THE UNIVERSITY OF SYDNEY

The University of Sydney Privacy Management Plan

Produced in accordance with section 33 of the *Privacy and Personal Information Act 1998* (NSW)

Produced by Archives and Records Management Services

Copies of this document, hardcopy or electronic, are available on request from:

privacy.enquiries@sydney.edu.au

or by post at:

Privacy Officer
Archives A14
University of Sydney NSW 2006

Approved by:

David Pacey, Chief Governance Officer

Date:

28 April 2023

Contents

Note: As this document is used by University staff, affiliates and students some links in the text are not accessible by members of the public. Please contact the Privacy Officer for more information.

1. Privacy Management Plan overview

(1) Purpose

The purpose of this Privacy Management Plan **(the plan**) is to explain how the University of Sydney (**the University**) manages personal and health information in accordance with the NSW privacy acts:

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

In particular, it deals with the Information Protection Principles (**the IPPs**) and Health Privacy Principles (**the HPPs**) contained is the above acts. These privacy principles regulate collection, storage, access and correction, use and disclosure of personal and health information in NSW.

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

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

(2) What the plan covers

This plan meets the requirements in section 33(2) of the PPIP Act including:

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

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

(3) Students

The University's students are not generally subject to the NSW privacy acts, as the legislation applies to the University not individual students. The *Student Charter 2020* sets out the University's expectations of the personal and academic conduct of students. Conduct adversely affecting the privacy of others may be contrary to that charter and may result in disciplinary action being taken against a student.

The privacy acts apply to research done by a student as part of their award course as that academic work forms part of the activities of the University.

The University has nine graduate qualities which underpin students' education experience and are developed as they progress through their award courses. One of the qualities is:

> Integrated professional, ethical, and personal identity.

This is defined as:

> An integrated professional, ethical and personal identity is understanding the interaction between one's personal and professional selves in an ethical context.

Students in the medical and allied health sciences complete units of study which deal with professional practice. These cover matters of ethics, legislation and compliance, privacy being one of the topics. Students undertaking clinical placement are required to be familiar with the NSW Ministry of Health policies. In addition, there are specific units of study for postgraduate research students that deal with ethics, the law and professional conduct for human research in the medical and non-medical fields.

(4) Definitions

affiliate - means a person appointed or engaged by the University to perform duties or functions on its behalf, including but not limited to:

- an honorary title holder engaged under the *Honorary Titles Policy 2013*
- a consultant or contractor to the University; and
- an office holder in a University entity, a member of any University committee, board or foundation.

An affiliate is not an employee of the University.

collection – (of personal information) the way in which the University acquires personal or health information, which can include a written or online form, a verbal conversation, a voice recording, or a photograph.

disclosure – (of personal information) occurs when the University makes known to an individual or entity personal or health information not previously known to them.

exemptions from compliance with Information Protection Principles (IPPs) – (general, specific and other exemptions) are provided both within the principles (and under Division 2 and Division 3 of Part 2 of the PPIP Act).

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

investigative agencies – any of the following: Audit Office of NSW, the Ombudsman NSW, the Independent Commission Against Corruption (ICAC) or the ICAC inspector, the Law Enforcement Conduct Commission (LECC) or the LECC Inspector and any staff of the Inspector, the Health Care Complaints Commission, the Office of the Legal Services Commissioner, and Inspector of Custodial Services.

law enforcement agencies – any of the following: the NSW Police Force or the police force of another State or Territory, the NSW Crime Commission, the Australian Federal Police, the Australian Crime Commission, the Director of Public Prosecutions of NSW or another State

or Territory or of the Commonwealth, Department of Communities and Justice, Office of the Sherriff of NSW.

personal information – information or an opinion (including information or an opinion forming part of a database and whether or not recorded in a material form) about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion, including such things as an individual's fingerprints, retina prints, body samples, or genetic characteristics. Exclusions to the definition of personal information are contained in section 4(3) of the PPIP Act and includes health information; (see the definition at section 4 PPIP Act and section 4(3) PPIP Act and section 5 of the HRIP Act).

privacy principles – the Information Protection Principles (**the IPPs**) set out in Division 1 of Part 2 of the PPIP Act and Health Privacy Principles (**the HPPs**) set out in Schedule 1 of the HRIP Act. The privacy principles set out the minimum standards for all NSW public sector agencies when handling personal and health information. Within these principles lawful exemptions are provided.

public register – a register of personal information that is required by law to be, or is made, publicly available or open to public inspection, whether or not upon payment of a fee.

> Note: public register exemptions are provided for in clause 7 of the *Privacy and Personal Information Protection Regulation 2019*.

privacy obligations – the information privacy principles and any exemptions to those principles that apply to the University, which is a public sector agency

sensitive personal information – means personal information relating to an individual's ethnic or racial origin, political opinions, religious or philosophical beliefs, trade union membership or sexual activities.

staff – means all University employees at all levels, including casual employees.

student - means a person who is:

- currently admitted to candidature in an award course of the University; or
- where relevant, an exchange student or non-award student.

University health clinic - means a health clinic or clinical service which is operated with the approval of the University:

- by University staff as part of their University employment;
- by University affiliates as part of their University engagement;
- jointly by the University and a third party (to the extent to which the third party is bound to comply with this policy); or
- using the University's name or brand.

2. About the University

(1) the University's object and functions

The University collects and retains personal information in the course of meeting its object and functions as set out in section 6 of the *University of Sydney Act 1989* (NSW):

(1) The object of the University is the promotion, within the limits of the University's resources, of scholarship, research, free inquiry, the interaction of research and teaching, and academic excellence.

(2) The University has the following principal functions for the promotion of its object—

(a) the provision of facilities for education and research of university standard,

(b) the encouragement of the dissemination, advancement, development and application of knowledge informed by free inquiry,

(c) the provision of courses of study or instruction across a range of fields, and the carrying out of research, to meet the needs of the community,

(d) the participation in public discourse,

(e) the conferring of degrees, including those of Bachelor, Master and Doctor, and the awarding of diplomas, certificates and other awards,

(f) the provision of teaching and learning that engage with advanced knowledge and inquiry,

(g) the development of governance, procedural rules, admission policies, financial arrangements and quality assurance processes that are underpinned by the values and goals referred to in the functions set out in this subsection, and that are sufficient to ensure the integrity of the University's academic programs.

