2022], and may be updated from time to time as required, or when relevant laws are amended.

Consultation, Training and Information

(177) This PMP was available for consultation with staff before its implementation and, following approval, all staff will be provided with information about the plan and how to access it on the University's publicly available Policy Document Development System (Policy DDS).

(178) Staff responsibilities with respect to privacy are incorporated into the University's staff induction program. In addition, supervisors are responsible for ensuring that staff under their supervision, including contractors and casual staff, are informed of their privacy responsibilities and, where possible, undertake appropriate training.

(179) Training about privacy requirements should be incorporated into all training programs relating to use of University's systems and processes where privacy issues are relevant. This includes the University's staff induction program. Customised training sessions about privacy requirements can be delivered upon request.

(180) The University has developed an online privacy training module which is mandatory for all staff to complete every two years. The online module is also made available to research students and contractors to complete.

(181) The University also has comprehensive, publicly available, information on its privacy policies available on its University's Privacy website. The website provides high level information about how the University complies with privacy legislation and provides a link to further information about privacy at the University, including resources and contact information.

Publication

(182) This PMP is publicly available on the University's Policy DDS. Copies can be sent to individuals upon a written request to privacy@westernsydney.edu.au.

(183) A copy of this PMP has been provided to the NSW Privacy Commissioner as required under the PPIPA.

Review

(184) This PMP is subject to reviews to be undertaken by the Office of University Secretary and the Office of General Counsel together with the University's Privacy Officer.

Section 20 - Related Documents, Further Information and Useful Contacts

Related Policies and Other Documents

(185) This PMP should be read alongside the University's Privacy Policy. Other related policies include:

a. Acceptable Use of Digital Services Policy;
b. Cyber Security Policy;
c. Death Response Policy;
d. Digital Information Security Policy;
e. Digital Services Implementation Policy;
f. Health Privacy Information for Students Undertaking Clinical Experience (or Other Placement) in Health Sector;
g. Records and Archives Management Policy;
h. Research Code of Practice;
i. Research Data Management Policy;
j. Student Declaration;
k. Workplace Surveillance Policy.

(186) Staff and students should refer to the University's Privacy website or the Policy DDS to obtain copies of these documents.

Contacts

(187) The University's Privacy Officer can be contacted as follows:

a. By phone: (02) 4570 1428
b. By email: privacy@westernsydney.edu.au

(188) Other useful external contacts include:

Information and Privacy Commissioner of New South Wales
Level, 15 McKell Building, 2-24 Rawson Place, Haymarket 2000 (correct as at 7 April 2022)
www.ipc.nsw.gov.au

Civil and Administrative Tribunal of New South Wales
John Maddison Tower, Level 10, 86-90 Goulburn Street Sydney 2000 (correct as at 7 April 2022)
1800 006 228
www.ncat.nsw.gov.au

Section 21 - Annexure A: Information Protection Principles

Summary

(189) Information Protection Principles are the guiding principles which regulate how the University can collect, use, hold and disclose personal information of individuals. They are set out in a number of different parts of the relevant legislation.

General Terms

(190) In general terms, the Information Protection Principles (sections 8-21 of the PPIPA) are as follows.

(191) Lawful purpose

a. The University must collect personal information only for a lawful purpose directly related to its functions and activities and the information must be reasonably necessary for those purposes.

(192) Collection from individual directly

a. The University must collect personal information directly from the individual to whom the information relates unless the individual has authorised collection from someone else, or if the person is under 16 the information has been provided by a parent or guardian.

(193) Requirements when collecting information

a. After collecting personal information about an individual, the University must advise the purpose for which the information is collected, who may receive it, whether the supply of information is required by law or voluntary, the rights of access to and correction of the information and the name and address details of the party or entity holding the information (being a limb or department of the University). Further, the University needs to advise whether the supply of the information is required by law and the consequences for the individual if they fail to provide the information.
b. The University must take steps to ensure as is reasonable in all the circumstances that the information collected is relevant, is not excessive, is accurate, up to date and complete. Further, the University must ensure

that the information does not intrude to an unreasonable extent on the personal affairs of the individual to whom the information relates.

