THE UNIVERSITY OF SYDNEY

Privacy Management Plan

2013

Prepared in accordance with s.33 of the *NSW Privacy and Personal Information Protection Act 1998* to provide information to staff, students and the public about the personal information held by the University of Sydney, and to direct members of staff of the University to the procedures and practices required to comply with that Act and the *NSW Health Records and Information Privacy Act 2002.*

Produced by Archives and Records Management Services, the University of Sydney.

Contents

Foreword

The University of Sydney was incorporated by the Parliament of NSW on 1 October 1850, and operates under the *University of Sydney Act 1989* (as amended).

The second edition of this plan has been prepared in accordance with s.33 of the *NSW Privacy and Personal Information Protection Act 1998* to provide information to staff, students and the public about the personal information held by the University of Sydney, and to direct members of staff of the University to the procedures and practices required to comply with that Act and the *NSW Health Records and Information Privacy Act 2002*.

This Plan is an administrative instrument prepared in compliance with the Privacy Acts: it is not legal advice.

Issued by: Richard Fisher, General Counsel

Signature: 

Date: 04.03.13

1. Purpose

This Privacy Management Plan (hereafter this Plan) provides information to students, staff and members of the public about the personal information held by the University, and the procedures to be used to seek access to information about themselves and where appropriate, to correct it.

This Plan provides guidance to the staff of the University of Sydney on the procedures to comply with the two NSW privacy acts: the *Privacy and Personal Information Protection Act 1998* (hereafter the PPIP Act) and the *Health Records and Information Privacy Act 2002* (hereafter the HRIP Act), which deals only with health information. The two Acts are referred to in this Plan as the Privacy Acts.

The Plan does not constitute legal advice, nor can it cover every situation which may arise.

2. Scope

This Plan applies to the personal information and records of staff, students and members of the public held by the entire University. Faculties, departments, schools, foundations, centres and research institutes, administrative divisions and units must collect, manage and use the personal information they hold in accordance with this Plan.

It does *not* apply to information and records held by independent bodies established to serve the interests of students, which are not under the direction or control of the University's staff or structures. Such bodies include:

- Child care centres;
- Cumberland Student Guild;
- Residential colleges (with the exception of International House);
- Students' Representative Council (SRC);
- Sydney University Postgraduate Representative Association (SUPRA);
- Sydney Uni Sport and Fitness (SUSF); and
- The University of Sydney Union (USU).

This Plan applies to personal information in all forms of data capture and information collection, storage, analysis, use, communication, reporting and disclosure, including email and other correspondence, spreadsheets and other database applications, online and paper-based forms and meeting records. In certain circumstances it applies to verbal communication.

2.1 Audience

This Plan's procedures and guidance must be followed by all members of staff, affiliates and contractors. Henceforth, these three categories will be referred to collectively as staff.

Note: "Affiliates refers to clinical title holders; adjunct, conjoint and honorary appointees; consultants and contractors to the University; holders of offices in University entities, members of Boards of University Foundations, members of University Committees; and any other persons appointed or engaged by the University to perform duties or functions on its behalf." (*Code of Conduct – Staff and Affiliates*)

This Plan's description of the personal information held by the University is addressed to students, staff and members of the public to enable them to apply for access to their personal information.

The procedures for applying for access or making a complaint about a breach of the privacy principles are provided for use by anyone about whom information is held by the University.

2.2 Responsibilities

All staff must comply with the Privacy Acts in the course of their collecting, managing, using and disclosing personal information.

Staff who engage service providers or other contractors must ensure the provider or contractor complies with the Privacy Acts, noting the liability for compliance remains with the University.

Applications for access to University records and information under the Privacy Acts are directed to:

The Privacy Officer
Archives and Records Management Services
A14
University of Sydney NSW 2006

The Privacy Officer is responsible for processing applications; inquiries regarding an application should be directed to the Privacy Officer. For further details, see s.12 in this Plan.

Decisions to release records and information are made by the University's Group Secretary, in the Office of General Counsel.

3. References

NSW Privacy and Personal Information Protection Act 1998 (http://www.legislation.nsw.gov.au/fullhtml/inforce/act+133+1998+FIRST+0+N?)

NSW Health Records and Information Privacy Act 2002 (http://www.legislation.nsw.gov.au/fullhtml/inforce/act+71+2002+FIRST+0+N?)

The University's *Privacy Policy* (sydney.edu.au/policies)

The University's *Information Guide* (sydney.edu.au/arms/gipa)

The University's *Code of Conduct* (sydney.edu.au/policies)

The University's *Code of Conduct for Responsible Research Practice and Guidelines for Dealing with Allegations of Research Misconduct* (sydney.edu.au/policies)

Office of the NSW Privacy Commissioner: Public Interest Directions (Section 41 Directions) (http://www.ipc.nsw.gov.au/privacy/ipc_legislation.html)

Office of the NSW Privacy Commissioner: Statutory Guidelines ((http://www.ipc.nsw.gov.au/privacy/ipc_legislation.html)

4. Outline

The Plan:

- provides guidance to the interpretation of the Privacy Acts' definitions of personal information (s.5);
- identifies the principal collections and databases holding personal information (s.6);
- describes the information privacy and health principles for both Acts (s.7 – see also Appendices 1 and 2);
- outlines procedures, for collecting, storing, using, providing access to and disclosing personal information, to be followed by staff (s.8);
- describes the procedures for individuals to apply for access to their personal information (s.8.3 – see also Appendices 4.1, .2 and .3);
- describes the procedures for updating or correcting personal information (s.8.4 – see also Appendix 6);
- describes the procedures relating to an application for internal review of conduct including notification to the Privacy Commissioner (s.9 – see also Appendix 7);
- describes the process of external review of conduct (s.10);
- describes the University's training and awareness programs for staff and third-party service providers (s.11); and
- identifies the University officers responsible for implementing the Privacy Management Plan and processing applications under the Acts (s.12).

5. Definitions

5.1 Personal information

The *Privacy and Personal Information Protection Act* defines personal information as:

> "*…information or an opinion … about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion*" s.4(1).

The definition does not depend on the form or format of the information. The University holds personal information in all sorts of media, such as photographs and other image formats, video and film footage, voice recordings, computer-stored records including databases, fingerprint images, human tissue and DNA samples as well as paper-based formats.

Examples include (this list is not exhaustive):

- paper-based and electronic files on students, staff and contractors;
- the University's business systems, such as the student system, the human resources system and the finance system;
- University electoral rolls;
- alumni records;
- email addresses, mailing lists and other contact details;
- name-identified or Student Identification number (SID) identified student assessments;

- student/staff evaluation forms;
- the conflict of interests register, management plans and declaration of external interest forms;
- digital images;
- closed circuit television footage;
- human-based research data;
- human tissue samples;
- body registers;
- debtor records;
- library loan records.

5.2 Health information

The *Health Records and Information Privacy Act* defines health information as:

> "*(a) personal information that is information or an opinion about:*
>
> *(i) the physical or mental health or a disability (at any time) of an individual; or*
>
> *(ii) an individual's express wishes about the future provision of health services to him or her; or*
>
> *(iii) a health service provided, or to be provided, to an individual; or*
>
> *(b) other personal information collected to provide, or in providing, a health service; or*
>
> *(c) other personal information about an individual collected in connection with the donation, or intended donation, of an individual's body parts, organs or body substances; or*
>
> *(d) other personal information that is genetic information about an individual arising from a health service provided to the individual in a form that is or could be predictive of the health (at any time) of the individual or of any sibling, relative or descendant of the individual; or*
>
> *(e) healthcare identifiers*." (s.6).

The University holds health information in a wide variety of media and places, for example, certificates from health service providers, records of the University Health Service, counselling services and other clinics.

The Human Resources (HR) records hold health information about staff, for example, sick leave applications (with or without medical certificates). HR also hold workers' compensation case records and rehabilitation records.

Examples of health records of students held by the University are: Special Consideration forms and professional practitioner certificates; accident report forms; counselling records; and records of other student services such as those concerned with disability services or financial assistance which may hold information relating to students' health.

The other main areas of collection of health information are:

- teaching of medical and human science; and
- research about human health and development.

5.3 Exclusions from the definitions

Both Privacy Acts exclude the following categories of personal information from their scope:

- information which relates to a person who has been dead for more than 30 years; or
- information which is contained in a publicly available publication; or
- information which refers to a person's suitability for employment as a public sector official.

Information in a publicly available publication

The definitions exclude information about named or identifiable people which is published in newspapers, books or the Internet, broadcast on radio or television, posted on social media such as Facebook or Twitter, or made known at a public event like the graduation ceremonies of the University, because it is regarded as publicly available. Because such information is publicly available, it cannot be protected from use or further disclosure.

Note: Graduation ceremony programs containing the names of graduates are also distributed to the legal deposit libraries.

Employment-related information

Information referring to suitability for employment as a University member of staff (such as selection reports and references for appointment or promotions, or disciplinary records) is excluded from the definitions and therefore from the provisions of the Privacy Acts. Such information, however, is still treated by the University with the same care as if it were protected by the Acts.

Other employee-related personal information is protected by the Privacy Acts. For example, records or information about work activities such as video or photographs of staff in their workplace, are protected and may only be used in compliance with the Acts' provisions. Other examples of work-related personal information are staff training records, leave applications and attendance records. All these are within the scope of the definitions and are protected by the Acts.

Note: Workplace video footage from cctv is subject to the *Workplace Surveillance Act 2005*.

6. Types of personal information held by the University

The University collects and retains personal information in the course of undertaking its functions.

The broad functions of the University are:

1. Teaching;
2. Research;
3. Administration and Support; and
4. Community Engagement.

The records and personal data accumulated by the University are held in a wide variety of places, forms and formats. However, access to this information is best approached under the classifications derived from its statutory functions and activities undertaken to fulfil those functions. Requests for access under the PPIP Act in the first instance are made to the University's Privacy Officer (see s.12 of this Plan).

6.1 Teaching

Following are the principal records of teaching which hold personal information.

(a) Student records – electronic and hardcopy –record the units of study and the results against the name and student identification number (SID) of every student who has enrolled at the University. Also held are the student records that were received from the amalgamated institutions and their predecessors. Additional details of students include units of study attempted but not completed, prizes and scholarships attained by students, and graduation date and award conferred. Digital images are made and kept of each student as part of enrolment for the production of student cards and other University purposes. There are also contact details for the student including the email account provided by the University for official communications and other information which the student may provide for statistical purposes. The personal information accumulated through a student's time at the University is maintained principally in the computerised student system SydneyStudent ; the predecessor series of student records are held in the University Archives dating back to 1852 (registers of results, student record cards and also the records transferred from amalgamated institutions).

The records of students' results and degrees conferred are retained on a continuing basis. The fact of graduation (a public ceremony) and the degree conferred are both information in the public domain.

(b) Student files and other file-based records (in the format of paper or electronic documents, spreadsheets, email and other correspondence) relating to: students' applications for admission, enrolment, changes to enrolment, progression, deferral, withdrawal and graduation; and student assessment records including examinations, academic appeals, Special Consideration applications, academic dishonesty, misconduct, and exclusion. These records are retained for 6 years after the student's last year of enrolment.

(c) Learning management systems (WebCT, now a part of Blackboard): these systems contain teaching material, online class discussions, communications between students and academic staff and assessment records. These records are retained for six years after the last action date.

6.2 Research

The University conducts human-based research in a wide variety of areas. All human-based research projects must be approved by the University's Human Research Ethics Committee (HREC) which requires the researchers, staff and students, to inform human participants of what information about them will be collected, what it will be used for and how long it will be retained (provided in the Participant Information Statement).

Authorisation from participants to use and disclose their personal information in accordance with the description of the research in the Participant Information Statements is on the consent form and kept with the Participant Information Statement for as long as the research data are retained.

The information about participants (research data and contact information) in research projects conducted by University staff is retained by the University for up to 25 years after completion of the research, or in instances of research projects of national significance, the data may be retained on a

continuing basis. Conditions of holding, using and disclosing research data are as follows:

(a) The personal information held as research data may be collected by: administering questionnaires/surveys; conducting interviews or focus groups; investigating or observing human behaviour; routine testing of human participants; administering drugs, ionising radiation, chemical agents or vaccines including clinical trials; and any other experimentation involving human beings.

(b) The data can be held in a variety of formats (for example, paper, audio or video tape or film, electronic and tissue samples), and depending on the project may also be reported in the results and publications produced from the project. In many instances the research data is de-identified.

(c) The practice of sharing research data of human participants may only be done with data de-identified before action to share the data is taken, unless there is written consent from the participants to authorise sharing. The original consent forms identifying the participants are retained.

(d) It is the norm that publication of research data in which participants are identified or are identifiable be done with the written consent of the participants. For full the exceptions to this see health privacy principle 11 in Appendix 2 to this Plan.

The records of research administration hold the personal information of the researchers in relation to: the application for and administration of grants; application for ethical approval; intellectual property rights; reporting and publications; and commercialisation of research discoveries. This may include the personal information of student researchers and the personal information (eg, contact details) of human research participants. Research administration records are usually retained for a minimum of 7 years after completion of the project.