(3) The University has other functions as follows—

(a) the University may exercise commercial functions comprising the commercial exploitation or development, for the University's benefit, of any facility, resource or property of the University or in which the University has a right or interest (including, for example, study, research, knowledge and intellectual property and the practical application of study, research, knowledge and intellectual property), whether alone or with others,

(a1) without limiting paragraph (a), the University may generate revenue for the purpose of funding the promotion of its object and the carrying out of its principal functions,

(b) the University may develop and provide cultural, sporting, professional, technical and vocational services to the community,

(c) the University has such general and ancillary functions as may be necessary or convenient for enabling or assisting the University to promote the object and interests of the University, or as may complement or be incidental to the promotion of the object and interests of the University,

(d) the University has such other functions as are conferred or imposed on it by or under this or any other Act.

(4) The functions of the University may be exercised within or outside the State, including outside Australia.

The University records related to its object and functions which may hold personal information include:

- student administration records relating to admission, identification, enrolment, academic progression, assessment, learning management systems, misconduct and discipline, learning analytics, results, special consideration, academic appeals, graduation and contact lists
- student services records including health, counselling, disability support and wellbeing services
- staff related records including recruitment, identification, superannuation, remuneration, leave, misconduct, performance management and declarations of external interests
- affiliate related records including nomination, appointment and conditions
- administrative records dealing with governance, finance, property (land and buildings), security (including Closed Circuit Tele Vision (**CCTV**)), procurement
- alumni and donor records
- research related records such as ethics committee minutes, participant consent and information forms, research data, intellectual property agreements and licences, and grant applications
- libraries, museum and archive records of donors and users of these services
- Information and communication technologies (**ICT**) records such as email and other account information, web sites and cookies.

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

(2) Bodies that are not part of the University

There are independent bodies established to serve the interests of students and others which are not under the direction or control of the University's staff or structures. Such bodies include:

- child care centres
- the residential colleges
- Students' Representative Council (SRC)
- Sydney University Postgraduate Representative Association (SUPRA)
- Sydney Uni Sport and Fitness (SUSF)
- The University of Sydney Union (USU).

These bodies are not part of the University and this plan does not apply to them.

3. How the University collects personal and health information

This section explains ways in which the University collects personal and health information to carry out its functions.

The collection of personal information directly from individuals may be by writing, email, through forms on the University website and online business systems, by phone, or in person at the Student Centre and other University service points.

Personal information is also collected by the University from third parties – generally government agencies but from individuals in some circumstances. See part 4 of this plan for more information.

The University aims to tell students, staff, affiliates and members of the public how it will manage their personal information at the time of collection.

(1) Enquiries

The University responds to enquiries from:

- prospective students
- current students
- those wishing to undertake Law Extension Committee or Centre for Continuing Education courses
- alumni and former students
- applicants for employment
- current staff and affiliates
- former staff and affiliates
- research participants, and
- members of the public

relating to its functions as described above.

These enquiries are made:

- over the phone (which may be recorded)
- in writing (e-mail, letter, online through the facilities such as Student Enquiries and the Services Portal)
- in person (at the service points on the University's campuses, offices such as the Student Centre and at events).

The University decides what level of information is appropriate to be collected for each enquiry on a case-by-case basis, with the understanding that the details collected must contain enough information to be an accurate record of the enquiry and the advice given in response, but should not contain unnecessary personal and/or health information.

If someone writes to the University in any media, a full copy of whatever is sent is generally kept by the University in the relevant business system.

The provision of personal information in an enquiry is usually voluntary and, in that respect, personal information may be provided that is unsolicited.

The University's telephones will display the number of the person who called, except for private/silent numbers. Where telephone conversations to a call centre may be recorded a notice will be provided when the call is answered.

(2) Programs for high school students

The University works with partner schools in supporting students to build awareness and preparedness for university study. The programs include regional programs, workshops, tutoring, residential blocks, and advice for teachers and other education professionals. For more information see: High school programs

Some faculties and schools offer workshops for HSC students, either in person on campus or online. Registration for these events requires the collection of personal information. See the Faculty of Science Community engagement web site as an example.

(3) Student Recruitment

Prospective domestic undergraduate, some international undergraduate, and postgraduate coursework students apply for admission to the University through the Universities Admission Centre (**the UAC**). Relevant information is accessed by the University for those school students who have selected any of its courses as a preference in their UAC application.

Additionally, prospective students can make enquiries regarding study at the University through an online form in the Services Portal which only collects the information necessary to respond to the enquiry

The University has objectives in recruiting and admitting outstanding domestic and international students across all programs and courses. There are a number of admission pathways available to Aboriginal and Torres Strait Islander students, domestic high school students who have experienced significant educational disadvantage during Year 11 and/or 12, elite athletes and performers, students who have experienced financial disruption in Year 11 and/or 12 or have attended a regional or remote school and have demonstrated the potential to succeed at the University, high academic achievers, by portfolio or audition, school captains and dux students. Information regarding each of these pathways and the required personal information for application are available on the Admission Pathways website.

Each year the University's flagship student recruitment event has been Open Day. Traditionally held on campus, prospective students can register online and express an interest in particular fields of study and subscribe to the latest news and events.

Prospective students can also choose at any time to subscribe to an information service about the University. International students can register for events held by the University regarding course options and study at the University. The personal information collected is limited to that necessary for identification, communication and to provide relevant information regarding study at the University.

(4) Scholarships

The University has a variety of scholarships for undergraduate and postgraduate students. Some scholarships do not require application as eligibility is assessed by the University based on result and other information, other scholarships require the completion of an application form available on the University's Scholarships website. External scholarship

funding organisations may have their own selection process and links to them are provided by the University's Scholarships website where applicable.

(5) Financial support and bursaries

The University has bursaries and interest free loans available to students in financial difficulty. The Financial Support website has a general enquiry form which collects minimal personal information. Applications are made through the Sydney Student portal where only information necessary to assess the application is required.

(6) Student Support Services

The University provides centres to support students in their study and learning, medical services and counsellors. Applying for all these services requires the collection of personal information and some services will require the collection of health information from the applicant. More information on these services is available on the University's Student Support website.

(7) Applications for Special Consideration

Students in exceptional circumstances such as illness, injury or misadventure that significantly affect their short-term academic performance in an assessment task, may be eligible for special consideration. Exceptional circumstances are defined as circumstances that are beyond the student's control and unavoidable. There is an online portal for applications. Applications may necessarily require the collection of health information of the student and/or third parties, depending on the circumstances

(8) Centre for Continuing Education

The University's Centre for Continuing Education (**the CCE**) provides short courses across a broad range of areas. Many courses are run in the evening and are designed to develop skills and knowledge in any chosen professional, personal or academic area of interest.

