Privacy Management Plan

Abstract

The Privacy Management Plan outlines how UTS will protect personal and health information, implement the principles outlined in the Privacy Vice-Chancellor's Directive and comply with privacy legislation.

Dates	Plan approved 29/05/2015 Plan takes effect 24/06/2015 Plan is due for review (up to two years) 05/2017
Approved by	Vice-Chancellor
Implementation Officer	Director, Governance Support Unit
Relevant to	All individuals, including staff, students and members of the public (see also section 2)
Related documents	Privacy Vice-Chancellor's Directive Privacy Impact Assessment Tool (.docm) (staff only) Records Management Vice-Chancellor's Directive Handling Student Complaints Policy Handling Staff Grievances Vice-Chancellor's Directive Fraud and Corruption Prevention and Public Interest Disclosures Policy Code of Conduct Acceptable Use of Information Technology Facilities Policy Information Technology Security Vice-Chancellor's Directive UTS Information Guide **External documents** General retention and disposal authorities, State Records NSW HRIPA statutory guidelines, Information and Privacy Commission NSW Annual Reports (Departments) Regulation 2010 (NSW)

Legislation	Privacy and Personal Information Protection Act 1998 (NSW) (PPIPIA) Health Records and Information Privacy Act 2002 (NSW) (HRIPA) Privacy Act 1988 (Cwlth) Government Information (Public Access) Act 2009 (NSW) (GIPA Act) State Records Act 1998 (NSW) University of Technology, Sydney, Act 1989 (NSW) Workplace Surveillance Act 2005 (NSW)
File number	UR05/887
Superseded documents	Privacy Management Plan, 15 June 2000

Contents

1. Purpose

This Privacy Management Plan (the Plan) details how the University of Technology, Sydney will manage personal and health information it collects and holds to ensure compliance with obligations under both the Privacy and Personal Information Protection Act 1998 (NSW) (PPIPA) and Health Records Information Privacy Act (NSW) 2002 (HRIPA) (collectively referred to as the Privacy Acts). Although the Plan explains how UTS aims to meet the requirements of the Privacy Acts and the University's Privacy Vice-Chancellor's Directive, it cannot reference every situation that may arise.

The Commonwealth Privacy Act 1988 is not directly applicable to UTS. However, the University may be subject to some provisions of this Act in meeting legislative obligations specified in other Commonwealth acts (such as the Higher Education Support Act 2003), as well as in meeting standards and codes of practices in relation to the conduct of research.

This Plan has been developed and approved in compliance with section 33 of PPIPA. The Plan is available on the Privacy at UTS website at: http://www.uts.edu.au/sites/default/files/gsu-utsprivacymanagementplan.pdf.

A copy may also be obtained from the UTS Privacy Officer (see section 7.1).

2. Scope

This Plan applies to past, current and prospective staff, elected members, adjunct and honorary appointees, as well as contracted third parties of UTS.

The Plan provides the necessary practical guidance for effective privacy management at UTS and a breach of the Plan constitutes a breach of the Privacy Vice-Chancellor's Directive (the Directive).

The Plan does not cover independent bodies or controlled or related entities associated with UTS that are not under the direct control of the University, including but not limited to accessUTS Pty Limited, INSEARCH Limited, UTS Global Pty Ltd, Sydney Educational Broadcasting Ltd, UTS Child Care Inc., UTS Students Association and the UTS Union Ltd (ActivateUTS).

3. Definitions

The definitions outlined in section 3 of the Directive apply to the Plan. Additional definitions applicable to the Plan are outlined in Appendix 1.

4. Privacy management at UTS

This section covers how UTS will implement:

- the Information Privacy Principles (IPP1–11) in sections 8–19 of PPIPA
- the Health Privacy Principles (HPP1–15) under Schedule 1 of HRIPA, and
- the statements outlined in section 5 of the Directive.

Further guidance is also available on the Privacy at UTS website.

Unless specified otherwise, 'personal information' includes health information.

4.1 Collecting information

The following requirements covering information collection relate to information that is collected by UTS directly, on request or via automated means. The requirements under section 4.1 do not apply to unsolicited information received by UTS. The other sections of this Plan will still apply to unsolicited information.

This section guides the implementation of section 5.2 of the Directive.

4.1.1 Purpose of collection

In line with the Directive and IPP1 and HPP1, UTS may collect personal information for the following University functions:

- teaching and learning
- research
- managing staff, including recruitment, performance, remuneration, safety and wellbeing
- managing students, including enrolment, assessment and graduations
- engaging with potential staff and students, alumni and donors, community groups, other educational institutions, industry and government
- provision of services to staff and students, and
- administrative functions, such as receipt and payment of monies, and security and safety of property and individuals.