6.3 Administration and Support

The University's principal administrative activities are governance, managing the University's funds, managing real property (land and buildings), procuring equipment and supplies, and hiring and managing staff. The principal support activities are provision of libraries, recordkeeping and information and communication technology, publications and web services, legal services, human support services in areas of health, disabilities, counselling, student financial and other support services. While recordkeeping underpins the creation and control of records for all of these activities, the following records are the main holdings of personal information about staff, students and sometimes members of the public:

(a) staff – Recruitment and HR systems which manage the hiring and management of staff; staff files (paper-based and electronic) which hold the records relating to individual members of staff; case management files (non-routine staff matters); and workers' compensation and rehabilitation records. The University's External Interests Policy requires the creation of a number of documents which contain personal information, including the register of conflict of interests, declarations of external interests and conflict of interest management plans. Digital images are taken of all staff members which are used for the production of staff identification cards and other University purposes. Payment records are managed by the pay system. Older staff records (cards and paper-based files) are held by the University Archives but only files of prominent members of staff are retained on a continuing basis; the other staff files are destroyed 7

years after separation or when the person would reach the age of 75, whichever is longer. A summary record of the service of every permanent member of staff is also retained on a continuing basis;

Note: As stated above, information about an individual's suitability for public employment, i.e., with the University, is excluded from the definition of personal information and not protected by the PPIP Act. Nevertheless, much of the personal information which the University holds about its staff (for example, contact details and home address) is protected by the privacy legislation.

(b) the records of the governing bodies (the Senate, Academic Board, the Senior Executive Group, Faculty boards and their committees) of the University refer to members of staff, students and members of the public from time to time. The background information will usually also be held on files in the records management system;

(c) procurement records may incidentally hold personal information about suppliers and vendors (for example, sole traders or property transactions);

(d) the business systems which are discussed above and below under the headings, Teaching, Research, Administration and Support and Community Engagement hold personal information. The systems are managed by the relevant administrative unit of the University;

(e) Information and Communications Technology (ICT) manage the IT infrastructure of the University which includes all servers and the email system and many other business applications. There is personal information throughout the records and data held in the various systems but it is normally managed and accessed in line with the business activities outlined above;

(f) the University provides: a medical service available to staff, students and members of the public, the records of which hold individuals' health information, managed and accessible in accordance with the provisions of the HRIP Act; disability and counselling services for students, which hold health and personal information likewise managed and accessible in accordance with the provisions of the HRIP Act; other support services for students (such as accommodation, financial assistance, study support), the records of which hold personal information primarily about students but which may also include personal information about third parties (e.g., student's family members); and

(g) library services (e.g., borrowing records), legal services (litigation and other case files) and publication and web services all hold personal information to a lesser degree, access to which may be sought under the PPIP Act.

6.4 Community Engagement

The University produces and makes available, free and for purchase, a range of publications about the University and its activities including publications of a scholarly nature. It also presents events such as public lectures, seminars, concerts and performances of the Carillon. Venues include the Seymour Centre, Sydney College of the Arts and the Sydney Conservatorium of Music. The University opens its collections to the public, in the University libraries, the University Archives, the University Art Gallery, the Macleay and Nicholson museums and other small museums. While most personal information and data accumulated through these activities are in the public domain, there is some information which is not public and which is protected by PPIP Act:

(a) the alumni database – generated from the graduation records of the student system but includes contact details and updates logged by the

alumni themselves or by the alumni office. Accessible with the permission of the individual alumnus or alumna and maintained by the University on a continuing basis; and

(b) donors' records – held by the development office. These contain contact details, details of donations made (gifts and bequests) and other information about individual donors; much of the information is confidential and is maintained by the University on a continuing basis; and

(c) collections – records of users and donors including contact details and records of visits and access to the collections; some information is confidential and is maintained on a continuing basis by the University.

7. Privacy principles

Both the PPIP and HRIP acts contain sets of principles which govern conduct to protect personal information. They are:

- Information Protection Principles (IPPs); and
- Health Privacy Principles (HPPs).

Note: Appendices 1 and 2 list the IPPs and the HPPs.

These principles set out legal obligations for:

- collection;
- storage;
- access and accuracy;
- use; and
- disclosure of personal and health information.

There are additional Health Privacy Principles concerning:

- the use of identifiers to protect identity;
- the right to anonymity in receiving health services;
- the flow of health information across the NSW border; and
- the consent to link health records of an individual in a system.

The University must comply with all information privacy principles in order to comply with the legislation.

The Principles given in the PPIP Act for protecting personal information (IPPs) are outlined in Appendix 1 of this Plan; the Principles of the HRIP Act for protecting heath information (HPPs) are outlined in Appendix 2 of this Plan.

8. Procedures

8.1 Collection

Information must only be collected by lawful means for purposes related to the functions and activities of the University. These purposes include:

- admission, enrolment, assessment, and graduation of students;
- communication with prospective and current students, and graduates;
- selection, employment, appraisal, and remuneration of staff;
- teaching;
- research; and
- receipt and payment of monies.

Whenever possible, the University must collect personal information directly from the individual to whom the information relates. The individual may authorise the collection of information from someone else. In the case of persons under the age of 16, their parent or guardian may authorise the collection of information from someone else.

Examples of circumstances where it is acceptable for the University to collect personal information from other sources include HSC results from the Universities Admission Centre (which is authorised by the applicant on the UAC form) and assessments of students on field work or professional experience programs.

Collection of personal and health information must be relevant and necessary to the University's purpose, and must be:

- accurate;
- up-to-date;
- complete; and
- not excessive.

The collection of information must not unreasonably intrude into the personal affairs of the individual.

For example, a student who has had surgery and needs to recuperate should present a medical certificate (or Professional Practitioner Certificate for Special Consideration) which is limited to stating the impact of the surgical procedure on his/her ability to study. The University does not need to know the nature of the procedure.

When the University collects personal or health information, it must:

- make it explicit that personal information is being collected;
- make it clear who is collecting the information and provide contact details;
- explain the reason the information is being collected;
- state what offices of the University will receive the information;
- state what are the other parties to which the personal information is usually disclosed;
- make clear the basis on which the information is being sought:
    - if required by law, explain what that law is;
    - if the supply of the information is voluntary, set out any consequences of not supplying it; and
- make it clear that the person supplying the information has rights of

access to, and correction of, the information.

This is usually done in the form of a privacy statement detailing the relevant points at the time individuals are asked to provide personal information. When the collection is occurring online, the privacy statement should be presented before any information is collected (see Appendix 3 for an example of an all-encompassing privacy statement). In some instances, forms will already meet some of the collection requirements and only a brief privacy statement will be necessary to meet all the collection requirements such as in the privacy related forms in the appendices to this Plan.

Examples

- Application forms (both hardcopy and online) for admission, enrolment, leave or Special Consideration collect personal information and so must comply with the collection requirements listed above.
- RSVP forms on invitations collect personal information and so should indicate if the contact information of respondents is intended to be kept for further contact, and provide an option to refuse permission to do so.

Notice must be given when it may not be obvious that personal information is being collected:

- where video cameras (CCTV) are used for security purposes, a notice must be placed in the areas covered by the cameras in compliance with the *Workplace Surveillance Act 2005*;
- where biometric identification devices for security systems are in use, a warning must be given; and
- when using social media such as Facebook and Twitter for research or promotional purposes.

Where information is collected over the phone, providers of the information must be told in advance if the information they supply about themselves is to be retained.

If unsolicited personal information is retained by the University, it must be handled and stored in compliance with the privacy legislation.

Examples

- General applications for employment.
- Details of a student's or his/her family's situation in applications submitted for assistance or Special Consideration.

Note: If possible the record of information about a third party should not be retained but a summary made by the University staff member receiving it and then the document handed back.

8.2 Storage

Retention and security of personal information

Personal information, both paper-based and electronic media, must be stored securely in University systems and protected from unauthorised access and alteration. Personal information must not be stored in any "cloud computing" solution.

Note: See the Defence Signals Directorate, Cyber Security Operations Centre, Initial Guidance, 6/2011 *Cloud Computing Security Considerations*, 12 April 2011: http://www.dsd.gov.au/infosec/cloudsecurity.htm

Personal information must be kept only as long as it is necessary for the purposes for which it may lawfully be used. When it is no longer needed, the personal information must be destroyed using a secure waste destruction service (for paper-based documents) and formal deletion processes for

electronic documents and data. This includes complete wiping or the reformatting of hard drives of computers and other equipment such as photocopier/scanners before they are disposed of or returned to leasing firms. The physical destruction of obsolete hard drives, where owned by the University, may also be appropriate.

Authorising disposal

Personal and health information in University records can only be disposed of in accordance with the University Recordkeeping Policy and the *NSW State Records Act 1998*. Destruction of records holding personal information must be properly authorised and appropriately supervised. Where undertaken off-site a certificate of destruction may be required.

Retention and disposal of files and documents controlled by Records Online, both paper and electronic, is managed by Archives and Records Management Services. Destruction of other documents or data holding personal information (eg, research data) must be approved by the head of the unit, authorised by specific citation of classes from the records disposal authorities issued by the State Records Authority of NSW.

For more information

- See Archives and Records Management Services website, Records Disposal: sydney.edu.au/arms/records_mgmt/services.shtml
- Contact the Deputy University Archivist on (02) 9351 7262, or the Disposal Officer on (02) 9036 9536, for specific advice.

8.3 Access

The Privacy Acts establish for individuals a right of access to information about themselves.

Individuals are entitled to know whether information about them is held by the University, the nature of the information, the main purposes for which it is used, and how they may gain access to it, including a right of correction if details are not correct. This right does not extend to a right to know the personal information about any other individual (third party).

Access to information and records created and controlled by NSW government agencies is regulated by four main acts of Parliament:

NSW State Records Act 1998;

NSW Privacy and Personal Information Protection Act 1998;

NSW Health Records and Information Privacy Act 2002; and

NSW Government Information (Public Access) Act 2009.

The *State Records Act* provides access to government records more than 30 years old. The Privacy Acts provide a right of access to personal information by individuals, allowing individuals to ensure the information held is up-to-date and correct. The *Government Information (Public Access) Act* (GIPA) provides a right of access to government information including personal information. It replaced the *NSW Freedom of Information Act 1989.*

As a matter of policy, the University encourages people to apply for access for information about themselves under the Privacy Acts, which do not require payment of an application fee. The Privacy Acts do not set down formal procedures for providing access to information. However, any conditions or limitations on access arising in the GIPA Act apply to release of personal information under the privacy acts as if the application had been made under GIPA. The GIPA Act must be used for access to information about an individual for information relating to employment or promotion. The GIPA Act's procedures are formal and highly regulated and include an application fee ($30, if no discount applies).

Student and staff access to their personal information

The University provides access to both staff and students to records about themselves under s.8 (Informal Release) of GIPA without the need to invoke the formal procedures of the legislation. The forms for making an application for access to the various categories of personal information are at Appendices 4.1–.3.

Informal release: Students

The Academic Board's *Assessment Procedure 2011* provides students with rights of access to their exam scripts.

Students may see their student file by application for access under s.8 of GIPA (see forms at Appendix 4). A week's notice is needed (for the faculty to prepare the file by numbering the pages and removing incidental references to other people). There is no fee.

For other personal information held in records such as Special Consideration forms, Student Appeals Body (SAB) proceedings or disciplinary proceedings, students may apply for access formally under the PPIP Act (see below and see the application forms in the appendices).

Informal release: Staff

Under GIPA, and as a matter of long-standing practice, University of Sydney staff are able to access:

- their staff files; and
- information about why they were unsuccessful in applying for another University position (selection process) or for academic promotion, without making a formal application under the legislation.

Staff have access to their routine records of personnel administration through *myHROnline*. They may still request access to their staff file by completing the relevant form at Appendix 4.2 to send to the HR Service Centre. A week should be allowed for access to be arranged. No fee is required.

Note: staff files are now electronic and consist of a number of sub-folders. Access to the folders containing routine records is afforded by this long-standing University administrative practice. Folder -008 (HR Advice) is used for non-routine matters and a formal application under the GIPA Act may be required by a staff member seeking access to its contents.

Unsuccessful (internal *and* external) candidates for appointment should apply to Sydney Recruitment or to the Chair of the Selection Committee for a copy of the part of the report which is about them. They may also request access to their referees' reports by formal request under the GIPA Act.

Unsuccessful applicants for academic promotion should request access to the report of the Committee to the Chair of the Local Promotions Committee (see *Academic Promotions Policy*, at sydney.edu.au/policies)

Providing access to a staff or student file

The process for preparing files for individuals to see is much the same for staff or students. The most important thing to check is references to other people (third parties) on the file which must be removed or redacted before release.

Note: "Third parties" does not include members of staff whose names are recorded in the course of carrying out their duties. Names of staff are not regarded as "personal information" in this context.

Once the file has been retrieved:

(i) number all the documents (folios) beginning with the oldest (normally at the back of the file) and check to see if there are references to other

people;

(ii) if there are references to other people, remove the folio (numbered) for temporary safekeeping, make a photocopy or scan of it and black out the name(s) and identifying details. Photocopy or save the blacked-out (redacted) folio again and place this copy on the file in the place of the original; and

(iii) ensure that the file does not contain any documents covered by legal privilege by removing those documents and putting an explanation page in their place.

The file may now be provided to the staff member or student to read under supervision.