The CCE has a mailing list which provides users with the ability to unsubscribe online. Those wishing to undertake a course enrol online in the CCE's system. The personal information collected is required to manage course payment, enrolment and delivery.

(9) University staff recruitment and affiliate nomination

The University collects personal and/or health information of applicants during recruitment. The University will never ask for more personal information than is required for that purpose.

During recruitment and throughout employment, information (including personal and/or health information) is collected from staff members for various reasons, such as leave management, unplanned absences, workplace health and safety and to help the University operate with transparency and integrity.

In the exercise of its functions the University collects and manages personal information about its staff including but not limited to:

- medical conditions and illnesses
- next of kin and contact details

- education
- research and publication history of academic staff
- contacting staff members about unexplained absences in accordance with the adopted Employee Welfare Check procedure
- performance and development information
- family and care arrangements
- secondary employment
- conflicts of interest
- financial information for payroll purposes
- employment history.

Information collected by the University is retained in accordance with the NSW *State Records Act 1998* and managed securely in University systems or in systems of its contracted service providers.

When people apply for jobs at the University, they send us personal information, including their name, contact details and work history. The University gives this information to the chair of the interview panel for that particular position. The chair of the panel does not use this personal information except for the purposes of the recruitment process. This includes sharing the information with members of the interview panel. Interview panels may include persons not employed by the University. Chairs store this information securely. After recruitment is finalised, Chairs return all personal information to the Recruitment Team.

Pre-employment checks are conducted in accordance with the University's *Recruitment and Employment Policy 2021*.

New staff provide personal information about themselves directly to the University via specific forms available on the recruitment website. The forms collect information necessary for employment at the University: bank account, personal information, identity and work rights confirmation, certification of documents, tax file numbers and prior service.

The personal details form, and the University's online Human Resources system (**the HR system**), include the provision for the supply of two emergency contacts. The HR system also has the provision for the voluntary supply of demographic information used for planning and reporting purposes.

The information collected about affiliates is similar, but not as extensive as that collected about staff. As affiliates are not paid by the University banking details are not collected.

(10) Research

A key function of the University is the conduct of research by staff, affiliates and students collects significant quantities of personal and health information. The means of collection include:

- direct from the individual, either in person, by phone, electronic and forms, and surveys
- from third parties, including research partners, government agencies, and health services
- from patients of the University's health clinics which deliver services to patients
- clinical trials – the Clinical Trials Centre (**CTC**) at the University conducts large scale clinical trials of treatments and therapies around the world.

(11) Human tissue

The University receives donations of the bodies of deceased persons for use in teaching and research under its Body Donor Program.

The Australian Sports Brain Bank is an international collaboration located at the University's Brain and Mind Centre. It researches the full impact of sports related concussion on the human nervous system.

The NSW Brain Tissue Resource Centre based at the Charles Perkins Centre supports the advancement of medical research into neurological illnesses by collecting, characterising and storing brain and spinal cord tissue and providing specimens for merit-based research.

(12) Fieldwork and travel

Staff, affiliates and students regularly undertake fieldwork and/or travel as part of their candidature (students) and research (staff, affiliates and students). These activities require the collection of additional personal information such as passport numbers or particular qualification – such as SCUBA diving certification. In addition, for WHS reasons information about some medical conditions and medication is required before approval can be granted to undertake some activities. Staff, affiliates and postgraduate research students use Field Friendly (login required) to manage fieldwork and Concur for their travel. In addition, staff and affiliates may join TripIt to facilitate travel.

(13) Surveys

The University conducts surveys regarding its administrative functions directed at students, staff, affiliates and alumni. These surveys generally collect limited information and the University ensures any proposed survey or other kind of collection complies with the PPIP Act and HRIP Act. When conducted, major surveys such as the Staff Engagement Survey or the Alumni and Supporter Census, have dedicated web pages providing details of the survey and appropriate collection notices.

Surveys are routinely used in academic research. The use of surveys in research must have approval by a properly constituted Human Ethics Research Committee. Further information may be found at the *National Statement for Ethical Conduct in Human Research*, the *Australian Code for the Responsible Conduct of Research 2018*, and the University's *Research Code of Conduct 2019*.

The University provides Research Electronic Data Capture (**REDCap**) for use by its researchers. It is a secure web-based database application maintained by the University for collecting and managing participant data and administering online surveys.

The University stores survey information in its business systems, including the corporate recordkeeping system, or in systems managed by contracted service providers or research partners. The University does not disclose personal information obtained through surveys, except by consent or as permitted or required by law.

(14) Visitors and members of the public

When members of the public, staff or students attend University events they may need to register with the University's events registration system. Attendance at performances at the Sydney Conservatorium of Music and the Seymour Centre, which may involve a fee, are managed through their individual booking systems.

(15) Subscriber, mailing and contact lists

Anyone can subscribe to the University's News and Opinion alerts. Only an email address is required, name and affiliation are optional. Users can change their preferences and unsubscribe from a link in all alerts.

Alumni can update their contact details or change their *Sydney Alumni Magazine* (SAM) preferences online.

Some centres, schools and the Chau Chak Wing Museum have their own newsletters. Subscriptions and preferences are managed on line at the respective sites.

(16) Conferences, exhibitions, fairs and events

Information on the University's many events open to the public are available at its Event Calendar and for those limited to staff and affiliates, behind a login. Individuals may register for information about events on these web pages.

Some career fairs for students are virtual, requiring online registration. These are often conducted using the vFairs platform.

Some events on its campuses may not be organised by the University, or may be jointly organised.

The University take the PPIP Act and the HRIP Act into consideration when organising such events and aims to inform people how the University will manage their personal and/or health information if it is collected, such as on registration forms or specific notices on its Privacy at the University website, for example the Welcome Week filming privacy collection notice.

If an event management company is used to assist with delivering an event, the University's standard contracts contain relevant privacy requirements. For further information see part 7(4) of this plan, Service Providers.

(17) Publications

Many faculties, schools, departments, centres, foundations and other units of the University produce publications that are available to the public by subscription via a web form, for example:

- News about the University
- the University Museum's newsletter *Muse*
- Sydney Ideas newsletter
- Faculty of Engineering industry newsletter *Ignite*

These sites include a link to collection notices and University privacy information.

(18) Security systems

The University uses CCTV on its campuses and in many of its buildings. This captures images of individuals which come in range of the cameras.

Access to many University buildings and facilities is regulated by a swipe card system, or other means or recording access. Swiping a staff or student card records the identity of the person to whom the card was issued.

Biometric information is collected to manage the attendance of some staff.