A variety of personal information is collected and held in support of these activities (see Appendix 2).

4.1.2 Sources of personal information collection

In line with the Directive and IPP2 and HPP3, collecting personal information directly from the individual it relates to assists in the receipt of appropriate consent and helps to ensure the accuracy of the information being collected. An individual can provide authority for a third party to act on their behalf in their dealings with UTS, which may include the collection or receipt of their personal information. The Third Party Authority form (PDF) enables individuals to provide this authority. Authority to act can also be provided through receipt of a letter or email. Appropriate proof of identity is required (see section 5.5.2).

There are activities of the University which require personal information to be collected from a third party. Where possible, consent should be included as part of the activity's process.

For example, where information is collected from:

- the Universities Admissions Centre (UAC) as part of a student's application process. Applicants provide the authority for UAC to liaise with UTS as part of their application process, which requires information to move between UTS and UAC to process an application.
- schools, hospitals or other organisations involved in supervising UTS students undertaking field work, practicums and professional experience programs. This is a requirement of the particular course and relevant consents are included in the enrolment process.
- other education providers for the purpose of verifying qualifications. UTS may verify where a prospective student or staff member has claimed qualifications or have indicated previous study.

- health care providers. Information may be collected about a client who was referred for medical tests from the UTS health services, or where a professional authority is required from a medical practitioner in support of a special consideration application.
- next of kin or a power of attorney in relation to a deceased individual (see section 4.7), or
- parents and legal guardians where an individual is under 16 years of age (see section 4.7).

Personal information may also be collected from third parties as part of formal investigations undertaken under a legislative requirement, or under the UTS Rules or Code of Conduct.

UTS collects information by automated means in some cases, such as:

- security cameras, which are used across all campus locations
- video recordings used for assessment purposes, such as assessing clinical practice (Faculty of Health) and moots (Faculty of Law)
- the UTS website, which records details about visits for quality improvement processes
- the UTS wireless internet (WiFi) service, which records login details of users
- audio, video or images taken of some lectures and events and from classroom sensors.

Information collected via automated means is collected from the individual through their participation in an activity or use of a system, etc. Where possible, the University will endeavour to ensure such automatic collections are open and transparent through relevant privacy notices, terms and conditions, or other methods of communication.

4.1.3 Openness and privacy notice specification

In line with the Directive and IPP3 and HPP4, a relevant privacy notice must be included when personal information is being collected. Not all activities are covered by one whole-of-University privacy notice. For example, there is a tailored privacy notice on the UTS website that covers information collected by virtue of someone browsing the web, which does not cover the collection of specific information via an online enrolment form. Similarly, the privacy elements in the UTS Student Declaration have specific purposes defined under the Declaration and do not cover all UTS activities involving use and disclosure of a student's personal information.

A relevant privacy notice needs to specify the following:

- who is collecting the information: for example UTS, the relevant business unit or where a collecting activity is outsourced. This needs to be clearly specified.
- why information is being collected and how it will be used. This may include primary purposes but should also include any known secondary purposes and, where possible, should indicate which areas of UTS may be receiving the information and for what purpose.
- whether it will be disclosed, to whom and why. This may include that information will not be disclosed or may specify where a disclosure is required.

- that the individual can access and correct personal information held about them, and
- whether the supply of the information is required by law or is voluntary, as well as any consequences for not providing the information being requested (if applicable).

The same details need to be provided when information is collected verbally or through an automated process.

4.1.4 Collecting relevant information only

In line with the Directive and IPP4 and HPP2, collection methods should be designed to ensure that only relevant and accurate information is received. This may be facilitated through use of automated fill-in boxes, validation of ID numbers and names, and mandatory fields where required.

Whether information is considered relevant and the level of detail required will depend on the defined primary and secondary purposes. For example:

- the level of personal information required relating to a staff member's application for sick leave will differ depending on whether they apply for one day leave, five days leave or whether the application is related to a workers compensation case.
- the level of detail required as part of a student request for special consideration may need to indicate how a particular condition affects a student's ability to undertake or complete a particular task, rather than specific details on the nature of the condition itself.
- if an individual's identity is not required as part of the information being collected, then it is preferable that names or other identifying information not be collected (such as statistical collection or general comments and feedback). However, it should be noted that elements collected separately may still enable an individual to be identified when matched together.