If the staff member or student wants a copy of part or the whole of the file, a small charge for copying may be made, not exceeding fifteen dollars.

After the staff member or student has seen the file, and before it is put away, if any folio were removed and replaced with a redacted copy, then the original folio should be restored to its place and the redacted copy together with the application for access should both be attached to the file. If copies were provided, a note specifying the folio numbers of the copies should be placed on the file with the date they were provided.

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

Members of the public and students or staff (who want access to records other than their student or personal file), may apply for access under the PPIP Act to their personal information held by the University using the general PPIP Act application form at Appendix 4. There is no application fee.

Applications are processed in 20 working days using the GIPA Act processes as a guide. A written acknowledgement of receipt of the application must be posted to the applicant within 5 working days.

The privacy staff in the University's Archives and Records Management Services gather the records and information from the relevant business units, assesses them for information which is out of scope, identifies any information which is not in the public interest to release, and prepares a recommendation for the University's Group Secretary regarding release. The decision to release the records and information is made by the University's Group Secretary.

If individuals other than the applicant are mentioned in the records, it may be necessary to consult them about the release of the documents. An additional 10 working days to allow for the consultation is added to the time to process the application, and the applicant is notified.

The consulted individuals may object to the release of information about themselves which is then taken into account by the decision-maker, but the objection may not be upheld. The consulted individuals are informed of any decision to release their personal information contrary to their wishes and of their rights of review of the decision. The applicant is informed of the decision to release but no material can be released until the consulted individuals have had the opportunity to exercise their rights of internal review of the decision.

The consulted individuals also have the right to take the outcome of an internal review either to the Privacy Commissioner and/or the Administrative Decisions Tribunal. Again, no information can be released to the original applicant until any external review is completed.

Other details in the information sought by the original applicant may be considered not in the public interest to release. The public interest considerations which may weigh against the disclosure of information are taken from s.14 of the GIPA Act (see Appendix 5). Any information not

disclosed is listed in a schedule provided with the copies of the released records or information. Individual documents may have portions or words (e.g., names of third parties) redacted, which are also listed. The applicant may indicate the preferred format in which the information should be provided with which, in most cases, the University will comply. The applicant is told of his or her rights to review when the decision and copies are provided.

If an applicant is not satisfied with the decision, she or he may apply to the University for an Internal Review, which is conducted by a different officer of the University, one who is not under the supervision of the original decision-maker. The applicant may also take the matter direct to an external review by the Privacy Commissioner or by the Administrative Decisions Tribunal. None of these applications for review requires payment of any fee.

Internal review of the decision in response to an application for access to personal information applicant is a Review of Conduct under s.53 of the PPIP Act (see below).

8.4 Accuracy

The Privacy Acts establish for individuals a right to correct information about themselves held by government agencies.

The University must not use personal information without taking reasonable steps to ensure that the information is relevant, accurate, up-to-date, complete and not misleading. One of the reasons individuals are able to access personal information about themselves under the legislation is so they have the opportunity to ensure the information is correct.

Communication

Ensuring contact information is up-to-date and accurate is an obligation under the legislation to guard against accidental disclosure of personal information by sending a communication to the wrong person. Particular care must be taken when using electronic forms of communication, for example, when sending email to multiple recipients, that the personal information of the other recipients is not disclosed to any individual recipient. An email address may name, or otherwise identify, the recipient and so is classified as personal information.

The University-issued student email address is the only email address to be used for formal University communication to a student. Staff sending communications to several students must ensure that they do not inadvertently disclose email addresses of the other students to any individual student. It is preferable to send emails individually only.

Use of social media such as Facebook or Twitter is limited to providing information to students on a broadcast basis, as for any other website presence. Social media must not be used for responding to any current or prospective student's question where the response would include personal information or would be giving specific advice regarding candidature. The student's official email account only should be used for providing University information specific to a current individual student. Other means of private communication should be used for prospective students.

Verification and correction

- Students verify their personal information as a part of the enrolment process. They may also check it at any time through the *MyUni* portal. Changes to contact information can be made online any time at the student administration area of MyUni, see: sydney.edu.au/current_students/student_administration
- Alumni can correct or update their personal information using AlumniOnline, see: sydney.edu.au/alumni/

- Staff can correct or update their personal information by using myHROnline, see: myhr.sydney.edu.au

All three sites require Unikey log-in access and are secure.

Note: Changes of name or corrections to names are submitted by the individual concerned supported by the original, relevant documents (e.g., marriage or birth certificate, passport). The original documents must be sighted by the University officer making the amendment and then returned to the individual.

This may also be done electronically (that is, by email) with scanned supporting documents. However, the scanned documents must be verified by presenting the originals when the individual is able to visit the University in person.

Applications for changes to other personal information are submitted to the Group Secretary. Examples of the changes which are not routine matters and require a formal application are statements about a person's health, competence, or qualifications which are considered inaccurate or misleading

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.

The person to whom the inaccurate 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.

Procedure for amendment of information

First, the University must be satisfied of the individual's identity and authority to request the change. The University can request evidence of identity or authority to confirm this.

There is a form at Appendix 6 to submit which asks for specific details of the claim that the personal or health information is inaccurate, out-of-date, irrelevant, incomplete or misleading. The application form is sent to the Group Secretary.

The University may then agree to amend the information and will let the individual know. 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. A statement of the amendment request is nonetheless attached to the relevant file or information as notified by the individual.

8.5 Use

The University must use personal information only for the purpose for which it was collected, or for a directly related purpose, unless consent has been obtained from the individual.

Privacy statement and communication

"Use" is understood as referring to an individual's personal information within the University. The use described in the privacy statement provided on all forms and in online collection of information sets the parameters for the University's use of personal information. As communication with individuals (students or members of the public) is a primary reason for collecting personal information, care must be taken to ensure contact information is up-to-date and accurate and that communication is only made for the use notified. When using email for communicating with multiple individuals, staff should note that the email addresses are also personal information and ensure they are not disclosed to any individual but the intended recipient.

Note: If a commercial service provider is being used for sending bulk email, the contract must include appropriate privacy measures. Contact the Office of General Counsel for advice. Otherwise Mail Merge must be used. While Blind Copying (BCC)

will hide email addresses of multiple recipients, mistakes are too easily made, and once an email message has been sent outside the University, it cannot be recalled.

Generally, only those University staff members who need to know particular personal information in order to carry out their work have access to it. The personal information is used by the section of the University named to the individual when it was collected for the purpose(s) notified at that time. It must not be used for a different purpose without authorisation from the individual concerned. It may be used by another section of the University for the same purpose or a directly related purpose.

For example, personal information may be used by another section or disclosed outside the University in the following instances:

- where the use is directly related to the purpose for which the information was collected (e.g., using student results for awarding prizes or identifying a student at risk of failing);
- if it is necessary to prevent or lessen a serious and imminent threat to life or health of any person (e.g., providing health information if a student or staff member is taken ill);
- if it is required for investigation relating to law enforcement purposes or to protect the public revenues (e.g., criminal investigations, but see the section below on requests from law enforcement agencies); or
- where the use and/or disclosure is permitted by a Public Interest Direction made by the NSW Privacy Commissioner.

Photographs

Students and staff have photo identity cards. The digital images taken for the student and staff cards are created and used for legitimate University identification purposes.

If the images of staff or students are needed for other University purposes such as a publication or for the web, the photographs are taken for that purpose and the individuals involved must sign a release form to authorise that use for a specified period of time. The form must be stored and be linked to the image. The image must be deleted or otherwise destroyed when the authorised time period has elapsed. Model release forms are available at: sydney.edu.au/staff/marketing_communications/design/permission.shtml

Health information to assist students

Using health information to provide assistance to students or staff with a disability is an appropriate use but it should only be provided and used on a need-to-know basis. As stated above under “Collection”, the information used should be confined to the impact of the disability and limited in detail. Such use should be made known to the individual concerned and authorisation given in advance wherever possible.

8.6 Disclosure

The University does not disclose personal information it holds about a student, a former student, a graduate, a member of staff or a member of the public to an external third party or organisation without the individual's express consent unless required or authorised by law.

“Disclosure” generally means providing an individual’s personal information to another person or another organisation outside the University.

Express consent

Express consent means that the University has been in contact with the individual concerned and obtained consent to disclose information that is precise as to the kind and, if possible, the exact contents of the information to which the consent relates, and precise as to whom the information may be disclosed. 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.

Express consent is *not* needed if the individual was told at the time of collection of the personal information that it would be disclosed to named third parties.

References for either students or staff should not be provided unless the individual has made a request for a reference, or in other words, given consent to the disclosure of the personal information.

Use of social media

Social media, especially Facebook and Twitter, are increasingly used as a means of communicating to current and potential students. Social media are considered to be communication in the public domain.

Care must be taken when using public interactive web applications for such social media *not* to use them in an interactive manner when any personal information might be collected or disclosed. Any such communication made to an individual student is a University record and must comply with the privacy legislation.

Exceptions to the non-disclosure rule:

- disclosure of the personal information is required for a purpose directly related to the purpose for which the information was collected and the University has no reason to believe the individual would object to the disclosure;
- it is reasonable to assume the individual is aware that the information is usually disclosed to the other organisation or party (this disclosure is usually included in the privacy statement the individual saw when supplying the information);
- it is reasonable to believe that the disclosure is necessary to prevent or lessen a serious and imminent threat to life or health of the individual or any other person;
- it is required for law enforcement or investigation purposes. In such instances, a valid warrant or court order (subpoena) may be required; ;
- the disclosure is required, permitted, implied or reasonably contemplated by an act or any other law; and
- the disclosure is permitted by a Public Interest Direction made by the NSW Privacy Commissioner.

Requests from law enforcement agencies

Note: The Privacy Acts define “law enforcement agencies” as the Police Service, or the police force of another State or a Territory; the New South Wales Crime Commission; the Australian Federal Police; the National Crime Authority; the Director of Public Prosecutions of New South Wales, of another State or a Territory, or of the Commonwealth; the Department of Corrective Services; and the Department of Juvenile Justice.

If a University member of staff is asked by a law enforcement officer for information or documents about any person, whether in person or in writing, the member of staff must refer the law enforcement officer to the Office of General Counsel who will brief the relevant senior officer of the University to assist with the decision regarding the release of the information.

Under no circumstances should a member of staff provide personal information in response to a request by telephone to a party outside the University without either the express consent of the individual to whom the information relates , or authorisation from the relevant officer of the University.

Emergencies do happen, and there are occasions when personal information is disclosed without reference to the individual for authorisation. Decisions to disclose personal information held by the University without the consent of the individual concerned are made as follows:

- relating to students - by the Registrar or his nominee (currently the Director, Student Lifecycle Management);
- relating to staff members - by the University's Director, Human Resources;
- relating to members of the public - by the University's Group Secretary.

A record of the decision and the basis on which it is made is kept in the University's corporate records system.

The University has the discretion to disclose personal information to law enforcement agencies without the consent of the individuals concerned or a warrant when the disclosure:

• concerns proceedings for an offence or for law enforcement purposes;

• is related to the whereabouts of a person reported as missing to the police, and the disclosure is to be made directly to a law enforcement agency;

• is reasonably necessary for the protection of public revenue or to investigate an offence where there are reasonable grounds to believe that an offence has been committed.

It is important to note that the University is not required to disclose personal information in the absence of a search warrant, subpoena or other lawful requirement.

Subpoenas and warrants

Subpoenas or warrants, issued by a court or a magistrate, which demand the release of information or records are forwarded to the Office of General Counsel which supervises the response to the subpoena or warrant (see below).

Subpoenas, warrants and other judicial orders are required to name the University Registrar as the Proper Officer of the University from whom the court seeks information. General Counsel may accept service of such documents on behalf of the University. The legal proceedings can be litigation to which the University is joined as a party, or they can be matters to which the University is not a party.

Solicitors or insurance companies seeking personal information from the University are informed that the University will not supply personal information without:

- the written consent of the subject of the information; or
- a subpoena or similar court order.

The Office of General Counsel supervises all responses to such demands. Individual departments or officers must not accept or deal with requests from solicitors, subpoenas or other orders except as directed by the General Counsel. No other officer is permitted to disclose University records in relation to legal proceedings.

Restricted personal information

There are some categories of personal information given stricter protection under s.19 of the PPIP Act. They are personal information relating to:

- an individual's ethnic or racial origin;
- political opinions;
- religious or philosophical beliefs;
- trade union membership; and
- sexual activities.

These categories of information are generally collected and used for statistical purposes and may only be disclosed if it is necessary to prevent a serious or imminent threat to the life or health of the individual concerned or of another person. There are exceptions such as for providing services or assistance to specific groups of students, or if another act requires the disclosure (see s.25 of the PPIP Act).

Health information was included in this set of categories but is now governed by its own legislation – *Health Records and Information Privacy Act* (see below for procedures).

Commonwealth government departments

Notices issued under Commonwealth Acts override the provisions of any NSW legislation by virtue of s.109 of the Constitution, which provides that where a State law is inconsistent with a law of the Commonwealth, the latter prevails and former is invalid, to the extent of the inconsistency.

Various Commonwealth government departments under their legislation require the University to disclose personal information to them.