(19) Website publishing

The University owns and maintains its corporate website which provides information to current and prospective students, alumni, staff, affiliates and members of the public. The website facilitates many University functions and gives access to business systems.

All pages on the University's corporate websites contain a link to a web privacy statement which explains the personal information the site collects and gives links to further privacy information.

(20) Complaints

Personal and health information is received by the University in many different forms related to complaints and related matters under its policies, including:

- bullying, sexual assault, harassment or discrimination
- academic appeals
- allegations of research misconduct
- complaints about University agents
- privacy complaints
- reports of wrongdoing
- protected disclosures.

Students are able to make a complaint to the University under the *Student Complaints Procedures 2015*, and staff and affiliates are able to make a complaint on behalf of a student with their consent, or on behalf of a student who wishes to remain anonymous.

Complaints or concerns about:

- the conduct of a University of Sydney research investigator
- a University of Sydney research project or activity
- the decisions of a University of Sydney Human Research Ethics Committee
- research activities undertaken without appropriate ethics approval
- another ethical review body
- research projects which are non-compliant with the relevant legislation, codes and guidelines.

Are received by the Director of Research Integrity and Ethics Administration.

Information regarding making a privacy complaint (an internal review) is at part 20 of this plan.

In addition to complaints to be investigated by the University, staff, affiliates and students may make complaints or disclosures about sexual misconduct they have experienced or witnessed which they do not want investigated. In addition, staff may make a disclosure on behalf of a student. Members of the public may report sexual misconduct connected with the University.

All forms relating to complaints contain privacy collection notices.

(21) Collection of Health Information

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

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

Health information may be collected:

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

(22) Special provisions relating to COVID-19

The University may hold information regarding COVID-19 infections in staff, affiliates student, contractors or visitors to campus as a result of:

- Self-reporting by the infected person, or
- Notification by NSW Health

The information is managed in accordance with the *Recordkeeping Policy 2017* and the *Privacy Policy 2017* and will only be used for contact tracing, notification, and to organise cleaning or other response management that may be necessary to protect health and safety at the University.

The University is required under the NSW Public Health Orders to exchange personal or health information with other government sector agencies if necessary to protect the health or welfare of the community during the COVID-19 pandemic. This includes providing NSW Health with access to University building access data when this is requested.

Where the University becomes aware of an emergency on campus in advance of NSW Health, the University may also use this data to identify and notify close contacts.

For more detail see the University's COVID-19 privacy collection notice.

4. When does the University collect personal information direct from the individual or from third parties?

(1) General

The circumstances in which the University collects personal information are set out in part 3 of this plan. In general, the University collects personal information directly from the individual unless it is lawful and reasonable to do otherwise.

However, there are specific collections of personal information from third parties. These include:

- Each year information is received from the NSW Universities Admissions Centre (**the UAC**) and similar bodies in other states about people seeking to study at the University in accordance with the UAC's procedures.
- Education providers delivering preparation programs which provide a pathway to the University
- Authorised agents can provide personal information on behalf of their prospective international student clients.
- Organisations where students undertake field work, practicums, professional experience programs or internships.
- Student accommodation providers contracted to the University are required to provide reports to the University relating to discipline and pastoral care of students in residence.
- Students and staff may provide emergency contact details to be held in the HR and student systems.
- Information from the Employee Assistance Program may be disclosed to the University with the consent of the staff member concerned.
- Safety and wellbeing apps available to students do not ordinarily disclose personal information to the University without the consent of the student concerned, unless it is required or authorised by law.
- Information regarding students studying at other institutions as part of their award course will be disclosed to the University.
- The University receives nominations for honorary awards from members of the public on a confidential basis.
- The University may also receive personal information about third parties in the course of its complaints processes. Such collections are permitted under section 24 of the PPIP Act as the University is an investigative agency under the definition in Section 3(1)(b) of that act.

(2) Research

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

Where a research project proposes to collect personal or health information from a Commonwealth agency without individual participants' consent, for the purposes of medical

research the HREC can only approve such a request if it meets certain criteria set out in the Guidelines Under Section 95 of the *Privacy Act 1988* (Commonwealth). Such research applications must provide the reasons such a collection is necessary and are then individually assessed by the HREC before deciding if approval will be given.

As described above, the University received donated bodies and human brains. It may also collect other tissue samples, genetic material and medical images as part of its specific research in the medical and health sciences.

5. How does the University notify a person that their personal information is being collected?

(1) General

When the University collects personal information using a form, either online or hardcopy, a collection notice, often called a privacy statement, is included on the form or one is linked to it. Section 3 of this plan set out the ways in which the University collects personal information. Each of those collection activities includes a relevant collection notice. This may be specific to the particular collection, or a link to statements covering particular functions of the University such as student administration.

(2) Collection notices – audio, photographs and video

At events, including staff only occasions, where photographs or video recordings will be taken appropriate notification must be made. Typically this would include:

- notice in invitations or promotion for the event, in hardcopy and online
- signs at the event itself
- announcement at the event, and/or
- notices on the University's privacy website.

Attendees at events are able to indicate that they do not wish to be photographed or recorded.

At internal University events where it is likely images will be used later for publication releases from significant guests, speakers or others whose images may be captured and used release forms available.

The University has installed signs regarding the use of CCTV on its campuses and there is are formal procedures regarding its use: CCTV Procedures 2019.

Where information is collected by telephone and individuals are identifiable, a verbal notice or directions to the relevant collection notice are given.

Many lectures are recorded so as to be more available to students. Academic staff advise students that their conversations may be picked up during any break.

(3) Research

Research involving the collection of personal and health information must be approved by an HREC. The application process requires that participant information statements and

participant consent forms be approved by an HREC. Approved documents ensure that participants are fully informed of all aspects of the research project, including the collection, use, management and disclosure of personal and health information.

The University's Research Integrity unit has specialist advisers to assist researchers provides training and resources for researchers intending to submit an application to the HREC.

6. How the University ensures that the collection of personal information is relevant, not excessive and is not an unreasonable intrusion?

(1) Business systems

The University collects most personal information required for administrative functions through its business systems. The framework of data and information governance contributes to ensuring the collection of personal information by the University is relevant, not excessive and is not an unreasonable intrusion into the personal affairs of individuals. Two components are key in relation to the collection of personal information in the University's business systems:

- Data Governance

  The Advanced Analytics Planning and Enterprise Data (**the AAPED**) team in the Strategy Portfolio reports to the University's Chief Data and Analytics Officer (**the CDAO),** this team is a single source of data for institutional analytics and reporting across the University. The team incorporates functions staff from across Institutional Analytics and Planning unit (**the IAP**) in the Strategy Portfolio, Research Reporting Analytics and Data Systems in the Research Portfolio, and analytics staff in the Education Portfolio. The IAP unit is responsible for business data governance in the University including organisation principles, policies, standards, processes, measurements, monitoring, and necessary technology to administer and manage its information resources. This framework supports the strategy of the Data Owners Management Group to ensure data governance is implemented across various levels of the organisation. Guided by the Data Management Body of Knowledge the data governance function at the University encompasses planning, supervision and control over data use to support the overarching business strategy. Key areas of consideration are data quality, regulatory requirements, security and privacy, and information.