(194) Retention and security

a. The University must ensure that the information is kept for no longer than is necessary for the purpose for which it was collected and may lawfully be used and is disposed of securely. The University must have safeguards against the loss, unauthorised access, use, modification or disclosure of the information. If the information is to be given to a person in connection with the provision of the service, everything reasonable must be done by the University to ensure that the agent does not allow an unauthorised use or disclosure of the information.

(195) Openness

a. The University must take steps to enable any person to ascertain whether personal information is held about them and if so the nature of the information, the purpose for which the information is used and the existence of an entitlement to gain access to the information.

(196) Access

a. The University must, at the request of an individual, without delay or expense provide an individual with access to personal information subject to exceptions set out below.

(197) Amendment of personal information

a. The University must, at the request of an individual, make any amendments to personal information to ensure it is relevant, accurate, up to date, complete and not misleading in light of the purpose for which it is held.
b. If the University amends the personal information at the request of an individual, it must let the person know of the amendments.
c. If the University does not amend the personal information requested, it must attach to the information a statement provided by the individual of the nature of the amendments sought.

(198) Ongoing accuracy obligation

a. The University cannot use or continue to use personal information without ensuring that it is relevant, accurate, up to date, complete and not misleading in light of the purpose for which it is held.

(199) Limits on use

a. The University must not use the personal information for a purpose other than which it was collected unless:
    i. the individual consents to the use of the information for another purpose; or
    ii. the use of the information is directly related to the primary purpose for which the information was collected; or
    iii. the University believes on reasonable grounds that the information is necessary to prevent or lessen a serious and imminent threat to the life or health of the individual to whom the information relates or of another person.

(200) Limits on disclosure

a. The University must not disclose personal information unless:
    i. it is directly related to the purpose for which the information was collected and there is no reason to

believe that the person in question would have any objection to the information being disclosed; or

ii. the person for whom the personal information is held had been made aware (or is likely to have been made aware) that information of the kind is usually disclosed to third parties; or

iii. the University believes on reasonable grounds that the disclosure is necessary to prevent or lessen a serious or imminent threat to the life or health of an individual concerned or another person.

(201) Sensitive personal information and serious and imminent threat

a. The University may only disclose sensitive personal information to prevent a serious or imminent threat to the life or health of an individual concerned or another person, including information about an individual's:
   i. ethnic or racial origin; or
   ii. political opinions; or
   iii. religious or philosophical beliefs; or
   iv. trade union membership; or
   v. sexual activities.

(202) Transborder data flows (outside of NSW)

a. The University must not disclose personal and/or health information to a person or body outside New South Wales, including a Commonwealth agency, unless one of the following applies:
   i. the University reasonably believes that the recipient of the information is subject to a law, binding scheme or contract that effectively upholds principles for fair handling of the information that are substantially similar to the information protection principles; or
   ii. the individual expressly consents to the disclosure; or
   iii. the disclosure is necessary for the performance of a contract between the individual and the University or for the implementation of pre-contractual measures taken in response to the individual's request; or
   iv. the disclosure is necessary for the conclusion or performance of a contract concluded in the interest of the individual between the University and a third party; or
   v. all of the following apply:
      - the disclosure is for the benefit of the individual
      - it is impracticable to obtain the consent of the individual to that disclosure
      - if it were practicable to obtain such consent, the individual would be likely to give it
   vi. the disclosure is reasonably believed by the University to be necessary to lessen or prevent a serious and imminent threat to the life, health or safety of the individual or another person; or
   vii. the University has taken reasonable steps to ensure that the information that it has disclosed will not be held, used or disclosed by the recipient of the information inconsistently with the information protection principles; or
   viii. the disclosure is permitted under or required by any other Commonwealth or NSW law.

Section 22 - Annexure B: Health Privacy Principles

Summary

(203) The HRIPA contains Health Privacy Principles which are very similar the Information Protection Principles those contained in the PPIPA. To avoid duplication, set out below are only the areas where the Health Privacy Principles differ from the Information Protection Principles. This should not be read as an exhaustive summary and staff requiring detailed advice about their obligations under the HRIPA should contact the Office of General Counsel.

(204) Some “personal information” will also be classified as “health information” and governed by the principles in the Health Records and Information Privacy Act 2002 (NSW) (the HRIPA).