Departments with responsibilities such as social security and services (including Centrelink), immigration and taxation have a lawful need and right to access some personal information held by the University. Students are informed in general of these requirements in the Enrolment Privacy Statement.

The University supplies the information to any Commonwealth department requiring personal information about students only in response to a formal (written) notice under the department's legislation citing the relevant section. Such requests are normally processed and recorded by the Student Centre.

Under amendments made to the *Higher Education Support Act 2003* (HES Act) in 2012, the Department of Industry, Innovation, Science, Research and Tertiary Education is able to disclose personal information about staff or students from the University to a number of specified agencies and organisations. Any personal information so disclosed is protected by the HES Act.

If there is a non-routine request for personal information from a Commonwealth government agency, please contact the Privacy Officer on 9351 4263.

Tax file numbers

The collection, use and disclosure of Tax File Numbers (TFN) by the University is controlled by the *Commonwealth Privacy Act 1988*. The Commonwealth Privacy Commissioner has issued extensive, legally binding Tax file number guidelines which are available at: http://www.comlaw.gov.au/Details/F2011L02748

The University must ensure that Tax file numbers are protected against loss, unauthorised access, use, modification, disclosure or other misuse.

External service providers

External service providers contracted to the University are subject to the NSW privacy laws. For the purposes of the privacy legislation, they are regarded as part of the University and the University is responsible if there is a privacy breach. Service providers must be made aware that personal information held by the University to which they have access must be handled in compliance with the privacy legislation.

The contract under which service providers are engaged must specify exactly what personal information is to be provided to them and include a confidentiality agreement. The contract must specify that either the personal information is returned to the University, or destroyed in a secure manner, when the service has been completed. The contract must specify how the information is to be returned or destroyed and the service provider must certify that no copies of the information have been retained by them. Please refer to the Office of General Counsel for the current version of the University's standard contract.

Information technology vendors and service providers who may require access to the University's business systems in order to fulfil the requirements of their contract must sign non-disclosure agreements before they are granted access to the systems. For further information please contact the Office of General Counsel: sydney.edu.au/legal/

Contractors and volunteers, while working for the University, must comply with the Privacy Acts just as if they were a part of the University as the University is liable for any breaches. Contracts or agreements about working arrangements must include reference to privacy requirements if access to personal or health information is involved.

8.7 Use and disclosure of health information

The PPIP and HRIP Acts have different requirements relating to the use and disclosure of personal and health information.

There is no distinction made between "use" and "disclosure" of health information in the HRIP Act. The strict rules for *disclosure* apply to *use* of health information within the University.

The University does not use or disclose an individual's health information for any purpose other than the original purpose for which it was collected. The original purpose is called the primary purpose.

In certain circumstances, generally related to the medical purpose for which health information is originally collected, stored, provided or used, health information may be disclosed lawfully without authorisation by the individual concerned. Any purpose for which it may be lawful to disclose health information without further authorisation is referred to as a secondary purpose.

Health information must be protected from unauthorised use and disclosure wherever it is held and all authorised use and disclosure made of it should be tracked or recorded.

Teaching

The HRIP Act recognises the need for health services to share information about an individual in order to provide appropriate service, and the need to train and educate health service providers. All such use and disclosure require that consent be given as far as possible.

Please see the NSW Privacy Commissioner's website for a copy of the statutory guideline on training.

http://www.ipc.nsw.gov.au/privacy/ipc_legislation.html

Research

The HRIP Act recognises the value of health information for research and provides statutory guidelines for its use in research based on obtaining consent and where appropriate, using means to remove identification. Research using health information should use de-identified information where possible.

Please see the NSW Privacy Commissioner's website for a copy of the statutory guidelines on research:

http://www.ipc.nsw.gov.au/privacy/ipc_legislation.html

Consent to use and/or disclose individuals' health information in the course of the research must be obtained and recorded. The records of consent must be linked to, or be incorporated into the participant information statement given to the individual about how, why and what health information (research data) will be collected, used and disclosed in the research. The participant information statement governs the use and disclosure of the health information for the duration of the research project. A copy of the participant information statement with the record of consent must be provided to the participant and a copy retained by the Chief Investigator. These records of the consent of the individual(s) must be retained in accessible form with the research information used in the research for as long as the research information is retained.

Note: It is sometimes impossible to obtain consent for the use and/or disclosure of health information for research purposes. Under the *Statutory guidelines on research* issued by the NSW Privacy Commissioner if the project meets the 5 requirements in Part 1 clause 1.2 of those *Guidelines*, the University's HREC may exempt the researcher from obtaining the consent of individuals to use and disclose their health information. This is not the normal course of obtaining, using and /or disclosing health information in research.

General

Health information must be not be used or disclosed unless:

- the University has obtained consent from the person;
- it is used for a related health treatment or research purpose (called the secondary purpose) and the secondary purpose is within the reasonable expectations of the person;
- there is a serious threat to the health, safety or welfare of the person or to public health or safety;
- it is reasonably necessary for the management of health services, training or research;
- it is necessary to find a missing person;
- there is a suspected unlawful activity, unsatisfactory professional conduct or breach of discipline;
- it is for law enforcement purposes;
- it is lawfully authorised or required, or permitted under another law; or
- it is disclosed on compassionate grounds.

Under the *NSW Work Health and Safety Act 2011*, there is a duty to disclose information to supervisors which will reduce, eliminate or minimise risks to health or safety in the workplace. When health information is provided by a member of staff to a supervisor for this purpose, it should not be further disclosed except where necessary to reduce or eliminate risks. The supervisor may seek the consent of the member of staff before further disclosing the information.

8.8 Additional health information protection principles

Identifiers and anonymity

The HRIP Act provides an additional information privacy principle (12) concerning the use of identifiers assigned by organisations to protect individuals' identities. This can be done only if it is reasonably necessary for the organisation to carry out its functions efficiently. Such identifiers, which have no meaning outside the research, should be assigned where possible in the case of research using health data so that it is de-identified.

Note: The key elements of identifying individuals are full names, dates of birth and addresses. All three elements are removed to de-identify data for research use. Email addresses in online research are the equivalent to both names and residential addresses. Where age is significant to the research it should limited to the age in years. The identifying details are replaced by a unique identifier, preferably a running number. If the de-identification of data is adequate the data is no longer subject to the Privacy Acts.

The identifier stands for the individual. In many circumstances, for example, Student Identification numbers which are widely used in the University, the use and disclosure of the identifier itself is governed by the same sort of requirements for consent from the individuals concerned as identified health information.

There is a further information privacy principle, 13, in the HRIP Act which provides the right of individuals to receive health services without having to identify themselves, where this is practicable and lawful.

Transferrals and linkage

The University must not transfer any health information outside New South Wales or the Commonwealth unless it is sent to a jurisdiction which the University reasonably believes has a similar standard of privacy protection for health information.

The University must not include health information about any individual in a health records linkage system unless the individual has expressly consented to this.

While the proposal to link health records across health services and across state borders is based on the intention of providing better health services, the links or transfers of health information must not be undertaken except with the individual's express consent.

9. Complaints or internal review

An individual who considers his or her privacy has been breached can make a complaint to the University under s.53 of PPIP Act and request a formal, internal review of the University's conduct in relation to the privacy matter.

A breach of an individual's privacy is defined as a breach of one or more of the Information Protection Principles or the Health Privacy Principles.

Applications for internal review must:

- be in writing;
- be addressed to the Privacy Officer ;
- include a return address in Australia; and
- be lodged with the University within six months of the time the applicant first became aware of the conduct which is the subject of the application.

There is a form at Appendix 7 for applying for a review of conduct under s.53 of the PPIP Act.

The internal review is conducted by an officer of the University who has not had any involvement in the matter which gave rise to the complaint of breach of privacy.

The PPIP Act requires that the NSW Privacy Commissioner be informed of the receipt of an application for an internal review of conduct, and receive regular

progress reports of the investigation. In addition, the Commissioner is entitled to make submissions to the University in relation to the application for internal review.

There is an example of a letter of notification to the Privacy Commissioner of receipt of request for an internal review at Appendix 8.

The person processing the internal review must consider any relevant material submitted by:

- the applicant; and
- the Privacy Commissioner.

The University follows the model of the internal review process provided by the Office of the Privacy Commissioner. A copy is at Appendix 8**.**

An internal review must be completed within 60 days of the receipt of the application. The applicant is advised of the finding within 14 days of the completion of the review.

The University may:

- take no further action on the matter;
- make a formal apology to the applicant;
- take appropriate remedial action, which may include the payment of monetary compensation to the applicant;
- undertake that the conduct will not occur again; and/or
- implement administrative measures to ensure that the conduct will not occur again.

A summary of the findings of the review must be given to the Commissioner within 14 days of its completion.

10. External review

An individual who considers his or her privacy has been breached can also make a complaint to the Privacy Commissioner under s.45 without going through the internal review process of the University.

If the applicant is unhappy with the outcome of the University's internal review she or he can apply to the NSW Administrative Decisions Tribunal (the Tribunal) to review the decision. If the University has not completed the internal review within 60 days, the applicant can also take the matter to the Tribunal.

The Tribunal can review the conduct from which the complaint arose, or the University's internal review decision and subsequent action. The Tribunal will assess whether or not the University complied with its privacy obligations.

The Tribunal may order the University to change its practices, apologise, or take steps to remedy any damage suffered, including payment of monetary compensation for any financial loss, or psychological or physical harm suffered by the applicant because of the University's conduct.

11. Communication and training

11.1 Communication

Archives and Records Management Services (ARMS) distribute hard copies of the Privacy Management Plan to all heads of units and heads of departments. Electronic access is provided through the University's Privacy website: sydney.edu.au/arms/privacy/privacy_mgmt_plan.shtml

Reference is made to compliance with the privacy legislation in the Code of Conduct which is provided to all new staff.

The issue of the revised Privacy Management Plan will be publicised through the weekly electronic *Staff News.* ARMS conduct a program of briefings for

faculties and administrative units on a regular basis as well as providing more detailed training on demand.

Any member of staff who has a query about personal information and privacy protection may phone or email the Privacy officers at any time for information about compliance with the privacy legislation or more specific advice (see s.12 of this Plan).

11.2 Training

Training courses on how to comply with the privacy legislation are delivered each semester for all University staff, on a voluntary basis, through the Learning Solutions unit. The courses cover the general outline of the Information and Health Privacy Principles but are tailored to specific issues such as management of email or student recordkeeping. They include discussion of typical scenarios to help staff apply the definitions and procedures outlined in the Plan.

Briefings are also provided to faculties and administrative units on request in relation to specific issues. In response to demand, guidelines on specific issues are released by the Privacy officers, on such matters as email management (in planning), student academic appeals or drafting privacy statements.

A privacy training module is available through CareerPath in myHRonline for University staff and affiliates. A specific online module is also available for researchers at the same location.

A link to materials developed by the Office of the NSW Privacy Commissioner is included in the University's Privacy website: Sydney.edu.au/arms/privacy

12. Contact information

Please direct all privacy enquiries to the following officers:

Tim Robinson
Privacy Officer
Archives A14
University of Sydney NSW 2006
Telephone: (02) 9351 4263
Email: tim.robinson@sydney.edu.au

Anne Picot
Privacy Officer
Archives A14
University of Sydney NSW 2006
Telephone: (02) 9351 7262
Email: anne.picot@sydney.edu.au

May Robertson
Privacy Officer
Records Management Services A14
University of Sydney NSW 2006
Telephone: (02) 9351 2037
Email:
may.robertson@sydney.edu.au

Appendix 1 – Information Protection Principles

Privacy and Personal Information Protection Act 1998 – Division I

8 Collection of personal information for lawful purposes

(1) A public sector agency must not collect personal information unless:

(a) the information is collected for a lawful purpose that is directly related to a function or activity of the agency; and

(b) the collection of the information is reasonably necessary for that purpose.

(2) A public sector agency must not collect personal information by any unlawful means.

9 Collection of personal information directly from individual

A public sector agency must, in collecting personal information, collect the information directly from the individual to whom the information relates unless:

(a) the individual has authorised collection of the information from someone else; or

(b) in the case of information relating to a person who is under the age of 16 years, the information has been provided by a parent or guardian of the person.

10 Requirements when collecting personal information

If a public sector agency collects personal information from an individual, the agency must take such steps as are reasonable in the circumstances to ensure that, before the information is collected or as soon as practicable after collection, the individual to whom the information relates is made aware of the following:

(a) the fact that the information is being collected;

(b) the purposes for which the information is being collected;

(c) the intended recipients of the information;

(d) whether the supply of the information by the individual is required by law or is voluntary, and any consequences for the individual if the information (or any part of it) is not provided;

(e) the existence of any right of access to, and correction of, the information; and

(f) the name and address of the agency that is collecting the information, and the agency that is to hold the information.

11 Other requirements relating to the collection of personal information

If a public sector agency collects personal information from an individual, the agency must take such steps as are reasonable in the circumstances (having regard to the purposes for which the information is collected) to ensure that:

(a) the information collected is relevant to that purpose, is not excessive, and is accurate, up-to-date and complete; and
(b) the collection of the information does not intrude to an unreasonable extent on the personal affairs of the individual to whom the information relates.