- Standard project framework

  New systems that are classed as major University projects are developed in accord with the University Standard Project Framework and other processes set out in the University Project Hub on the Staff Intranet. This governance framework ensures all relevant experts and stakeholders provide relevant input to projects, necessarily including privacy.

  A change request lodged with the University's ICT division is required for alteration of business systems. Part of the change request process is the conduct of a Privacy Impact Assessment (**PIA**). The University has a PIA guide and template available on

the staff intranet, as part of the Technology Knowledge Base and on the Privacy and Right to Information staff intranet pages.

- Expert staff

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

(2) Routine collections

For routine or *ad hoc* collections of personal information the Privacy Advisor and other expert staff provide advice and assistance to business units. The Privacy Advisor also provides custom training for units on request. Solicitors with privacy expertise from the University's Office of General Counsel (**the OGC**) provide legal advice when it is required.

(3) Research

All research involving humans must be approved by a properly constituted HREC. Part of the process includes an assessment of the justification for the collection of the personal or health information by the HREC. The collection for the purposes of the research cannot commence until approval is provided by the HREC. Where possible, research involving humans is conducted on a de-identified basis, through the removal of names and other unique identifiers. However, given the possibility of information being re-identified, all such information is treated as if it were personal or health information.

Further information may be found at the *National Statement for Ethical Conduct in Human Research*, the *Australian Code for the Responsible Conduct of Research 2018*, and the University's *Research Code of Conduct 2019*.

Where an approved research project or clinical trial will involve the use of personal or health information held by a third party the University will enter into an agreement for the transfer of tissue or data with the third party. All proposals for such transfers are reviewed by the University's Research Portfolio who liaise with the third party to finalise the agreement. Standard templates have been prepared by the OGC and contain provisions for the protection of personal and health information. If necessary, individual agreements are prepared to meet particular circumstances.

Where a third party is outside Australia, for example in the European Union (**the EU**) the University requires that any transfer of personal or health information is complaint with the legislation applying in that jurisdiction, such as the EU General Data Protection Regulation (**the GDPR**).

7. How the University stores, protects and disposes of personal information

(1) Policy and procedures

To ensure personal information is stored securely, and kept for no longer than necessary, disposed of appropriately, protected from misuse, and unauthorised access, use, modification or disclosure the University has implemented relevant policies. Key University policies and procedures include:

- *Privacy Policy 2017*
- *Recordkeeping Policy 2017*,
- *Cyber Security Policy 2019*
- *Research Data Management Policy 2014*
- *Research Data Management Procedures 2015*
- Faculty and school research data management provisions
- *Privacy Procedures 2018*
- *Healthcare Records Management Procedures 2020*
- *Cyber Security Procedures 2019*

The University's *Staff and Affiliates Code of Conduct 2021* relevantly includes:

> **18 Use and security of information**
>
> (1) Staff and affiliates must:
>
> (a) maintain the integrity, confidentiality and privacy of University records and information to which they have access;
>
> (b) retain, manage and dispose of all University records in accordance with the Recordkeeping Policy 2017;
>
> (c) take all reasonable precautions to prevent unauthorised access to, or misuse of, University records and information;
>
> (d) only use ICT resources consistently with the requirements of the Acceptable Use of ICT Resources Policy 2019; and
>
> (e) comply with the Privacy Policy 2017 and Cyber Security Policy 2019.
>
> (2) Staff and affiliates must not:
>
> (a) disclose or offer to supply confidential or private University records or
>
> information, except:
>
> (a) when authorised to do so; or
>
> (ii) when required or permitted to do so by University policy, State or Commonwealth law, court order or other legal instrument;
>
> (b) access or use information, including information on electronic systems and hardcopy files, other than for an authorised purpose; or

(c) destroy, or authorise the destruction of, University records other than in accordance with relevant policy and legislation.

Clause 7 of the *Student Charter 2020* sets out student expectations of the University, clause 7(h) states that students can expect the University to protect the personal or health information it holds.

(4) Training and awareness

All staff and affiliates are required to complete the online compliance training modules on privacy, recordkeeping, information access, cyber security and the Staff and Affiliate Code of Conduct. Staff and affiliates are notified of the need to complete refreshed modules at a 1, 2 or 3 year interval. New staff must complete the modules as part of their induction. In addition, "My Learning" in Workday contains many privacy resources available to all staff.

The University's privacy staff provide training to business units on privacy as routine activity and on demand in relation to specific issues. This plan is one of the resources used in training.

(5) Other resources

The resources available on the University web site (some are limited to staff) include:

- The *Recordkeeping Manual*
- Recordkeeping guidelines
- Records system manuals and tools
- Provision of the corporate recordkeeping system to all staff, with strict controls on access to information based on the staff member's duties.
- Recordkeeping workflows for many administrative functions involving personal information such as complaints, practicum, higher degree research administration and some staff processes.
- Cyber security advice for staff and students
- This *Privacy Management Plan* on the University's website.
- Mandatory training for all new and continuing staff on privacy, recordkeeping and cyber security.

(6) Expert staff

As stated above, the University employs specialist recordkeeping, privacy and cyber security staff who provide expert advice and services related to the integrity, security and proper management of all the University's records.

The University's Protective Services provide physical security for its campuses by regular security patrols, concierge services, locking, alarms and surveillance systems. Where external service providers hold University information minimum standards of physical and data security are contractually required.

(7) Service providers

Contracts with external service providers dealing with personal information contain provisions relating to the security, privacy, access to and use of the University's personal or health information. The contracts may use the relevant templates developed by the OGC available from Procurement Services on the staff intranet which include confidentiality agreements. Where the University procures information and communications technology related goods and services it must use the NSW government's Procure IT Framework. Contracts under this framework include the necessary and relevant privacy requirements.