(205) “Health information” is defined as personal information that is information or any opinion about:

a. the physical or mental health or a disability (at any time) of an individual;
b. an individual’s express wishes about the future provision of health services to them;
c. a health service provided to an individual;
d. personal information collected to provide a health service;
e. personal information collected in connection with the donation of body parts, organs or body substances;
f. personal information that is genetic information about an individual;
g. healthcare identifiers (numbers assigned to an individual used in connection with health information).

(206) The University does not assign healthcare identifiers to individuals.

Collection from Individual Directly

(207) Under the HRIPA, health information must be collected from the individual concerned unless it is “unreasonable or impracticable to do so”.

Requirements when Collecting Health Information

(208) The HRIPA contains additional requirements than the PPIPA to inform individuals of certain matters when information is collected. Individuals must also be made aware of:

a. the identity of the organisation and how to contact it;
b. the persons to whom the organisation usually discloses the information;
c. any law that requires the particular information to be collected;
d. the consequences for the individual if the information is not provided.

(209) If the health information is collected from a third party, steps must be taken to ensure the individual concerned is aware of the above matters, unless informing the individual concerned would pose a serious threat to the life or health of any individual or the collection is made in accordance with guidelines issued by the NSW Privacy Commissioner.

(210) Exceptions to these requirements include:

a. consent by the individual to non-compliance;
b. if compliance would prejudice the interests of the individual concerned;
c. non-compliance as otherwise authorised or permitted by law.

Limits on Use and Disclosure

(211) There are some additional exceptions to those under the PPIPA which University staff dealing with health information should be aware of. They include, but are not limited to:

a. the management of health services to assist students or staff;
b. the training of employees of the organisation;
c. research, or the compilation of analysis of statistics;
d. suspected unlawful activity, unsatisfactory professional conduct or breach of discipline; and
e. disclosure is to an immediate family member for compassionate reasons.

(212) Using health information to assist students or staff with a disability is an appropriate use of the information. Access and use is not confined to one area of the University, but this should only occur on a strictly “need to know” basis. Any such access and use should be made known to the individual concerned and, wherever possible, authorisation should first be obtained.

(213) For use and disclosure of information in circumstances described in (210)(a) [where appropriate] and (210)(b), reasonable steps must be taken to de-identify the information.

Anonymity

(214) HPP 13 provides that, wherever lawful and practicable, individuals should be given the opportunity to remain anonymous when receiving health services from the University.

(215) This is an option for staff using the Employee Assistance Program (EAP) for support or counselling.

(216) However, due to the nature of the health services provided by the University, it is impracticable for students accessing Equity, Safety and Wellbeing services to remain anonymous.

Section 23 - Annexure C: Types of Personal Information Collected by the University

Students

(217) The University engages over 49,000 domestic and international students, including students enrolled within The College and the University's institutes. The University must collect a wide variety of personal information to maximise the student experience. This includes collection of information using a digital service (including online and mobile services).

(218) The types of information collected about prospective and current students related to student enrolment, include:

a. name, date of birth, gender, marital status, address, email address, phone number, contact details and billing address;
b. assessment and examination results;
c. academic transcripts and/or other academic records;
d. degrees, qualifications and honorariums;
e. graduation or attainment records;
f. any prizes, scholarships or other bursaries;
g. photographic records or digital images of the student’s appearance, including images recorded during filming or live streaming of graduation ceremonies and other events, or in any of the circumstances referred to in clause (42);
h. information about the student’s conduct during the course of the student’s attendance at the University;
i. applications for enrolment, changes to enrolment, registration, progression, deferral, withdrawal or graduation;
j. information or opinion about an individual arising from investigation or inquiry into matters relating to the University;
k. Disruption to Studies applications;
l. information in relation to matters of discipline or misconduct;
m. reference numbers – tax file numbers, passport numbers, bank account numbers, drivers licence number;
n. details about next of kin and emergency contacts;
o. personal welfare, health, or medical information;

p. information collected through the provision of identification documents, such as race, religion, gender, sexual orientation and citizenship;
q. admission information, enrolment, registration, progression, assessment, misconduct and graduation information;
r. information about the student's fieldwork, placement or practicum including reports and assessments;
s. health information about the student, including information collected Equity, Safety and Wellbeing;
t. information collected in surveys;
u. information collected by University services to provide benefits to students, including inter-University exchange, MATES program, Transition Success, careers and in other University operated activities.