12 Retention and security of personal information

A public sector agency that holds personal information must ensure:

(a) that the information is kept for no longer than is necessary for the purposes for which the information may lawfully be used; and

(b) that the information is disposed of securely and in accordance with any requirements for the retention and disposal of personal information; and

(c) that the information is protected, by taking such security safeguards as are reasonable in the circumstances, against loss, unauthorised access, use, modification or disclosure, and against all other misuse; and

(d) that, if it is necessary for the information to be given to a person in connection with the provision of a service to the agency, everything reasonably within the power of the agency is done to prevent unauthorised use or disclosure of the information.

13 Information about personal information held by agencies

A public sector agency that holds personal information must take such steps as are, in the circumstances, reasonable to enable any person to ascertain:

(a) whether the agency holds personal information; and

(b) whether the agency holds personal information relating to that person; and

(c) if the agency holds personal information relating to that person:

(i) the nature of that information; and

(ii) the main purposes for which the information is used; and

(iii) that person's entitlement to gain access to the information.

14 Access to personal information held by agencies

A public sector agency that holds personal information must, at the request of the individual to whom the information relates and without excessive delay or expense, provide the individual with access to the information.

15 Alteration of personal information

(1) A public sector agency that holds personal information must, at the request of the individual to whom the information relates, make appropriate amendments (whether by way of corrections, deletions or additions) to ensure that the personal information:

(a) is accurate; and

(b) having regard to 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.

(2) If a public sector agency is not prepared to amend personal information in accordance with a request by the individual to whom the information relates, the agency must, if so

requested by the individual concerned, take such steps as are reasonable to attach to the information, in such a manner as is capable of being read with the information, any statement provided by that individual of the amendment sought.

(3) If personal information is amended in accordance with this section, the individual to whom the information relates is entitled, if it is reasonably practicable, to have recipients of that information notified of the amendments made by the public sector agency.

(4) This section, and any provision of a privacy code of practice that relates to the requirements set out in this section, apply to public sector agencies despite section 25 of this Act and section 21 of the *State Records Act 1998*.

(5) The Privacy Commissioner's guidelines under section 36 may make provision for or with respect to requests under this section, including the way in which such a request should be made and the time within which such a request should be dealt with.

(6) In this section (and in any other provision of this Act in connection with the operation of this section), ***public sector agency*** includes a Minister and a Minister's personal staff.

16 An agency must check accuracy of personal information before use

A public sector agency that holds personal information must not use the information without taking such steps as are reasonable in the circumstances to ensure that, having regard to the purpose for which the information is proposed to be used, the information is relevant, accurate, up-to-date, complete and not misleading.

17 Limits on the use of personal information

A public sector agency that holds personal information must not use the information for a purpose other than that for which it was collected unless:

(a) the individual to whom the information relates has consented to the use of the information for that other purpose; or

(b) the other purpose for which the information is used is directly related to the purpose for which the information was collected; or

(c) the use of the information for that other purpose 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.

18 Limits on disclosure of personal information

(1) A public sector agency that holds personal information must not disclose the information to a person (other than the individual to whom the information relates) or other body, whether or not such other person or body is a public sector agency, unless:

(a) the disclosure is directly related to the purpose for which the information was collected, and the agency disclosing the information has no reason to believe that the individual concerned would object to the disclosure; or

(b) the individual concerned is reasonably likely to have been aware, or has been made aware in accordance with section 10, that information of that kind is usually disclosed to that other person or body; or

(c) the agency believes on reasonable grounds that the disclosure is necessary to prevent or lessen a serious and imminent threat to the life or health of the individual concerned or another person.

(2) If personal information is disclosed in accordance with subsection (1) to a person or body that is a public sector agency, that agency must not use or disclose the information for a purpose other than the purpose for which the information was given to it.

19 Special restrictions on disclosure of personal information

(1) A public sector agency must not disclose personal information relating to an individual's ethnic or racial origin, political opinions, religious or philosophical beliefs, trade union membership or sexual activities unless the disclosure is necessary to prevent a serious and imminent threat to the life or health of the individual concerned or another person.

(2) A public sector agency that holds personal information must not disclose the information to any person or body who is in a jurisdiction outside New South Wales or to a Commonwealth agency unless:

(a) a relevant privacy law that applies to the personal information concerned is in force in that jurisdiction or applies to that Commonwealth agency; or

(b) the disclosure is permitted under a privacy code of practice.

(3) For the purposes of subsection (2), a *relevant privacy law* means a law that is determined by the Privacy Commissioner, by notice published in the Gazette, to be a privacy law for the jurisdiction concerned[1].

(4) The Privacy Commissioner is to prepare a code relating to the disclosure of personal information by public sector agencies to persons or bodies outside New South Wales and to Commonwealth agencies.

(5) Subsection (2) does not apply:

(a) until after the first anniversary of the commencement of this section; or

(b) until a code referred to in subsection (4) is made,

whichever is the later.

[1] At the time of the production of this Plan, the Privacy Commissioner had made no such determinations.

Appendix 2 – Health Privacy Principles

Health Records and Information Privacy Act 2002 – Schedule 1

1 Purposes of collection of health information

(1) An organisation must not collect health information unless:

(a) the information is collected for a lawful purpose that is directly related to a function or activity of the organization; and

(b) the collection of the information is reasonably necessary for that purpose.

(2) An organisation must not collect health information by any unlawful means.

2 Information must be relevant, not excessive, accurate and not intrusive

An organisation that collects health information from an individual must take such steps as are reasonable in the circumstances (having regard to the purposes for which the information is collected) to ensure that:

(a) the information collected is relevant to that purpose, is not excessive and is accurate, up-to-date and complete; and

(b) the collection of the information does not intrude to an unreasonable extent on the personal affairs of the individual to whom the information relates.

3 Collection to be from the individual concerned

(1) An organisation must collect health information about an individual only from that individual, unless it is unreasonable or impracticable to do so.

(2) Health information is to be collected in accordance with any guidelines issued by the Privacy Commissioner for the purposes of this clause.

4 Individual to be made aware of certain matters

(1) An organisation that collects health information about an individual from the individual must, at or before the time that it collects the information (or if that is not practicable, as soon as practicable after that time), take steps that are reasonable in the circumstances to ensure that the individual is aware of the following:

(a) the identity of the organisation and how to contact it;

(b) the fact that the individual is able to request access to the information;

(c) the purposes for which the information is collected;

(d) the persons to whom (or the types of persons to whom) the organisation usually discloses information of that kind;

(e) any law that requires the particular information to be collected; and

(f) the main consequences (if any) for the individual if all or part of the information is not provided.

(2) If an organisation collects health information about an individual from someone else, it must take any steps that are reasonable in the circumstances to ensure that the

individual is generally aware of the matters listed in subclause (1) except to the extent that:

(a) making the individual aware of the matters would pose a serious threat to the life or health of any individual; or

(b) the collection is made in accordance with guidelines issued under subclause (3).

(3) The Privacy Commissioner may issue guidelines setting out circumstances in which an organisation is not required to comply with subclause (2).

(4) An organisation is not required to comply with a requirement of this clause if:

(a) the individual to whom the information relates has expressly consented to the organisation not complying with it; or

(b) the organisation is lawfully authorised or required not to comply with it; or

(c) non-compliance is otherwise permitted (or is necessarily implied or reasonably contemplated) under the Act or any other law (including the *State Records Act 1998*); or

(d) compliance by the organisation would, in the circumstances, prejudice the interests of the individual to whom the information relates; or

(e) the information concerned is collected for law enforcement purposes; or

(f) the organisation is an investigative agency and compliance might detrimentally affect (or prevent the proper exercise of) its complaint handling functions or any of its investigative functions.

(5) If the organisation reasonably believes that the individual is incapable of understanding the general nature of the matters listed in subclause (1), the organisation must take steps that are reasonable in the circumstances to ensure that any authorised representative of the individual is aware of those matters.

(6) Subclause (4) (e) does not remove any protection provided by any other law in relation to the rights of accused persons or persons suspected of having committed an offence.

(7) The exemption provided by subclause (4) (f) extends to any public sector agency, or public sector official, who is investigating or otherwise handling a complaint or other matter that could be referred or made to an investigative agency, or that has been referred from or made by an investigative agency.

5 Retention and security

(1) An organisation that holds health information must ensure that:

(a) the information is kept for no longer than is necessary for the purposes for which the information may lawfully be used, and

(b) the information is disposed of securely and in accordance with any requirements for the retention and disposal of health information, and

(c) the information is protected, by taking such security safeguards as are reasonable in the circumstances, against loss, unauthorised access, use, modification or disclosure, and against all other misuse, and

(d) if it is necessary for the information to be given to a person in connection with the provision of a service to the organisation, everything reasonably within the power of the organisation is done to prevent unauthorised use or disclosure of the information.

> **Note:** Division 2 (Retention of health information) of Part 4 contains provisions applicable to private sector persons in connection with the matters dealt with in this clause.

(2) An organisation is not required to comply with a requirement of this clause if:

(a) the organisation is lawfully authorised or required not to comply with it; or

(b) non-compliance is otherwise permitted (or is necessarily implied or reasonably contemplated) under an Act or any other law (including the *State Records Act 1998).*

(3) An investigative agency is not required to comply with subclause (1) (a).

6 Information about health information held by organisations

(1) An organisation that holds health information must take such steps as are, in the circumstances, reasonable to enable any individual to ascertain:

(a) whether the organisation holds health information; and

(b) whether the organisation holds health information relating to that individual; and

(c) if the organisation holds health information relating to that individual:

(i) the nature of that information; and
(ii) the main purposes for which the information is used; and
(iii) that person's entitlement to request access to the information.

(2) An organisation is not required to comply with a provision of this clause if:

(a) the organisation is lawfully authorised or required not to comply with the provision concerned; or

(b) non-compliance is otherwise permitted (or is necessarily implied or reasonably contemplated) under an Act or any other law (including the *State Records Act 1998*).

7 Access to health information

(1) An organisation that holds health information must, at the request of the individual to whom the information relates and without excessive delay or expense, provide the individual with access to the information.

> **Note:** Division 3 (Access to health information) of Part 4 contains provisions applicable to private sector persons in connection with the matters dealt with in this clause.

Access to health information held by public sector agencies may also be available under the *Government Information (Public Access) Act 2009* or the *State Records Act 1998*.

(2) An organisation is not required to comply with a provision of this clause if:

(a) the organisation is lawfully authorised or required not to comply with the provision concerned; or

(b) non-compliance is otherwise permitted (or is necessarily implied or reasonably contemplated) under an Act or any other law (including the *State Records Act 1998*).

8 Amendment of health information

(1) An organisation that holds health information must, at the request of the individual to whom the information relates, make appropriate amendments (whether by way of corrections, deletions or additions) to ensure that the health information:

(a) is accurate; and

(b) having regard to 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.

(2) If an organisation is not prepared to amend health information under subclause (1) in accordance with a request by the individual to whom the information relates, the organisation must, if so requested by the individual concerned, take such steps as are reasonable to attach to the information, in such a manner as is capable of being read with the information, any statement provided by that individual of the amendment sought.

(3) If health information is amended in accordance with this clause, the individual to whom the information relates is entitled, if it is reasonably practicable, to have recipients of that information notified of the amendments made by the organisation.

> **Note:** Division 4 (Amendment of health information) of Part 4 contains provisions applicable to private sector persons in connection with the matters dealt with in this clause.

Amendment of health information held by public sector agencies may also be able to be sought under the *Privacy and Personal Information Protection Act 1998*.

(4) An organisation is not required to comply with a provision of this clause if:

(a) the organisation is lawfully authorised or required not to comply with the provision concerned; or

(b) non-compliance is otherwise permitted (or is necessarily implied or reasonably contemplated) under an Act or any other law (including the *State Records Act 1998*).

9 Accuracy

An organisation that holds health information must not use the information without taking such steps as are reasonable in the circumstances to ensure that, having regard to the purpose for which the information is proposed to be used, the information is relevant, accurate, up-to-date, complete and not misleading.

10 Limits on use of health information

(1) An organisation that holds health information must not use the information for a purpose (a ***secondary purpose***) other than the purpose (the ***primary purpose***) for which it was collected unless:

(a) **Consent**
the individual to whom the information relates has consented to the use of the information for that secondary purpose; or

(b) **Direct relation**
the secondary purpose is directly related to the primary purpose and the individual would reasonably expect the organisation to use the information for the secondary purpose, or

> **Note:** For example, if information is collected in order to provide a health service to the individual, the use of the information to provide a further health service to the individual is a secondary purpose directly related to the primary purpose.