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

(8) Research

The University has a suite of digital tools that enable our researchers and students to manage their research data optimally and remain compliant with best practice. All these tools have been assessed and approved for use by the University Cybersecurity unit. Support is available for these tools from the Research Data Consulting team. Some of the research data management tools include:

- Research Data Store (**RDS**) – Secure backup and file storage
- REDCap – Data capture, forms and surveys
- eNotebook – Collaboration, context and managing workflows
- OneDrive – Collaboration, file syncing/sharing and manuscript writing
- CloudStor and OneDrive – Secure file transfer
- Encryption of new pc's as standard using Bitlocker or File Vault
- Multi-factor authentication to use University business systems
- VPN for staff and students.

Reference is made in Part 6, above, to the agreements the University enters into with third parties regarding the transfer of personal and health information. There are agreements for both incoming and outgoing transfers. The agreements contain provisions for the use, disclosure, breach notification, security and protection of the information. In outgoing agreements, the University may make directions for the recipient concerning use, storage or security of the information. Where a publication related to the information is envisaged, the University may require a review copy of any proposed publication prior to publication and that the recipient reasonably consider any review comments made.

Contracts with external service providers dealing with personal information must use the relevant templates developed by the OGC for this purpose. These include confidentiality agreements and are available from Procurement Services on the staff intranet.

(9) Retention and disposal

Personal and health information in University records are disposed of in accordance with the *State Records Act 1998 (NSW)*. Retention and disposal of records is managed by Archives and Records Management Services (**ARMS**). Part 7 of the University's *Recordkeeping Manual* is titled *Retention and Disposal* and provides guidance and advice to staff on compliance with the *State Records Act* and University policy.

There is a University records disposal program and dedicated Records Disposal Officer to ensure lawful and timely disposal of University records.

The University Archives preserves records of enduring and permanent value, some which contain personal information. Part 5 of the University's *Recordkeeping Manual* relates to the University Archives and provides guidance relating to appraisal and archival selection and the management of the University's holdings.

Destruction of records outside of those controlled by ARMS is carried out in accordance with the process on the staff intranet. Once approval for destruction has been given, destruction is carried out in a secure manner using specialised services.

Specific advice is provided to researchers on the research support pages of the staff intranet: https://intranet.sydney.edu.au/research-support/reporting-services-and-requirements/data-retention-periods.html

See also:

- *Recordkeeping Policy 2017*
- *Research Code of Conduct 2019*

8. How the University ensures the accuracy of personal information before using it

The majority of personal information used by the University is collected as part of its functions and is then held in business systems to be available for authorised use. Verification at the time of collection is an important step in ensuring the accuracy of personal information. Major business systems are the "single source of truth" for the respective functions of the University, such as Sydney Student and the HR system.

The following are relevant examples of the ways the University ensure the accuracy of personal information:

- Information regarding students received from the UAC has undergone stringent verification processes at the time of collection and correction as required during its use by that agency.
- Documents provided by students as part of their admission application are verified with the issuer of the document. Students are notified of this requirement.
- Students verify their personal information as a part of the enrolment process. They may also check and update it at any time through MyUni. See Úpdate your and contact information. Changes to some personal information require the provision of appropriate supporting documentary evidence.
- All students, including applicants, and staff are assigned a unique identification

number that is used in business systems and transactions in preference to any other form of identification to avoid errors.

- Alumni can correct or update their personal information online. In addition, the University conducts a voluntary alumni census permitting alumni to update information about themselves held by the University.
- New staff provide personal information about themselves directly to the University via specific forms available on the recruitment website.
- Staff can correct or update their personal information by using Workday. Changes to some personal information require the provision of appropriate supporting documentary evidence.
- Patients at University clinics provide their personal information to the clinic at the time of registration.
- Research participants recruited directly to research projects provide their own personal information.

All sites referred to above require secure log-in and are securely maintained.

9. How the University limits its use of personal information?

University business processes are standardised through its systems. How the University develops and modifies these systems is described in Part 6, above. The systems are designed to conduct or facilitate business process and are not able to be configured for other purposes by end users.

(1) Data

Access to administrative data, including personal information, within the University is managed by AAPED and IAP, whose data governance is described in Part 6 of this plan. Access is provided by:

- Dashboards – each of which has an owner, and request access to those dashboards through a formal request process which includes approval from the owner.
- Data – requests to access data that contains personal information must be made by a staff member approved for such access. If they are not an approved user the staff member must request access and provide evidence in support of the request and of the purpose the information is needed.

When data is provided in the University the recipient must provide evidence how they will keep data safe, what is purpose, and who is accessing the data.

Any request for data from outside the University is referred for advice from the University Privacy team, as are any non-routine requests.

(2) Learning analytics

The University stores data from many sources that is used for reporting, planning, research and non-research purposes. Learning analytics is the analysis and use of University-held student information to improve students' learning experience and outcomes. Access to student information requires the approval of the Deputy Vice-Chancellor (Education).

(3) General

Access to the University's business systems is not automatic and must be made by application with increasing levels of justification and approval required depending on the nature of the information in each system. Many business systems have graded levels of users access and functionality, what is granted is dependent on the duties of the staff member. Examples are the corporate recordkeeping system, Sydney Student and the HR system.

The login to major business systems holding personal information includes a notice to the user of their responsibilities regarding the use of the information and, in some systems, the penalties that apply for misuse of the information.

New business systems, and changes to existing systems, must be approved by the University's ICT Architecture Review Board (**the ARB**). The Manager, ARMS and the Privacy Adviser are members of the ARB. They provide advice on all aspects of recordkeeping, privacy and access to information related to systems under review.

10. How the University deals with sensitive personal information?

(1) Administrative

Sensitive personal information is collected only where it is required by law, for planning purposes or for the provision of services. For example, the University is required to report detailed statistical information to the Commonwealth Department of Education, Skills and Employment. This necessitates the collection of student ethnic or racial origin, which is also used for planning purposes in the University. Similarly, some such information about staff may be required to comply with employment related laws.

Examples of circumstances when sensitive information may be collected:

- initiatives to assist Aboriginal and Torres Strait Island peoples wishing to study, including the pre-tertiary outreach program, admission pathways and scholarships and other financial support.
- indigenous employment is a key focus of the University and there is an Aboriginal and Torres Strait Islander Staff Network.
- Trade union membership fees may be deducted from a staff member's pay, and so this sensitive information may be held by the University for some staff.

The information is retained in the University's secure business systems. Disclosure of information regarding racial or ethnic origin is only made with the consent of the relevant individual.

(2) Research

Sensitive personal information may be collected, used and disclosed in the conduct of research. Any such research must be conducted in accordance with the approval by a HREC following *Statutory Guidelines on Research*.