A privacy impact assessment (undertaken when initiating or changing a collection activity) will assist areas to ensure information collection is relevant and not excessive (see section 4.9).

4.2 Storage of personal and health information

In line with section 5.3 of the Directive and IPP5 and HPP5, the following statements apply to the storage of personal information.

4.2.1 Secure storage

Personal information is protected through a combination of practices. These include:

- various University-level governance instruments including the Privacy Vice-Chancellor's Directive and a number of instruments related to information technology
- local operational procedures in relation to the access, use and disclosure of personal information held by business units, covering what staff are permitted to do with personal information in their care
- the requirements of the Records Management Vice-Chancellor's Directive and Records Management Program, which includes the capture, accessibility, secure storage and destruction of records

- secure storage, transportation and destruction of paper and digital records, computers and portable devices
- protection of IT systems through design, and the implementation of access controls and passwords, security testing and monitoring
- appropriate assessment and contractual arrangements with third party providers which may be hosting systems or collecting and/or storing paper or data on behalf of UTS, and
- ensuring staff are trained in relation to their privacy obligations.

4.2.2 Storing personal information outside UTS

At times, UTS may need to store personal information outside the University, for example, when using an off-site commercial storage company to store paper records, engaging a third party to host and manage an information system or when storing data in the cloud.

The area of UTS responsible for such activities is required to complete a privacy impact assessment beforehand, to ensure the activity meets privacy obligations and community expectations (see section 4.9). For IT-related systems, this may also include undertaking an IT security risk assessment.

In addition, when engaging a third party, privacy obligations are to be included in contractual arrangements.

Refer also to the Information Technology Security Vice-Chancellor's Directive and the IT Security Standards for further information about security of IT systems.

4.2.3 System access

Protection of personal information held within information systems can be achieved through the application of access controls. Staff should only have access to information systems for legitimate purposes as required by their role at UTS. Where possible, access to information held within systems should be limited based on user roles and responsibilities and the type of information held. The appropriate business process owner should authorise staff to access systems holding information that the business process owner is responsible for.

4.2.4 Retaining and destroying personal information

Personal and health information will only be retained by UTS for as long as required to satisfy both the purpose for which it was collected and any legal retention obligations, such as minimum retention requirements defined in general retention and disposal authorities issued under the State Records Act 1998 (NSW).

Staff are required to follow the requirements of the Records Management Vice-Chancellor's Directive and the University's records destruction procedures, regardless of the records data format or storage media involved.

UTS provides secure destruction bins for the destruction of confidential material. Areas who deal with highly sensitive personal information are encouraged to use a document shredder.

Where personal information may be held on leased or owned IT equipment, all equipment must be reformatted before it is disposed of, to ensure the permanent deletion of all data. For other storage media types, such as DVDs or tapes, advice on appropriate destruction methods is provided by University Records.

Where it may be useful to have data over a longer timeframe, it may be de-identified rather than destroyed. In such cases, destruction of the identifying components must follow the University's records destruction procedures.

In the event that an individual requests their information be destroyed, it will only be destroyed in line with the requirements under this section.

4.3 Access and accuracy

4.3.1 Accessing information

In line with the Directive and IPP6 and HPP6, access rights and details of how information will be used are required to be included in privacy notices (see section 4.1.3). In addition, information about access rights should also be provided to an individual upon request.

4.3.2 Providing access

In line with the Directive and IPP7 and HPP7, the volume and nature of personal information being requested will often affect how long it takes to action a request to access that information. Negotiating appropriate timeframes and regular communication with individuals are essential to ensure requests are processed efficiently and expectations are managed.

The following systems and processes are in place to provide access to individuals about their personal information at UTS:

- For staff: access to personal details, pay, leave and staff development records is available online via the NEO HR and finance system. Further to this, staff can request access to other information in their personnel records by contacting Client Services in the Human Resources Unit.
- All access requests from past staff should be referred to the Human Resources Unit in the first instance.
- For students: access to personal details and study information is available online via My Student Admin and My Subject Admin (class timetables). Further to this, students can request access to other information in their student record by contacting a UTS Student Centre or the relevant faculty or unit.
- All access requests from past students should be referred to a UTS Student Centre in the first instance.
- For other individuals: initial requests to access information should be made through the relevant faculty or unit that they believe holds the information. The UTS Privacy Officer can also provide assistance in locating information.

Sufficient proof of identity will be required where an individual has requested action relating to their information (see section 5.5.2). Procedures for the certification of documents should also be referred to.