(c) **Serious threat to health or welfare**
the use of the information for the secondary purpose is reasonably believed by the organisation to be necessary to lessen or prevent:

(i) a serious and imminent threat to the life, health or safety of the individual or another person; or
(ii) a serious threat to public health or public safety; or

(d) **Management of health services**
the use of the information for the secondary purpose is reasonably necessary for the funding, management, planning or evaluation of health services and:

(i) either:
(A) that purpose cannot be served by the use of information that does not identify the individual or from which the individual's identity cannot reasonably be ascertained and it is impracticable for the organisation to seek the consent of the individual for the use; or
(B) reasonable steps are taken to de-identify the information; and

(ii) if the information is in a form that could reasonably be expected to identify individuals, the information is not published in a generally available publication; and

(iii) the use of the information is in accordance with guidelines, if any, issued by the Privacy Commissioner for the purposes of this paragraph; or

(e) **Training**
the use of the information for the secondary purpose is reasonably necessary for the training of employees of the organisation or persons working with the organisation and:

(i)either:
(A) that purpose cannot be served by the use of information that does not identify the individual or from which the individual's identity cannot reasonably be ascertained and it is impracticable for the organisation to seek the consent of the individual for the use; or
(B) reasonable steps are taken to de-identify the information; and

(ii) if the information could reasonably be expected to identify individuals, the information is not published in a generally available publication; and

(iii) the use of the information is in accordance with guidelines, if any, issued by the Privacy Commissioner for the purposes of this paragraph; or

(f) **Research**
the use of the information for the secondary purpose is reasonably necessary for research, or the compilation or analysis of statistics, in the public interest and:

(i) either:
(A) that purpose cannot be served by the use of information that does not identify the individual or from which the individual's identity cannot reasonably be ascertained and it is impracticable for the organisation to seek the consent of the individual for the use; or
(B) reasonable steps are taken to de-identify the information; and

(ii) if the information could reasonably be expected to identify individuals, the information is not published in a generally available publication; and

(iii) the use of the information is in accordance with guidelines, if any, issued by the Privacy Commissioner for the purposes of this paragraph; or

(g) **Find a missing person**
the use of the information for the secondary purpose is by a law enforcement agency (or such other person or organisation as may be prescribed by the regulations) for the purposes of ascertaining the whereabouts of an individual who has been reported to a police officer as a missing person; or

(h) **Suspected unlawful activity, unsatisfactory professional conduct or breach of discipline**
the organisation:

(i) has reasonable grounds to suspect that:

(A) unlawful activity has been or may be engaged in; or

(B) a person has or may have engaged in conduct that may be unsatisfactory professional conduct or professional misconduct under the *Health Practitioner Regulation National Law (NSW)*; or

(C) an employee of the organisation has or may have engaged in conduct that may be grounds for disciplinary action; and

(ii) uses the health information as a necessary part of its investigation of the matter or in reporting its concerns to relevant persons or authorities; or

(i) **Law enforcement**
the use of the information for the secondary purpose is reasonably necessary for the exercise of law enforcement functions by law enforcement agencies in circumstances where there are reasonable grounds to believe that an offence may have been, or may be, committed; or

(j)**Investigative agencies**
the use of the information for the secondary purpose is reasonably necessary for the exercise of complaint handling functions or investigative functions by investigative agencies; or

(k) **Prescribed circumstances**
the use of the information for the secondary purpose is in the circumstances prescribed by the regulations for the purposes of this paragraph.

(2) An organisation is not required to comply with a provision of this clause if:

(a) the organisation is lawfully authorised or required not to comply with the provision concerned; or

(b) non-compliance is otherwise permitted (or is necessarily implied or reasonably contemplated) under an Act or any other law (including the *State Records Act 1998*).

(3) The Ombudsman's Office, Health Care Complaints Commission, Anti-Discrimination Board and Community Services Commission are not required to comply with a provision of this clause in relation to their complaint handling functions and their investigative, review and reporting functions.

(4) Nothing in this clause prevents or restricts the disclosure of health information by a public sector agency:

(a) to another public sector agency under the administration of the same Minister if the disclosure is for the purposes of informing that Minister about any matter within that administration; or

(b) to any public sector agency under the administration of the Premier, if the disclosure is for the purposes of informing the Premier about any matter.

(5) The exemption provided by subclause (1) (j) extends to any public sector agency, or public sector official, who is investigating or otherwise handling a complaint or other

matter that could be referred or made to an investigative agency, or that has been referred from or made by an investigative agency.

11 Limits on disclosure of health information

(1) An organisation that holds health information must not disclose the information for a purpose (a ***secondary purpose***) other than the purpose (the ***primary purpose***) for which it was collected unless:

(a) **Consent**
the individual to whom the information relates has consented to the disclosure of the information for that secondary purpose; or

(b) **Direct relation**
the secondary purpose is directly related to the primary purpose and the individual would reasonably expect the organisation to disclose the information for the secondary purpose; or

Note: For example, if information is collected in order to provide a health service to the individual, the disclosure of the information to provide a further health service to the individual is a secondary purpose directly related to the primary purpose.

(c) **Serious threat to health or welfare**
the disclosure of the information for the secondary purpose is reasonably believed by the organisation to be necessary to lessen or prevent:

(i) a serious and imminent threat to the life, health or safety of the individual or another person; or

(ii) a serious threat to public health or public safety; or

(d) **Management of health services**
the disclosure of the information for the secondary purpose is reasonably necessary for the funding, management, planning or evaluation of health services and:

(i) either:

(A) that purpose cannot be served by the disclosure of information that does not identify the individual or from which the individual's identity cannot reasonably be ascertained and it is impracticable for the organisation to seek the consent of the individual for the disclosure; or
(B) reasonable steps are taken to de-identify the information; and

(ii) if the information could reasonably be expected to identify individuals, the information is not published in a generally available publication; and

(iii) the disclosure of the information is in accordance with guidelines, if any, issued by the Privacy Commissioner for the purposes of this paragraph; or

(e) **Training**
the disclosure of the information for the secondary purpose is reasonably necessary for the training of employees of the organisation or persons working with the organisation and:

(i) either:

(A) that purpose cannot be served by the disclosure of information that does not identify the individual or from which the individual's identity cannot reasonably be ascertained and it is impracticable for the organisation to seek the consent of the individual for the disclosure; or
(B) reasonable steps are taken to de-identify the information; and

(ii) if the information could reasonably be expected to identify the individual, the information is not made publicly available; and

(iii) the disclosure of the information is in accordance with guidelines, if any, issued by the Privacy Commissioner for the purposes of this paragraph; or

(f) **Research**
the disclosure of the information for the secondary purpose is reasonably necessary for research, or the compilation or analysis of statistics, in the public interest and:

(i) either:

(A) that purpose cannot be served by the disclosure of information that does not identify the individual or from which the individual's identity cannot reasonably be ascertained and it is impracticable for the organisation to seek the consent of the individual for the disclosure; or

(B) reasonable steps are taken to de-identify the information; and

(ii) the disclosure will not be published in a form that identifies particular individuals or from which an individual's identity can reasonably be ascertained; and

(iii) the disclosure of the information is in accordance with guidelines, if any, issued by the Privacy Commissioner for the purposes of this paragraph; or

(g) **Compassionate reasons**
the disclosure of the information for the secondary purpose is to provide the information to an immediate family member of the individual for compassionate reasons and:

(i) the disclosure is limited to the extent reasonable for those compassionate reasons; and

(ii) the individual is incapable of giving consent to the disclosure of the information; and

(iii) the disclosure is not contrary to any wish expressed by the individual (and not withdrawn) of which the organisation was aware or could make itself aware by taking reasonable steps; and

(iv) if the immediate family member is under the age of 18 years, the organisation reasonably believes that the family member has sufficient maturity in the circumstances to receive the information; or

(h) **Find a missing person**
the disclosure of the information for the secondary purpose is to a law enforcement agency (or such other person or organisation as may be prescribed by the regulations) for the purposes of ascertaining the whereabouts of an individual who has been reported to a police officer as a missing person; or

(i) **Suspected unlawful activity, unsatisfactory professional conduct or breach of discipline**
the organisation:

(i) has reasonable grounds to suspect that:

(A) unlawful activity has been or may be engaged in; or

(B) a person has or may have engaged in conduct that may be unsatisfactory professional conduct or professional misconduct under the *Health Practitioner Regulation National Law (NSW)*; or

(C) an employee of the organisation has or may have engaged in conduct that may be grounds for disciplinary action; and

(ii) discloses the health information as a necessary part of its investigation of the matter or in reporting its concerns to relevant persons or authorities, or

(j) **Law enforcement**
the disclosure of the information for the secondary purpose is reasonably necessary for the exercise of law enforcement functions by law enforcement agencies in circumstances where there are reasonable grounds to believe that an offence may have been, or may be, committed; or

(k) **Investigative agencies**
the disclosure of the information for the secondary purpose is reasonably necessary for the exercise of complaint handling functions or investigative functions by investigative agencies; or

(l) **Prescribed circumstances**
the disclosure of the information for the secondary purpose is in the circumstances prescribed by the regulations for the purposes of this paragraph.

(2) An organisation is not required to comply with a provision of this clause if:
(a) the organisation is lawfully authorised or required not to comply with the provision concerned; or

(b) non-compliance is otherwise permitted (or is necessarily implied or reasonably contemplated) under an Act or any other law (including the *State Records Act 1998*); or

(c) the organisation is an investigative agency disclosing information to another investigative agency.

(3) The Ombudsman's Office, Health Care Complaints Commission, Anti-Discrimination Board and Community Services Commission are not required to comply with a provision of this clause in relation to their complaint handling functions and their investigative, review and reporting functions.

(4) Nothing in this clause prevents or restricts the disclosure of health information by a public sector agency:

(a) to another public sector agency under the administration of the same Minister if the disclosure is for the purposes of informing that Minister about any matter within that administration; or

(b) to any public sector agency under the administration of the Premier, if the disclosure is for the purposes of informing the Premier about any matter.

(3) If health information is disclosed in accordance with subclause (1), the person, body or organisation to which it was disclosed must not use or disclose the information for a purpose other than the purpose for which the information was given to it.

(4) The exemptions provided by subclauses (1) (k) and (2) extend to any public sector agency, or public sector official, who is investigating or otherwise handling a complaint or other matter that could be referred or made to an investigative agency, or that has been referred from or made by an investigative agency.

12 Identifiers

(1) An organisation may only assign identifiers to individuals if the assignment of identifiers is reasonably necessary to enable the organisation to carry out any of its functions efficiently.

(2) Subject to subclause (4), a private sector person may only adopt as its own identifier of an individual an identifier of an individual that has been assigned by a public sector agency (or by an agent of, or contractor to, a public sector agency acting in its capacity as agent or contractor) if:

(a) the individual has consented to the adoption of the same identifier; or

(b) the use or disclosure of the identifier is required or authorised by or under law.

(3) Subject to subclause (4), a private sector person may only use or disclose an identifier assigned to an individual by a public sector agency (or by an agent of, or contractor to, a public sector agency acting in its capacity as agent or contractor) if:

(a) the use or disclosure is required for the purpose for which it was assigned or for a secondary purpose referred to in one or more paragraphs of HPP 10 (1) (c)–(k) or 11 (1) (c)–(l); or

(b) the individual has consented to the use or disclosure; or

(c) the disclosure is to the public sector agency that assigned the identifier to enable the public sector agency to identify the individual for its own purposes.

(4) If the use or disclosure of an identifier assigned to an individual by a public sector agency is necessary for a private sector person to fulfil its obligations to, or the requirements of, the public sector agency, a private sector person may either:

(a) adopt as its own identifier of an individual an identifier of the individual that has been assigned by the public sector agency; or

(b) use or disclose an identifier of the individual that has been assigned by the public sector agency.

13 Anonymity

Wherever it is lawful and practicable, individuals must be given the opportunity to not identify themselves when entering into transactions with or receiving health services from an organisation.

14 Transborder data flows and data flow to Commonwealth agencies

An organisation must not transfer health information about an individual to any person or body who is in a jurisdiction outside New South Wales or to a Commonwealth agency unless:

(a) the organisation 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 Health Privacy Principles; or

(b) the individual consents to the transfer; or

(c) the transfer is necessary for the performance of a contract between the individual and the organisation, or for the implementation of pre-contractual measures taken in response to the individual's request; or

(d) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the individual between the organisation and a third party; or

(e) all of the following apply:

(i) the transfer is for the benefit of the individual;

(ii) it is impracticable to obtain the consent of the individual to that transfer;

(iii) if it were practicable to obtain such consent, the individual would be likely to give it; or

(f) the transfer is reasonably believed by the organisation to be necessary to lessen or prevent:

(i) a serious and imminent threat to the life, health or safety of the individual or another person; or

(ii) a serious threat to public health or public safety; or

(g) the organisation has taken reasonable steps to ensure that the information that it has transferred will not be held, used or disclosed by the recipient of the information inconsistently with the Health Privacy Principles; or

(h) the transfer is permitted or required by an Act (including an Act of the Commonwealth) or any other law.

15 Linkage of health records

(1) An organisation must not:

(a) include health information about an individual in a health records linkage system unless the individual has expressly consented to the information being so included; or

(b) disclose an identifier of an individual to any person if the purpose of the disclosure is to include health information about the individual in a health records linkage system, unless the individual has expressly consented to the identifier being disclosed for that purpose.

(2) An organisation is not required to comply with a provision of this clause if:

(a) the organisation is lawfully authorised or required not to comply with the provision concerned; or

(b) non-compliance is otherwise permitted (or is necessarily implied or reasonably contemplated) under an Act or any other law (including the *State Records Act 1998*); or

(c) the inclusion of the health information about the individual in the health records information system (including an inclusion for which an identifier of the individual is to be disclosed) is a use of the information that complies with HPP 10 (1) (f) or a disclosure of the information that complies with HPP 11 (1) (f).

(3) In this clause:

Health record means an ongoing record of health care for an individual.