11. How the University discloses personal information

Clause 4 of the University's *Privacy Procedures 2018* (**the Procedures**) states:

> **4 Disclosure of personal information generally**
>
> (b) The University will only disclose personal information that it holds about an individual if:
>
> (c) the individual to whom the information relates has given their express consent;
>
> **Note:** An individual cannot give express consent in advance to disclosure of information which does not exist, or is unknown, at the time consent is sought.
>
> (b) the disclosure is required or authorised by law;
>
> (c) the disclosure is directly related to the purpose for which the information was collected and there is no reason to believe the individual would object;
>
> (d) the individual has been made aware, or is reasonably likely to have been aware, that information of that kind is usually disclosed;
>
> (e) in the case of health information, and in accordance with the relevant statutory guidelines, it is reasonably necessary for the management of health services, training or research or it is being used for a related health treatment; or
>
> (f) one of more of clauses 5 – 12 of these procedures applies.
>
> (g) The University will only disclose personal information that it holds about an individual which relates to an individual's ethnic or racial origin, political opinions, religious or philosophical beliefs, trade union membership, or sexual activities if:
>
> (h) the individual has given their express consent;
>
> (i) the University reasonably believes that it is necessary to prevent a serious or imminent threat to any person's life or health; or
>
> (j) the disclosure is required or authorised by law.

The Procedures detail how the University will disclose personal information:

- in an emergency
- to government agencies
- under subpoena, warrant or other order
- to law enforcement agencies
- contained in CCTV vision
- to external service providers

- for research purposes
- to other third parties.

Other disclosures of personal information:

- The University Archives holds records of the University and the amalgamated institutions. Those older than 30 years are generally open to the public under the *State Records Act 1998* (NSW). The University has made access directions under the State Records Act for some archival records containing personal information.
- Under the GIPA Act individuals may seek access to government information, see Part 10 Clause 5 of this plan. Where an access application concerns the personal information of a third party the Act requires that they consulted as part of the balancing of public interest considerations for and against the disclosure. The consulted persons are informed of their rights of review over any decision to release their personal information.
- In accordance with protocols approved an HREC the University may information outside NSW as part of a health research project. It is usual for such information to be de-identified or anonymised prior to any use or disclosure.

University clinics may disclose health information to jurisdictions outside NSW:

- With the consent of the individual to whom the information relates
- Where the disclosure is directly related to the purpose for which it was collected
- When it is reasonably believed 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 a serious threat to public health or safety
- When it is reasonably necessary for the management of health services, training or research
- For compassionate reasons
- To find a missing person
- In relation to suspected unlawful activity, unsatisfactory professional conduct or breach of discipline
- For law enforcement or to investigative agencies
- In other prescribed circumstances.

All disclosures of health information are made in accordance with HPP 11 and the relevant *Statutory Guidelines.*

12. Does the University include information in a health records linkage system?

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

Linkage systems are used for health information collected during research projects, in some clinical trials as well as University biobanks with health information held by the relevant health departments. These projects may make use of linkage service providers such as the Centre of Health Record Linkage (**CHeReL**).

13. Does the University assign identifiers to individuals?

Clause 6 of the University's *Healthcare Records Management Procedures 2020* requires that all University health clinics use a unique identifier (eg, a patient or participant identifier or a medical record number). The unique identifiers must appear on every page of screen of a health care record.

14. Does the University give individuals the opportunity to remain anonymous?

Where appropriate, some University clinics enable individuals to receive medical services anonymously. In general, the University's other functions are unable to be fulfilled where an individual remains anonymous. However, anonymity is possible in:

- reporting of sexual assault
- Public Interest Disclosures
- some collection personal/health information research
- some surveys.

15. Accessing and amending personal information held by the University

The University holds information relating to its students, staff, affiliates, alumni, donors, research participants and members of the public who use it services or attend its events. Its collection notices make it clear that personal information is being collected, the nature of that information and the main purpose of the collection. In addition, all University web pages contain a link to a website privacy collection statement.

The Privacy at the University public webpages include contact details for the University's privacy officers who can provide more information. In addition, the Right to Information Officers and the University Archives are able to help a person find out if the University holds information about them and the nature of that information and the main purpose for its collection.

(1) Access to personal information

Application for personal information can only be made by the person to whom the personal information relates or with their written authority. The University will provide access to requested personal information as soon as practicable, and should usually be within 20 working days of the date of request. Access applications under the Privacy Acts invoke any conditions or limitations from the NSW *Government Information Public Access Act 2009* ("GIPA Act") that would apply if the access application were made under that Act. In particular, the public interest considerations against disclosure in the table at section 14 may be relevant in a decision. The restrictions on access imposed by Schedules 1 and 2 of the GIPA Act will override the access rights provided by the Privacy Acts.

(i) Access by Students

Students have access to their personal information held in a number of University business systems including:

- Canvas (learning management)
- myUni
- Sydney Student
- Special consideration
- Disability Assist
- Library
- Sonia (student placement)

Students may also access their exam scripts without the need for a formal application under the acts in accordance with the part 9(5) University's *Assessment Procedure 2011*.

In addition, students may request access to their own personal information under the PPIP Act without charge, or under the GIPA Act which requires the payment of a $30 fee. Information and links on these processes is provided on the *Your privacy* web page for students.

(ii) Access by staff

University staff are able to access information from their staff files without the need for a formal application under legislation. Staff have access to some routine records of their employment through Workday.

In addition, staff and affiliates may request access to their own personal information under the PPIP Act without charge, or under the GIPA Act which requires the payment of a $30 fee. Information and links on these processes is provided on the *Privacy and right to information* web page in the staff intranet.

(iii) Applying for access to personal information held by the University of Sydney

Members of the public and students or staff and affiliates may apply for access under the PPIP Act to their personal information held by the University using the general PPIP Act application form**.** There is no application fee.

Applications are processed in 20 working days. A written acknowledgement of receipt of the application will be posted to the applicant within 5 working days.

The privacy officers gather the records and information from the relevant business units. The information is assessed in the light of the acts and prepare a recommendation for consideration by the authorised the decision maker. Should any information not be released the decision will broadly identify that information and the reasons it has not been released.

If an applicant is not satisfied with the decision, she or he may apply to the University for an internal review, which is conducted under section 53 of the PPIP Act by a different officer of the University.

Members of the public and students or staff may apply for access to information, including information about themselves held by the University under the GIPA Act, for which there is a

$30 fee. Further information and an application form are at the Accessing University information web page.

The University's public facing privacy websites:

- Privacy at the University
- Your Privacy for students specifically

and all privacy collection notices provide details on individual's rights of access to information under the Privacy Acts and contact details for further information. The Privacy page at the University website listed above has links to the access application form.