Where an individual wishes to access their medical records held by UTS (eg Health Services in Students Services Unit, or the Traditional Chinese Medicine Clinic), requests to access the records must be referred directly to the relevant area in the first instance. The Information and Privacy Commission NSW publishes a fact sheet on accessing your health information in NSW (PDF).

Further avenues that can be used to access personal information include:

- an application under PPIPA or HRIPA, directed to the UTS Privacy Officer, or

- an access application under the Government Information (Public Access) Act 2009 (NSW) (the GIPA Act). Note: this avenue cannot be used to correct information. See Right to Information (GIPA) for further information about accessing information under the GIPA Act.

A request to access information may be refused by UTS in certain circumstances. In cases where access to information is refused, the decision to withhold access and justification for the decision, as well as any appeal rights, must be provided to the individual in writing and captured on an official file. Examples of where access may be refused include where:

- access would disclosure another individual's personal information. Where another individuals' information is included, attempts to remove the other information should first be made before access is either provided or denied.
- documents holding the information are subject to legal professional privilege
- it is determined that access would pose a serious threat to the life or health of any individual
- access is not permitted by any law or court order
- access would prejudice law enforcement activities, or
- access would prejudice existing or pending investigations and dispute resolution proceedings.

Fees can only be charged where original documents (such as transcripts, testamurs or statement letters of course completion or enrolment) are requested to be produced. Fees may also be charged where access is requested to health information. Any fees charged must be reasonable in the circumstances.

Fees will also be charged for applications made under the GIPA Act.

4.3.3 Correcting information

In line with the Directive and IPP8 and HPP8, inaccurate information is required to be updated where necessary and where it is possible to do so. In some cases, evidence of the required change may be requested, for example, to apply name changes or changes to date of birth.

Individuals can correct information held about themselves or request information be corrected through the accessing information processes outlined in section 4.3.2.

A request to correct information may be refused by UTS in certain circumstances. In cases where a request to correct information is refused, the decision not to correct information and justification for the decision, as well as any appeal rights, must be provided to the individual in writing and captured on an official file. In addition, the notation about the requested change or viewpoint of the individual must be recorded on an official file or in a relevant information system (in such a way that the notation can be read with the information concerned).

Examples of where a request to correct information may be refused include where:

- the change cannot be facilitated due to system design
- the change conflicts with legislation or the law or with University governance or recordkeeping requirements
- the question of accuracy is contentious (for example, where the information is a University business decision and is not deemed inaccurate by UTS).

4.4 Using personal information

4.4.1 Accuracy

In line with the Directive IPP9 and HPP9, action taken to ensure information is accurate before it is used will depend on the information in question. Where practical, multiple separate sources of the same information will be limited in favour of having one authoritative source that can be maintained. In addition, certain types of information are required to be maintained and updated by individual's themselves, such as staff and student contact details (see section 4.3.2).

4.4.2 Limits on using personal information

While the Directive requires that personal information can only be used for the primary purpose for which it was collected, a directly related purpose or where consent has been received (in line with IPP10 and HPP10), exemptions to these principles may apply. For example, where:

- the use is necessary as part of a formal investigation
- the use is required or permitted by law, or
- the use is considered necessary in an emergency situation.

The use of information should be determined before the collection process commences, however, in some cases a new use for previously collected information may be identified after the collection process has begun. Using personal information collected in the past for a new purpose requires consent, unless the additional use is covered by the above exemptions.

Surveillance information can only be used in accordance with the Workplace Surveillance Act 2005 (NSW), where surveillance is open and staff have been informed of the existence of surveillance, or by court order.

In the event that an individual withdraws consent for their information to be used, the University will take reasonable steps in the circumstances to comply with the request. Action taken will depend on the context of the request; for example, it would not be possible for the University to stop using an enrolled student's contact details for sending communications that are required by law.

4.5 Disclosing personal information

4.5.1 Limits on disclosing information

While the Directive provides specific limits on the disclosure of personal information (in line with IPP11 and HPP12), exemptions to these principles may apply. For example, where:

- an individual provides separate consent for their information to be disclosed. For example, where an individual authorises another individual to act on their behalf in dealing with the University. The Third Party Authority form (PDF) is available to facilitate consent in these circumstances. Authority to act can also be provided through receipt of a letter or email.
- the individual should be aware that such personal information is usually disclosed to the particular third party. For example, where Centrelink needs to confirm study details of students who have applied for FEE-HELP. In such cases, students acknowledge that Centrelink will require information from UTS in their application.