Health records linkage system means a computerised system that is designed to link health records for an individual held by different organisations for the purpose of facilitating access to health records, and includes a system or class of systems prescribed by the regulations as being a health records linkage system, but does not include a system or class of systems prescribed by the regulations as not being a health records linkage system.

Appendix 3 – Example of a Privacy Statement

(**Note**: The PPIP Act does not specify how the information required to be provided by s.10 when collecting personal information must be given. It is usual to include a privacy statement, but some or all of the required information can be included in an introductory statement on a web site or in a covering letter or explanatory document accompanying a form. What is important is that all the requirements of s.10 are met.)

The personal information collected on this form will be used by the Office of Chocolate of the University of Sydney for the purpose of processing your application for chocolate and for communicating with you about your application. The supply of information by you is voluntary, but if you do not provide all the information requested you may not receive the chocolate to which you may be entitled.

Your personal information will not be disclosed to any other person or organisation outside the University except with your express consent or where required or allowed by law. You should be aware that the University is required by the Commonwealth *Chocolate Act 2010* to provide the names of chocolate recipients to the Department of Chocolate in Canberra.

It may be necessary to correspond about your application with other offices of the University in the process of determining your eligibility for chocolate and providing the chocolate. Your personal information will be provided to those other offices on a need-to-know basis. Information given to this office in confidence will be kept securely and will not be provided to any other person or office without proper authorisation but absolute confidentiality is not possible.

Your application may be used for statistical and similar reporting purposes but the personal information will be de-identified and the data presented in aggregation.

You may apply at any time to see what personal information about you is held by the University and to check its accuracy. If any of the information is inaccurate, out-of-date or incorrect, you may apply to have the information corrected.

If you consider the University has not managed or used your personal information in accordance with this statement you may apply for a Review of Conduct (privacy complaint) under section 53 of the NSW *Privacy and Personal Information Protection Act 1998.*

Please contact us with any queries you may have about the management of your personal information, or call the Privacy Officer at (02) 9351 4362. Please see the University's Privacy web page for further information and to access application forms: sydney.edu.au/arms/privacy

Appendix 4.1 – Application for access to a student file

Under section 8 of the NSW *Government Information (Public Access) Act 2009*, students may have access to their student files by submitting this form to their Faculty Office.

Appointments must be made with the relevant Faculty Office to view the student file. Please allow at least one week for the Faculty Office to prepare the file for access. Preparation consists of numbering all the folios (pages) of the file and removing any incidental references to third parties which may have been placed on the file.

The exact time should be negotiated with the staff in the Faculty Office.

Your details

Surname: ..... **Title**: Mr/Ms/Dr/Prof

Other names: .....

Daytime telephone: .....

Email: .....

SID: .....

Faculty: .....

I wish to access the student file held on me by the University.

Signature: .....

Date: .....

Conditions of access to student files:

- I will only be able to view the file under the supervision of a member of the Faculty staff;
- I may be charged for copies of material held on the file;
- I may not remove, add to or annotate the file or its contents*****; and
- Incidental information relating to other students which may be on my file will not be made available to me.

** If there is out-of-date, inaccurate or misleading information on the file, you may apply under s.15 of the Privacy and Personal Information Protection Act 1998 for correction. Please contact the University Privacy Officer: tim.robinson@sydney.edu.au*

The exact time should be negotiated with the staff in the Faculty Office.

Faculty use only:

Appointment date and time: .....

Staff member supervising access: .....

Appendix 4.2 – HR Service Centre application form for access to a staff file

Your name:	
Your staff ID number:	
Requested date to view your staff file:	
What section(s) of your staff file would you like to view? *(tick one or more sections below)*	
Employment	
Leave	
Leave – SSP	
Performance	
Payroll	
Immigration	
Termination	
List the reason(s) why you would like to view your staff file:	
User obligations Staff files may contain personal information which may only be used in accordance with the University's Privacy Policy and Code of Conduct. Staff members are not permitted to access files other than for the purposes of undertaking their duties. Unauthorised disclosure of personal information may constitute a breach of the University's Code of Conduct, which could result in disciplinary action for misconduct. I have read and understood the above user obligations.	
Signature:	Date:

Appendix 4.3 – Application for access to personal information held by the University of Sydney

Please complete this form to apply for access to personal information held by the University about you under section 14 of the NSW *Privacy and Personal Information Protection Act 1998*. If you need help in filling out this form, please contact the Privacy Officer on (02) 9351 4263, or visit the website at www.sydney.edu.au/arms/privacy

Your details

Surname: ..... **Title**: Mr/Ms/Dr/Prof

Other names: .....

Postal address: .....

..... **Postcode**: .....

Daytime telephone: .....

Email: .....

Information sought

I request access under s.14 of the NSW *Privacy and Personal Information Protection Act 1998* to personal information concerning me held by the University of Sydney including:

.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....

Applicant's signature: ..... Date: .....

There is no fee for applications to access personal information about yourself under the privacy legislation.

Post this form to: The Privacy Officer, ARMS, A14, University of Sydney, NSW 2006 Australia

The supply of the information is voluntary, but if you do not provide all the information requested, the University may not be able to process your request. The information on this form will be used by the University's Privacy staff and will not be disclosed outside the University without your express consent except where required or authorised by law. Any enquiries regarding access to, or correction of, personal information about you held by the University should be addressed to the Privacy officers at the above address.

Appendix 5 – Public interest considerations against disclosure from the NSW *Government Information (Public Access) Act 2009*

14 Public interest considerations against disclosure

(1) It is to be conclusively presumed that there is an overriding public interest against disclosure of any of the government information described in Schedule 1.

(2) The public interest considerations listed in the Table to this section are the only other considerations that may be taken into account under this Act as public interest considerations against disclosure for the purpose of determining whether there is an overriding public interest against disclosure of government information.

1 Responsible and effective government

There is a public interest consideration against disclosure of information if disclosure of the information could reasonably be expected to have one or more of the following effects (whether in a particular case or generally):

(a) prejudice collective Ministerial responsibility;
(b) prejudice Ministerial responsibility to Parliament;
(c) prejudice relations with, or the obtaining of confidential information from, another government;
(d) prejudice the supply to an agency of confidential information that facilitates the effective exercise of that agency's functions;
(e) reveal a deliberation or consultation conducted, or an opinion, advice or recommendation given, in such a way as to prejudice a deliberative process of government or an agency;
(f) prejudice the effective exercise by an agency of the agency's functions;
(g) found an action against an agency for breach of confidence or otherwise result in the disclosure of information provided to an agency in confidence;
(h) prejudice the conduct, effectiveness or integrity of any audit, test, investigation or review conducted by or on behalf of an agency by revealing its purpose, conduct or results (whether or not commenced and whether or not completed).

2 Law enforcement and security

There is a public interest consideration against disclosure of information if disclosure of the information could reasonably be expected to have one or more of the following effects (whether in a particular case or generally):

(a) reveal or tend to reveal the identity of an informant or prejudice the future supply of information from an informant;
(b) prejudice the prevention, detection or investigation of a contravention or possible contravention of the law or prejudice the enforcement of the law;
(c) increase the likelihood of, or prejudice the prevention of, preparedness against, response to, or recovery from, a public emergency (including any natural disaster, major accident, civil disturbance or act of terrorism);

(d) endanger, or prejudice any system or procedure for protecting, the life, health or safety of any person;
(e) endanger the security of, or prejudice any system or procedure for protecting, any place, property or vehicle;
(f) facilitate the commission of a criminal act (including a terrorist act within the meaning of the *Terrorism (Police Powers) Act 2002*);
(g) prejudice the supervision of, or facilitate the escape of, any person in lawful custody; or
(h) prejudice the security, discipline or good order of any correctional facility.

3 Individual rights, judicial processes and natural justice

There is a public interest consideration against disclosure of information if disclosure of the information could reasonably be expected to have one or more of the following effects:

(a) reveal an individual's personal information;
(b) contravene an information protection principle under the *Privacy and Personal Information Protection Act 1998* or a Health Privacy Principle under the *Health Records and Information Privacy Act 2002*;
(c) prejudice any court proceedings by revealing matter prepared for the purposes of or in relation to current or future proceedings;
(d) prejudice the fair trial of any person, the impartial adjudication of any case or a person's right to procedural fairness;
(e) reveal false or unsubstantiated allegations about a person that are defamatory;
(f) expose a person to a risk of harm or of serious harassment or serious intimidation; or
(g) in the case of the disclosure of personal information about a child – the disclosure of information that it would not be in the best interests of the child to have disclosed.

4 Business interests of agencies and other persons

There is a public interest consideration against disclosure of information if disclosure of the information could reasonably be expected to have one or more of the following effects:

(a) undermine competitive neutrality in connection with any functions of an agency in respect of which it competes with any person or otherwise place an agency at a competitive advantage or disadvantage in any market;
(b) reveal commercial-in-confidence provisions of a government contract;
(c) diminish the competitive commercial value of any information to any person;
(d) prejudice any person's legitimate business, commercial, professional or financial interests; or
(e) prejudice the conduct, effectiveness or integrity of any research by revealing its purpose, conduct or results (whether or not commenced and whether or not completed).

5 Environment, culture, economy and general matters

There is a public interest consideration against disclosure of information if disclosure of the information could reasonably be expected to have one or more of the following effects:

(a) endanger, or prejudice any system or procedure for protecting, the environment;

(b) prejudice the conservation of any place or object of natural, cultural or heritage value, or reveal any information relating to Aboriginal or Torres Strait Islander traditional knowledge,

(c) endanger, or prejudice any system or procedure for protecting, the life, health or safety of any animal or other living thing, or threaten the existence of any species;

(d) damage, or prejudice the ability of the Government or an agency to manage, the economy; or

(e) expose any person to an unfair advantage or disadvantage as a result of the premature disclosure of information concerning any proposed action or inaction of the Government or an agency.

6 Secrecy provisions

(1) There is a public interest consideration against disclosure of information if disclosure of the information by any person could (disregarding the operation of this Act) reasonably be expected to constitute a contravention of a provision of any other Act or statutory rule (of this or another State or of the Commonwealth) that prohibits the disclosure of information, whether or not the prohibition is subject to specified qualifications or exceptions.

(2) The public interest consideration under this clause extends to consideration of the policy that underlies the prohibition against disclosure.

7 Exempt documents under interstate Freedom of Information legislation

(1) There is a public interest consideration against disclosure of information communicated to the Government of New South Wales by the Government of the Commonwealth or of another State if notice has been received from that Government that the information is exempt matter within the meaning of a corresponding law of the Commonwealth or that other State.

(2) The public interest consideration under this clause extends to consideration of the policy that underlies the exemption.

(3) In this clause, a reference to a corresponding law is a reference to:

(a) the *Freedom of Information Act 1982* of the Commonwealth; or

(b) a law of any other State that is prescribed by the regulations as a corresponding law for the purposes of this clause.

Appendix 6 – Application to amend personal information

Please complete this form to apply for amendment of personal information held by the University of Sydney about you under s.15 of the *NSW Privacy and Personal Information Protection Act 1998*. If you need help in filling out this form, please contact the Privacy Officer on (02) 9351 4263 or visit our website at www.sydney.edu.au/arms/privacy

Your details

Surname: ..... **Title**: Mr/Ms/Dr/Prof

Other names: .....

Postal address: ..... **Postcode**: .....

Daytime telephone: ..... **Facsimile**: .....

Email: .....

Information sought to be amended

Please describe the personal information about you that you would like to amend in enough detail to allow us to identify it and provide the reasons that you consider it to be incomplete, incorrect, out-of-date, or misleading. Please provide the information you consider necessary in support of your application. Additional pages may be used and supporting any documents should be attached.

.....

.....

.....

.....

.....

.....

.....

.....

Applicant's signature: .....

Date: .....

There is no fee for applications to amend records.

Post this form to: The Privacy Officer, ARMS, A14, University of Sydney, NSW 2006 Australia

The supply of the information is voluntary, but if you do not provide all the information requested, the University may not be able to process your request. The information on this form will be used by the University's Privacy staff and will not be disclosed outside the University without your express consent except where required or authorised by law. Any enquiries regarding access to, or correction of, personal information about you held by the University should be addressed to the Privacy officers at the above address.

Appendix 7 – Application for review of conduct under section 53 of the *Privacy and Personal Information Protection Act 1998*

Use this form if you wish to make a privacy complaint to the University of Sydney.

If you need help in filling out this form, please contact the Privacy Officer on (02) 9351 4263 or visit our website at www.sydney.edu.au/arms/privacy

Your details

Surname: ..... Title: Mr/Ms/Dr/Prof

Other names: .....

Postal address: ..... Postcode: .....

Daytime telephone: ..... Facsimile: .....

Email: .....

Details of the complaint (Use continuation sheets if necessary)

What is the conduct complained of?

.....
.....
.....
.....
.....
.....
.....
.....
.....

When did the conduct you are complaining about occur? (Use dates if possible)

.....
.....
.....
.....
.....
.....
.....
.....

When did you become aware of this conduct?

.....
.....
.....
.....
.....
.....
.....
.....
.....
.....

What effect did the conduct have on you or another person?

……
……
……
……
……
……
……
……
……
……

What would you like to see the University do about the conduct?