Employee and Individual Contractors

(219) The University employs in excess of 3,500 academic and professional staff. There are a wide range of skills, professions, and activities undertaken by employees of the University.

(220) The University collects a wide scope of records in relation to employees, including:

a. name, date of birth, gender, marital status, address, email address, phone numbers, emergency contact information, and home and billing addresses;
b. workers compensation and rehabilitation details;
c. financial data in relation to employees including tax file number, bank account details, and other information of this kind;
d. proof of identity documents which may include birth certificate, drivers licence or passport details;
e. photographic records or digital images of the staff member's appearance;
f. timesheets;
g. letters of offer and job application details;
h. employment history and other information contained in a curriculum vitae;
i. information in relation to disclosure of conflicts of interest and potential conflicts of interest;
j. declarations of external interests;
k. photographs and digital images of members of staff, including audio and video images;
l. qualifications and details of academic achievement at the University or other institutions;
m. applications and appeals for academic promotions;
n. medical certificates and assessment reports;
o. referees' reports and other information gathered in the course of assessing a job application or an application for academic promotion;
p. information contained in emails and SMS and MMS messages sent to and from email accounts and mobile phones distributed by the University to members of staff;
q. details of higher duties or secondment arrangements;
r. information in relation to matters of discipline or misconduct;
s. health information about the staff member;
t. information collected through the provision of identification documents, such as race, religion, gender, sexual orientation and citizenship.

Alumni

(221) Through the Western Sydney Alumni network, the University also collects and holds personal information about former students and graduates. The alumni database builds on central University records held for students. Additional information that may be held includes but is not limited to:

a. personal contact details such as name, address, gender, marital status, email address, phone number, and other contact details;
b. photographs of current and former students;
c. changes to contact details as described above;
d. bank details through donations;
e. details of attendance at alumni events;
f. subscriptions to alumni services, including user/login names for membership sites for the alumni network such as volunteers, alumni chapters, etc.

Others

(222) The University collects and holds information in relation to a significant range of people who are neither students of, nor employed by, the University including:

a. residents of University-owned accommodation;
b. those who participate in research programs;
c. those who provide written references for prospective or current employees;
d. external committee members;
e. customers or visitors to University services operated through controlled entities, such as Western Sydney University Early Learning Ltd and the Whitlam Institute;
f. those who come into contact with the University community from time to time, including visitors to University campuses;
g. contractors or those who have a business relationship with the University;
h. third parties who attend or participate University-organised events or activities (including community engagement events such as Open Day and graduation ceremonies), or University buildings for other purposes;
i. prospective students and employees;
j. parents of students who are under 16 years of age.

(223) Types of information of this kind include, but are not limited to, the following:

a. information provided by individuals in the process of research undertaken by students or members of staff of the University from time to time;
b. information provided in tenders, requests for information, proposals, bids or offers for the provision of goods or services by third party contractors;
c. information provided by prospective employees , including eligibility lists;
d. information captured by University CCTV cameras or other electronic recording software and/or devices (including at community engagement events);
e. financial information in relation to third party contractors including bank account details, invoices and records of goods and services provided to the University by third party contractors;
f. contact details of third party contractors including names, addresses and email and other billing details;
g. information of individuals who contact the University seeking information in relation to services it offers or its activities or undertakings;
h. donors' records including contact details, records of financial contribution, or financial information in relation to donors to the University;
i. information provided by parents of students.

Workplace Surveillance

(224) The University also has in place a Workplace Surveillance Policy that details the University's rights and responsibilities with respect to surveillance of University employees in the workplace.

Status and Details

Status	Historic
Effective Date	5th October 2022
Review Date	19th April 2027
Approval Authority	Director, Governance Services
Approval Date	5th October 2022
Expiry Date	8th June 2023
Unit Head	Sophie Buck Director, Governance Services 45701415
Author	Jo Maguire Manager, Policy and Governance 45701428
Enquiries Contact	Sebastian Castro Leon Privacy and GIPA Officer s.castroleon@westernsydney.edu.au