(2) Amending personal information

(i) Routine amendment of personal information

Students are able to update their personal information (name, DOB, gender, address and contact details) through the "Current Students" pages of the University website.

Staff are able to update their personal information (gender, DOB, place of birth, race/ethnicity, citizenship status, nationality, sexual orientation, disability, emergency contacts, photograph, passports and visas, licences, legal name, preferred name, education, addresses, email, and phone numbers. Not all are mandatory) through Workday, the HR system accessible through the Staff Intranet.

In both cases appropriate supporting documentation is required to be provided. Details are available on the respective sites.

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

(ii) Procedure for amendment of information

A person who believes the University holds personal information about them not covered by the routine processes above, may request appropriate amendments to ensure that information is:

- accurate
- having regard for the purpose for which the information was collected (or is to be used) and to any purpose that is directly related to that purpose, is relevant, up to date, complete and not misleading

using the application form on the University's public facing website.

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

> **Note**: The right to correct information which relates to suitability for public employment (excluded from the definition of personal information) is limited to matters of fact. The right to correct does not apply to opinions. However, the individual has the right to have placed on the record his or her response to such an opinion.

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

16. Policy and procedure development

The University is required to set out in this plan how policies and practices are developed to ensure compliance with the requirements of privacy legislation.

All University policies are developed under the *University of Sydney (Policies Development and Review) Rule 2011 (as amended)* (**the Policy Rule**)and the *Policies Development and Review procedures 2012*.

This means that in the proposal of any policy in the University must be accompanied by:

a) a statement of the objectives of the policy;
b) a justification for the policy, including an analysis of potential alternative ways of achieving the objectives of the policy;
c) a statement of how the policy accords with the object of the University;
d) a statement of the consultations to be undertaken on the policy proposal, identifying who is to be consulted.

Once a draft policy has been developed the same requirements must be met when the policy is submitted to the determining authority with the addition of a certificate from the General Counsel to the effect that the policy is necessary.

In relation to privacy policy, the stakeholders relevant to consultation include the business areas of the University primarily concerned with the collection use and disclosure of personal information: student administration and services, human resources, research involving humans. In addition consultation with the student representative bodies (SRC and SUPRA) and the staff unions (the National Tertiary Education Union and the Public Service Association).

The Policy Rule requires that all policies must be reviewed within 6 months before the end of 5 years after the policy commenced. The review is to determine:

(a) whether the objectives of the policy are being achieved by the policy;

(b) whether the policy should continue to apply;

(c) whether any amendments should be made to the policy.

17. Public registers

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

18. Is the University subject to any exemptions?

The University is not covered by any:

- Privacy code of practice or public interest direction
- Legislation allowing it not to comply with any of the IPPs or HPPs

- Memorandums of Understanding or referral arrangements with other agencies that relate to personal information other than for research.

(1) Exemptions to the IPPs

Part 2, Division 3 of the PPIP Act contains exemptions that may allow the University to not comply with IPPs in certain situations. Most of the exemptions do not apply to the University's functions. Some examples of exemptions that may apply to the University include:

- The University is not required to comply with IPPs 2-3, 6-8, or 10-12 if the University is lawfully authorised or required not to do so
- the University is not required to comply with IPP 2 if the information concerned is collected in relation to court or tribunal proceedings.
- The way the University discloses personal information to government agencies, law enforcement agencies and for research is set out in its *Privacy Procedures 2018.*

(2) Exemptions to the HPPs

Exemptions are located mainly in Schedule 1 of the HRIP Act and may allow the University to not comply with HPPs in certain situations.

For example, the University is not required to comply with HPPs 4-8 and 10 if the University is lawfully authorised, required, or permitted not to comply with them.

Health privacy codes of practice and public interest directions can modify the HPPs for any NSW public sector agency. These are available on the NSW Information and Privacy Commission (**IPC**) website. Currently, there are none that are likely to affect how the University manages health information.

19. How to make a privacy complaint to the University

Students, staff, affiliates, alumni or other members of the public have the right to complain if they think the University has breached their privacy in the way it has handled their personal information. Complaints, known as applications for internal review under the PPIP Act, should be made in writing within six months from when the affected individual first become aware of the breach.

Many privacy concerns may be resolved with recourse to a formal application for internal review. Staff, affiliates, students and members of the public are encouraged to contact the University's privacy staff to discuss any privacy matters to see if they would prefer an informal resolution.

The University has a privacy complaint form that may be used to make a complaint.

Complaints, whether or not the form is used may be emailed to mailto:privacy.enquiries@sydney.edu.au or by post to:

Privacy and Right to Information
Archives and Records Management Services
A14
University of Sydney
NSW 2006

The University is required to advise the NSW Privacy Commissioner of their name and the details of complainants and to keep the Commissioner up to date with the progress of the internal review.

Privacy complaints are considered by the University's authorised decision makers. Complainants are advised of the results of the internal review and any action that the University proposes to take in respect of the complaint.

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

- Review of the University's decision by NCAT

  Complainants dissatisfied with the way the University has dealt with their complaint or are disappointed with our findings, can ask the NSW Civil and Administrative Tribunal (NCAT) to review the conduct, Level 10 John Maddison Tower, 86-90 Goulburn Street Sydney Post: PO Box K1026, Haymarket NSW 1240 | DX 11539 Sydney Downtown Email: mailto:aeod@ncat.nsw.gov.au

- Complaint to the Privacy Commissioner, Level 15, McKell Building, 2-24 Rawson Place, Haymarket NSW 2000. Postal | GPO Box 7011, Sydney NSW 2001. Email | ipcinfo@ipc.nsw.gov.au Phone 1800 472 679

  Whether or not an individual applies for an internal review, they can also make a complaint to the NSW Privacy Commissioner about an alleged breach of their privacy.

20. Offences

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

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

• intentionally disclose or use personal information accessed as a part of their work for an unauthorised purpose

• offer to supply personal information that has been disclosed unlawfully.

21. Contacting the University

For further information about this plan, the personal and health information the University holds, or any other concerns, please contact the University's Privacy Officer. The Privacy Officer can also provide information regarding:

- how the University manages personal and health information
- requests for access to and amendment of personal or health information
- guidance on broad privacy issues and compliance
- requests to conduct internal reviews about possible breaches of the PPIP Act and HRIP Act (unless the subject of the review is the conduct of the Privacy Officer).

Contact the Privacy Officer of the University at:

T +61 2 8627 5188

E privacy.enquiries@sydney.edu.au

Mail: Privacy Officer, Archives A14, University of Sydney 2006.