- the information is required by a third party who is undertaking a function on behalf of UTS, and where the third party is bound by the same privacy obligations. For example, where an IT company is contracted to provide support for a business system that holds personal information. The company may need access to system contents to facilitate system maintenance. However, where practical, access to actual data should be restricted.
- it is necessary in an emergency situation. For example, information may be provided to the police if necessary to protect the life or health of an individual.
- it is necessary for UTS to manage a formal internal investigation, litigation or insurance matter. For example, information may need to be disclosed where necessary to undertake an internal review under PPIPA.
- it is required or permitted to be disclosed by law. For example, where information is required to be released to government bodies, such as the Australian Taxation Office, federal education or immigration departments and Centrelink, for the purposes of those agencies undertaking their functions under their respective Acts. In some cases, disclosure is required by law, such as mandatory reporting obligations under the Health Practitioners Regulation National Law Act 2009 (NSW). See also the University's Course Related Work Experience: Procedures for Reporting Obligations to the Australian Health Practitioner Regulation Agency (AHPRA).

  Where disclosure of information under legislation is regular and routine, it should be included in relevant privacy notices, even if the disclosure is permitted by law.
- it is requested by a valid subpoena, warrant or court order. In such cases, the validity of requests, and the actioning of them, will be undertaken by UTS Legal Services.
- it is required for a legitimate law enforcement purpose, and the request to access information is covered by the investigation or law enforcement exemptions under the NSW privacy acts.

Staff need to document where information has been disclosed beyond its primary purposes, including under any of the above exemptions, and capture it on an official file.

4.5.2 Disclosing sensitive personal information

UTS is required to protect sensitive personal information. The provisions for the protection of this information are outlined in the Directive.

4.5.3 Verification and authenticity of UTS-issued documentation

UTS will confirm the existence of a qualification or the authenticity of an academic transcript, testamur or certificate provided by UTS or one of its antecedent institutions. This process is a matter of public interest and is considered vital to protect the value and integrity of the qualifications issued by UTS and its antecedent institutions.

Verifications can be undertaken via the online Qualifications Verification Service, which requires the requesting person to know the student name, student number and level of the qualification being verified. Requests can also be submitted via the Ask UTS website as not all qualifications can be verified through the Qualifications Verification Service.

As the information being verified is considered to be already held by the party undertaking the verification, no additional information will be released as part of this process without the student's consent unless it is covered by a disclosure exemption.

4.5.4 Limits on public access to personal information held in archival records

Official records of UTS that still exist after 30 years are considered to be open to the public under the State Records Act 1998 (NSW). UTS will issue access directions under the State Records Act to limit access to records and the disclosure of personal information where appropriate.

4.6 Additional requirements for managing health information

4.6.1 Secondary purposes for the use and disclosure of health information

UTS may use or disclose health information where it is deemed necessary for:

- the management of health services and for research which is approved by a human ethics committee, or
- training purposes, which requires signed privacy agreements.

These additional purposes are governed by the HRIPA statutory guidelines issued by the Privacy Commissioner.

UTS may use genetic information, or disclose it to a genetic relative of an individual the information relates to, without the individual's consent in situations where it is considered necessary to lessen or a prevent serious threat to the life, health or safety of the genetic relative or in accordance with the NSW Genetic Health Guidelines issued by the NSW Privacy Commissioner.

4.6.2 Using codes to identify an individual's health information

In line with the Directive and HPP12, unique identifiers, such as ID numbers, may be used to further enhance an individual's privacy. Although external identifiers, such as Medicare numbers, may be recorded where required, they will not to be adopted for this purpose. Any identifiers used by UTS must also be generated by UTS.

4.6.3 Anonymous health services

While UTS does not provide anonymous services to clients, as it is deemed impractical in the context of the health services available, discretion may be exercised on a case-by-case basis. This is in line with both the Directive and HPP13.

4.6.4 Transferring health information outside New South Wales (NSW)

In line with the Directive and HPP14, a requirement may arise for health information to be transferred outside NSW.

UTS has staff and students who come from outside NSW, including visiting academics and international students. UTS may be requested by an individual to provide a copy of their health information to them or a specified health care professional outside NSW. UTS would normally transfer health information outside NSW in response to such requests after receiving appropriate consent from the individual or where the transfer is in line with the Directive's requirements.

4.6.5 Participating in health records linkage systems

Clients of UTS health services are required to sign an information release form and provide the required identification documents before their health information is included in a computerised system that will link their information with records from other organisations for the purpose of facilitating access to those health records. This is in line with both the Directive and HPP15.