……
……
……
……
……
……
……
……
……
……
……

Declaration and signature

I understand that details of my application for review will be referred to the Privacy Commissioner in accordance with section 54(1) of the *NSW Privacy and Personal Information Protection Act 1998* and that the Privacy Commissioner will be kept advised of the progress of the review.

Applicant's signature: .....Date: .....

There is no fee for applications for personal information.

Please post this form to: The Privacy Officer
Archives and Records Management Services
A14
University of Sydney 2006

Office use only

Date received:.....

File reference:.....

The supply of the information is voluntary, but if you do not provide all the information requested, the University may not be able to process your request. The information on this form will be used by the University's Privacy staff and will not be disclosed outside the University without your express consent except where required or authorised by law. Any enquiries regarding access to, or correction of, personal information about you held by the University should be addressed to the Privacy officers at the above address.

Appendix 8 – Draft letter to the Privacy Commissioner regarding receipt of application for internal review under section 53

(University letterhead)

File number:

Date

Dr Elizabeth Coombs
NSW Privacy Commissioner
GPO Box 7011
Sydney NSW 2001

Dear Dr Coombs,

Notification in accordance with s. 54(1) of the NSW Privacy and Personal Information Protection Act of 1998.

The University has received an application for Internal Review under s. 53 of the *Privacy and Personal Information Protection Act 1998*. A copy of the letter of application is attached.

The matter is being investigated. I shall keep you informed of the progress and outcome of the review.

Should you have any submissions regarding this matter, please send them to me at the above address.

Yours sincerely,

Privacy Officer

Appendix 9 – Internal Review Checklist

office of the privacy commissioner
new south wales

OFFICE OF THE PRIVACY COMMISSIONER – COMPLAINTS TO PUBLIC SECTOR AGENCIES

The *NSW Privacy and Personal Information Protection Act 1998* (the PPIP Act) and the *NSW Health Records and Information Privacy Act 2002* (the HRIP Act) provide that public sector agencies deal with complaints by way of internal review. This process is the same under both Acts, although you will be assessing the alleged conduct against different standards (the IPPs and the HPPs).

A privacy complaint may come under:

- **the PPIP Act, section 53, if it relates to personal information, and the Information Protection Principles (IPPs); or**
- **the HRIP Act, section 21, if it relates to health information and the Health Privacy Principles (HPPs).**

	Steps to follow	Date completed
	Preliminary steps	
1	**Is the complaint about a person's *personal information*?** ☐ **Yes – You should treat their complaint as a request for internal review. Go to Q.2.** ☐ **No – Follow your agency's normal complaint handling procedures.**	
2	**Is the complaint about a person's *health information*?** ☐ **Yes – You should treat their complaint as a request for Internal Review under the HRIP Act. This means that the HPPs and other standards under the HRIP Act will apply.** ☐ **No – You should treat their complaint as a request for Internal Review under the PPIP Act. This means that the IPPs and other standards under the PPIP Act will apply.** ☐ **Both – See the notes below.**	
3	**According to the complainant, when did the alleged conduct occur?**	
4	**Is the complaint about conduct that occurred after 1 July 2000?** ☐ **Yes – Go to Q.5.** ☐ **No – The PPIP Act does not apply. Follow your agency's normal complaint handling procedures.**	

5	**Is the complaint about health information and conduct that occurred after 1 September 2004?** ☐ **Yes – the HRIP Act covers this complaint.** ☐ **No – the PPIP Act covers this complaint.**	
6	**According to the complainant, when did they first *become aware of* the alleged conduct?**	
7	**When was this application / privacy complaint first lodged?**	
8	**If more than six months lapsed between the date at Q.6 and the date at Q.7, your agency must decide whether you will accept a late application.** Will you accept this late application? ☐ **Yes – Go to Q.9.** ☐ **No – Explain your reasons as to why you are unable to accept this older than 6 months complaint to the complainant, then follow your agency's normal complaint handling procedures.**	
9	**When will 60 days elapse from the date at Q.7?** After this date the complainant may go to the Administrative Decisions Tribunal (the "Tribunal") without waiting for the results of this review.	
10	**For complaints about a person's** health information **go to Q.11.** **For complaints about a person's** personal information, **not including health information, tick all of the following types of *conduct* that describe the complaint, and then go to Q.12.** ☐ collection of the complainant's personal information (IPPs 1–4) ☐ security or storage of the complainant's personal information (IPP 5) ☐ refusal to let the complainant access or find out about their own personal information(IPPs 6–7) ☐ accuracy or relevance of the complainant's personal information (IPPs 8–9) ☐ use of the complainant's personal information (IPP 10) ☐ disclosure of the complainant's personal information (IPPs 11–12, and/or the public register provisions in Part 6 of the Act) ☐ other /it's not clear	
11	**For complaints about a person's** health information**, tick all of the following types of *conduct* which describe the complaint:** ☐ collection of the complainant's health information (HPPs 1–4) ☐ security or storage of the complainant's health information (HPP 5) ☐ refusal to let the complainant access or find out about their own health information (HPPs 6–7)	

	☐ accuracy or relevance of the complainant's health information (HPPs 8–9) ☐ use of the complainant's health information (HPP 10) ☐ disclosure of the complainant's health information (HPP 11) ☐ assignment of identifiers to the complainant (HPP 12) ☐ refusal to let the complainant remain anonymous when entering into a transaction with your agency (HPP 13) ☐ transfer of the complainant's health information outside New South Wales (HPP 14) ☐ including the complainant's health information in a health records linkage system (HPP 15) ☐ other /it's not clear		
12	**Appoint a reviewing officer.** *(The reviewing officer must be someone who was not substantially involved in any matter relating to the conduct complained about. For other requirements see s.53(4) of the PPIP Act. This also applies to the HRIP Act.)* Insert the reviewing officer's name here:		
13	**Write to the complainant, stating:** ☐ your understanding of the conduct complained about; ☐ your understanding of the privacy principle/s at issue (either IPPs at Q.10 or HPPs at Q.11); ☐ that the agency is conducting an Internal Review under the PPIP Act or the HRIP Act, as appropriate; ☐ the name, title, and contact details of the reviewing officer; ☐ how the reviewing officer is independent of the person/s responsible for the alleged conduct; ☐ the estimated completion date for the review process; ☐ that if your review is not complete by the date at Q.9, the complainant can go to the Tribunal for an external review of the alleged conduct; and ☐ that a copy of this letter will be provided to the NSW Privacy Commissioner for their oversight role.		
14	**Send a copy of your letter at Q.13 to the NSW Privacy Commissioner, GPO Box 7011, SYDNEY NSW 2001; or fax (02) 8114 3755; or email privacyinfo@privacy.nsw.gov.au** Include a copy of the complainant's application – either the written request or the information provided on the *Privacy Complaint: Internal Review Application Form*.		
	Now you can start the review itself		
15	**<u>Under the PPIP Act</u>** You need to determine: ☐ whether the alleged conduct occurred; ☐ if so, whether the conduct complied with all the IPPs (and Part 6 public register provisions if applicable); and	**<u>Under the HRIP Act</u>** You need to determine: ☐ whether the alleged conduct occurred; ☐ if so, whether the conduct complied with all the HPPs; and ☐ if the conduct did not comply with an	

	☐ if the conduct did not comply with an IPP (or the public register provisions), whether the non-compliance was authorised by an exemption under the PPIP Act; a Privacy Code of Practice; or a s.41 Direction from the Privacy Commissioner.	HPP, whether the non-compliance was authorised by an exemption under the HRIP Act; a Health Privacy Code of Practice; or a s.62 Direction from the Privacy Commissioner.	
16	**Four weeks after sending the letter at Q.13, send a progress report to the complainant and the Privacy Commissioner. Include:** ☐ details of progress of the review; ☐ if there are delays, an explanation of this and a revised estimated completion date for the review process; and ☐ a reminder that if the review is not complete by the date at Q.9, the complainant can go to the Tribunal for an external review of the alleged conduct.		

	On completion of the review		
17	**<u>Under the PPIP Act</u>** Write up your findings about the facts, the law, and your interpretation of the law. Set out your preliminary determination about: ☐ whether there was sufficient evidence to establish that the alleged conduct occurred; ☐ which of the IPPs (and/or the public register provisions) you examined and why; ☐ whether the conduct complied with the IPPs/ public register provisions; ☐ if the conduct did not comply with an IPP or public register provision, whether the non-compliance was authorised by an exemption under the PPIP Act; a Privacy Code of Practice; or a s.41 Direction from the Privacy Commissioner; and ☐ an appropriate action for the agency by way of response/ remedy.	**<u>Under the HRIP Act</u>** Write up your findings about the facts, the law, and your interpretation of the law. Set out your preliminary determination about: ☐ whether there was sufficient evidence to establish that the alleged conduct occurred; ☐ which of the HPPs you examined and why; ☐ whether the conduct complied with the HPPs; ☐ if the conduct did not comply with an HPP, whether the non-compliance was authorised by; an exemption under the HRIP Act; a Health Privacy Code of Practice; or a s.62 Direction from the Privacy Commissioner; and ☐ an appropriate action for the agency by way of response/ remedy.	
18	**Before completing the review, check whether the Privacy Commissioner wishes to make a submission. Ideally you should provide a draft copy of your preliminary determination to the Privacy Commissioner for comment.**		
19	**<u>Under the PPIP Act</u>** Finalise your determination of the internal review, by making one of the following **findings**: ☐ insufficient evidence to suggest alleged conduct occurred	**<u>Under the HRIP Act</u>** Finalise your determination of the internal review, by making one of the following **findings**: ☐ insufficient evidence to suggest alleged conduct occurred	

	☐ alleged conduct occurred but complied with the IPPs/ public register provisions ☐ alleged conduct occurred; did not comply with the IPPs/ public register provisions; but non-compliance was authorised by an exemption, Code or s.41 Direction ☐ alleged conduct occurred; the conduct did not comply with the IPPs/ public register provisions; the non-compliance was not authorised **(a "breach")**	☐ alleged conduct occurred but complied with the HPPs ☐ alleged conduct occurred; did not comply with the HPPs; but non-compliance was authorised by an exemption, Code or s.62 Direction ☐ alleged conduct occurred; the conduct did not comply with the HPPs; the non-compliance was not authorised **(a "breach")**	
20	**Did the agency breach an IPP or public register provision?** ☐ **Yes – Go to Q.22** ☐ **No – Go to Q.21**	**Did the agency breach an HPP?** ☐ **Yes – Go to Q.22** ☐ **No – Go to Q.21**	
21	**Even though the agency did not breach any IPP, public register provision or HPP, have you identified any need for improvement in policies, procedures, communicating with your clients, etc.?** ☐ **Yes – Go to Q.22** ☐ **No – Go to Q.24**		
22	**What action is proposed by the agency as a result of this review?** ***(You can have more than one.)*** ☐ apology to complainant ☐ rectification to complainant, for example.: ☐ access to their personal information or health information; ☐ correction of their personal information or health information; ☐ other type of rectification; ☐ expenses paid to complainant; ☐ compensatory damages paid to complainant; ☐ other remedy to complainant; ☐ review of policies, practices or systems; ☐ change in policies, practices or systems; ☐ training (or further training) for staff; ☐ other action; or ☐ no action.		
23	**Is the proposed action likely to match the expectations of the complainant?** ☐ **Yes** ☐ **No**		

	☐ **Unsure**		
24	**<u>Under the PPIP Act</u>** Notify the complainant and the Privacy Commissioner in writing: ☐ that you have completed the internal review; ☐ what your **findings** are, i.e. which one of the following: ☐ insufficient evidence to suggest alleged conduct occurred; ☐ alleged conduct occurred but complied with the IPPs/ public register provisions; ☐ alleged conduct occurred; did not comply with the IPPs/ public register provisions; but non-compliance authorised by an exemption, Code or s.41 Direction; ☐ alleged conduct occurred; the conduct did not comply with the IPPs/ public register provisions; the non-compliance was not authorised **(a "breach")**; ☐ what the **reasons** for your findings are; ☐ a plain English explanation of the **law** behind your findings, including quoting in full the relevant legislative provisions you are talking about; ☐ what action(s) you are going to take as a result; ☐ that the complainant has the right to apply to the Tribunal for a review of the conduct complained about; and ☐ the contact details for the Tribunal.	**<u>Under the HRIP Act</u>** Notify the complainant and the Privacy Commissioner in writing: ☐ that you have completed the internal review; ☐ what your **findings** are, i.e. which one of the following: ☐ insufficient evidence to suggest alleged conduct occurred; ☐ alleged conduct occurred but complied with the HPPs; ☐ alleged conduct occurred; did not comply with the HPPs; but non-compliance authorised by an exemption, Code, or s.62 Direction; ☐ alleged conduct occurred; the conduct did not comply with the HPPs; the non-compliance was not authorised **(a "breach")**; ☐ what the **reasons** for your findings are; ☐ a plain English explanation of the **law** behind your findings, including quoting in full the relevant legislative provisions you are talking about; ☐ what action/s you are going to take as a result; ☐ that the complainant has the right to apply to the Tribunal for a review of the conduct complained about; and ☐ the contact details for the Tribunal.	
25	**Keep a record of this review for your annual reporting requirements.**		

Index

NB – Index does not cover the appendices.