4.7 Third party interaction of behalf of an individual

Where an exemption does not already exist, consent is required from an individual to authorise UTS to deal with a third party in the management of their personal information. The Third Party Authority form (PDF) is available to facilitate consent in these circumstances.

4.7.1 Personal information of deceased individuals

For deceased individuals, the authority to provide consent lies with that individual's power of attorney or next of kin where nominated as part of the student or staff record.

4.7.2 Personal information of minors

Where the individual concerned is under 16 years of age, UTS may deal with an individual's parent or legal guardian in relation to the collection of personal information from minors or to obtain consent.

Disclosure of information about a minor under the age of 18 years to a parent or guardian will only be permitted where it is considered in the best interests of the minor in the circumstances.

In relation to health information in medical records of the UTS Health Service, consultation with a parent or legal guardian will be determined on a case-by-case basis, and will depend on the nature of the medical issues involved and the maturity of the individual. This will be a decision of the medical practitioner concerned in consultation with the Practice Manager.

4.8 Exemptions to privacy principles

4.8.1 Exemptions under legislation

There are exemptions to the IPPs and HPPs in the NSW privacy acts. UTS may also be exempt from privacy principles where an action is permitted or required under another law. Some examples of where these are relevant to the activities of UTS are covered in section 4 of this Plan. UTS will only rely on exemptions to privacy principles where appropriate in the circumstances and in consideration of an individual's privacy and expectations.

4.8.2 Public interest directions

The NSW Privacy Commissioner may make a public interest direction to modify the application of a privacy principle. The Information and Privacy Commission NSW publishes current public interest directions issued by the Commissioner.

4.8.3 Public registers

UTS does not hold any formal public registers that are applicable under the NSW privacy acts.

4.9 Privacy impact assessments

A privacy impact assessment is required when proposed new activity or change to an existing activity or process is likely to affect an individual's privacy or involve personal or health information. Examples of changes that can affect privacy include changing the collection of information from a paper to a digital form or changing how information is stored or used.

An assessment will review the new or changed activity or process against the relevant IPPs and HPPs specified in the privacy acts and defined in section 4 of this Plan. The Australian Privacy Principles (APPs) in Schedule 1 of the Commonwealth

Privacy Act may also need to be considered if an activity is governed by Commonwealth legislation that refers to compliance with the APPs.

An assessment tool is available to assist areas to undertake the assessment process. Approval to undertake an activity sits with the business unit head, or a committee or board, as appropriate in the circumstances. However, consultation with different areas of UTS (such as UTS Legal Services, Information Technology Division (ITD), University Records or the UTS Privacy Officer) may also be required at various stages of an assessment, to ensure the right advice is received and that all relevant information has been considered. For example, where the activity in question is an IT system, an IT security risk assessment will also be required.

In certain circumstances, an external privacy expert may be engaged to undertake a privacy impact assessment. This may be an option for projects that deal with large volumes of personal information where the risk of a privacy failure could be high. External experts should also be consulted where an independent review is required.

5. Education, training and communication

5.1 UTS governance instruments

The Privacy Vice-Chancellor's Directive is the primary UTS governance instrument covering privacy obligations. Other governance instruments that facilitate or relate to privacy are included in the related documents list at the beginning of this Plan.

5.2 Orientation and induction

Staff responsibilities in relation to privacy are incorporated into the legal and ethical obligations section of the UTS staff induction program. The requirement for new staff to undertake privacy training is specified on the staff orientation checklist.

Supervisors are responsible for ensuring staff under their supervision, including contractors and casual staff, are informed of their privacy responsibilities and undertake the appropriate training where possible.

5.3 Training

The privacy training program provides privacy essentials training sessions targeted at all staff to inform them of their responsibilities. Customised sessions are also run on request for areas who deal with personal information on a regular basis.

Privacy requirements should be incorporated into relevant training programs for systems and processes where privacy issues may arise.

Staff can access privacy training options and book into training through the Online Learning Module in NEO or by contacting the UTS Privacy Officer.

5.4 Practical information for staff

Staff can access practical information about privacy-related matters at Privacy practices for staff on the Privacy at UTS website.

Privacy practices include guidance on how to collect, store, use and disclose personal and health information appropriately, and how it can be accessed or corrected. These privacy practices have been made public under section 23(a) of the GIPA Act.

5.5 Communicating with individuals

5.5.1 General information distributed to individuals

Information about how UTS deals with the personal and health information of students, staff and members of the public is covered within this Plan and also available at Your privacy at UTS on the Privacy at UTS website.

Your privacy at UTS includes information on accessing and correcting information, how UTS will deal with requests to access another individual's information, requirements to prove your identify when dealing with UTS, surveillance and how to make a privacy-related complaint. It also includes links to relevant policies and procedures.

UTS also communicates with individuals through its use of privacy notices on forms and at points where personal information is collected (see section 4.1.3 in this Plan for details about open collection).

5.5.2 Identity verification checks

When dealing with individuals about their personal information — whether verbally, in person or in writing — the individual's identity must be verified. This also applies for a third party given authority to act on an individual's behalf.

An individual's identity may be verified through one or more of the following:

- staff or student ID number and date of birth.
- use of student or staff official email accounts. Emails received from a current UTS student or staff email account or an alumni-issued email account are considered to be from the individual concerned. No additional identification is usually required when communicating through these UTS-provided email accounts. Under section 2.3 of the Student Rules, official communication between UTS and a student is to be via their official UTS student email account.
- photo identification, such as a current staff or student card, valid passport or driver's licence. For inquiries made in person, such identification may only need to be sighted. Written or emailed inquiries may require a copy to be provided. Communication via a non-UTS-provided email account will require an appropriate form of identification to be provided.

5.6 Reporting on privacy matters

UTS reports its activities in relation to privacy in the UTS Annual Report as required under section 6 of the Annual Reports (Departments) Regulation 2010 (NSW). This includes a brief statement on the University's activities, statistics relating to internal reviews and privacy complaints received by UTS, as well as any other relevant privacy issues.

Details of internal review requests are also reported to the NSW Privacy Commissioner (see section 6.1 in this Plan).

6. Complaints

This section should be read in conjunction with section 5.11 of the Directive. A breach of this Plan is also considered a breach of the Directive.

6.1 Making a complaint

If an individual believes that UTS has breached their privacy they should contact the business unit responsible for the conduct in question as soon as possible. In many cases, these matters can be dealt with quickly in an informal manner by the business unit concerned. Alternatively, an individual may contact the UTS Privacy Officer for assistance, in particular where they do not know which area to contact.

If an individual is not satisfied with action taken, and wishes to make a formal complaint about an alleged privacy breach under the privacy acts, they can apply to UTS for an internal review (see section 6.2).

An individual may also complain directly to the NSW Privacy Commissioner. The Information and Privacy Commission NSW publishes further information about making a complaint.

6.2 Internal reviews

6.2.1 Applying for an internal review of conduct

An individual who wishes to apply for an internal review must lodge their application within six months of when they first become aware of the conduct in question.

UTS is required to inform the NSW Privacy Commissioner of all internal review applications it receives and provide any correspondence between the applicant and UTS. As part of their application for an internal review, an individual can request that only the summary of the conduct in question and outcome of the review are provided to the Commissioner, as opposed to the whole of their application. The Commissioner has the opportunity to make a submission to UTS before an internal review is finalised.

See Complaints on the Privacy at UTS website for information about how to apply for an internal review and the Request for an Internal Review form.

The UTS Privacy Officer can provide further advice.

6.2.2 Internal review process

An internal review must be completed by UTS within 60 days of a valid application being received, unless an extension is negotiated with the applicant.

The Director, Governance Support Unit or, in their absence, the Deputy Vice-Chancellor (Corporate Services) will delegate an appropriate officer to undertake an internal review on the University's behalf. In most cases, this will be the UTS Privacy Officer unless there is a conflict of interest or the Privacy Officer is unavailable.

An internal review necessitates the investigation of the conduct in question. This will include discussion with key parties involved or identified in the application. In investigating the conduct in question, the internal review officer will consider:

- all relevant material submitted by the applicant
- information obtained through interviews with relevant individuals as appropriate
- information obtained from the University's information and recordkeeping systems
- UTS Rules, governance instruments or other relevant documents
- relevant case law and NSW Civil and Administrative Tribunal decisions, and
- any submission received from the NSW Privacy Commissioner.

Anyone consulted as part of an internal review is required to provide all information which is requested and cooperate with the internal review process.

The draft findings of an internal review will be submitted by the reviewing officer to the Director, Governance Support Unit or, in their absence, the Deputy Vice-Chancellor (Corporate Services), who will be responsible for finalising the review. This may include approving any resulting recommendations. An applicant will be advised of the findings of the review and the reasons for those findings within 14 days of the review being finalised.

An internal review will have one of the following outcomes:

- Where a breach of privacy is identified, UTS may offer a formal apology, take reasonable steps to ensure the conduct will not occur again and/or review current policies, procedures, systems and training, as appropriate. Actions taken may also depend on the desired outcome of the applicant.
- Where no breach of privacy is identified, no further action will be taken. However, depending on the circumstances of the complaint, additional training or a review of procedures may still be initiated internally to improve the management of privacy.

If an internal review is not completed on time or the applicant is not satisfied with the outcome, the applicant can lodge an application for an external review of the findings.

6.2.3 External reviews and appeal rights

If an applicant is not satisfied with the outcome or handling of an internal review, they can lodge an appeal with the Administrative and Equal Opportunity Division of the NSW Civil and Administrative Tribunal (NCAT).

An applicant who wishes to appeal an internal review finding must apply to the NCAT for a review within 28 calendar days of receiving notice about the decision.

Where an internal review is not completed within 60 days, the 28-day time limit to request an NCAT review starts from the later of following two dates:

- the date the applicant was notified of the outcome of the internal review, or
- the day on which the 60-day internal review time limit expires.

Further information on reviews of privacy-related conduct by the NCAT is available on the NCAT website under Privacy of personal information.

6.2.4 Complaints not related to privacy

The internal review process is designed to formally investigate and deal with complaints relating to alleged breaches of privacy. Complaints (or elements of a complaint) that do not relate to privacy will not be dealt with as part of an internal review. Individuals will need to refer such complaints to the appropriate area of the University for action in line with the Policy on Handing Student Complaints or the Handling Staff Grievances Vice-Chancellor's Directive, as appropriate.

6.3 Dealing with disclosures of personal information in error

Although processes are in place to protect information, situations may arise where information is mistakenly disclosed or accessed.

Where this has occurred, immediate action is required to prevent further unauthorised access and reduce the potential impact of the occurrence. The following actions are required as soon as practical in the circumstances:

- inform the UTS Privacy Officer of what has occurred, action taken to date and proposed action moving forward. The Privacy Officer may also be consulted in the first instance, to obtain advice on how to deal with a privacy-related issue.
- for information system breaches, inform the relevant information system owner, the Chief Information Officer (CIO) and the Deputy Vice-Chancellor (Corporate Services)
- for deliberate breaches, potential corrupt behaviour or breaches of contracts by third parties, inform the Deputy Vice-Chancellor (Corporate Services)
- where it is believed that the information disclosed may pose a risk to an individual, such as a physical or health risk or a financial risk (eg disclosure of credit card details), the individual may be informed of the disclosure of their information. This will be decided on a case-by-case basis by the Deputy-Vice Chancellor (Corporate Services).

6.4 Corrupt conduct and breaches

Breaches of this Plan (as identified through an informal complaint, internal review or through other means) will be managed in line with the statements outlined in section 5.11.4 of the Directive.

Individuals who deliberately breach privacy legislation may be personally liable for that action and attract legislative penalties under PPIPA or HRIPA.

A third party may be personally liable if they attempt to bribe or engage in other forms of corrupt behaviour to induce a current or past staff member to breach privacy principles under privacy legislation

7. Contacts

7.1 Internal contacts

Initial inquiries should be directed to the relevant faculty or unit holding the information.

Students who wish to inquire about information held about them centrally should contact their relevant UTS Student Centre in the first instance.

Staff can inquire about information held about them centrally by contacting the Human Resources Unit in the first instance.

UTS Privacy Officer
Other inquiries should be referred to the UTS Privacy Officer:
telephone: +61 2 9514 1245
fax: +61 2 9514 1232
email: privacy@uts.edu.au
website: Privacy at UTS

7.2 External contacts

Privacy Commissioner, Information and Privacy Commission NSW
telephone: 1800 472 679
fax: +61 2 8114 3756
email: ipcinfo@ipc.nsw.gov.au
postal address: GPO Box 7011, Sydney NSW 2001
website: ipc.nsw.gov.au

NSW Civil and Administrative Tribunal (NCAT)
telephone: 1300 006 228
website: ncat.nsw.gov.au

Appendix 1. Definitions

Relevant definitions can be found in section 3 the Privacy Vice-Chancellor Directive.

The following additional definitions are applicable to this Plan. This includes expanded definitions of personal information and health information.

Anonymous refers to a situation where an individual is not identified or identifiable as part of the provision of a service to them. Essentially this means that any information collected as part of the service is not considered personal or health information under the respective definitions.

De-identified information refers to information that no longer identifies the individual it relates to. Identifying information is more than an individual's name or ID number. It may be any data elements that, when put together, can be used to identify an individual.

Note: Where information held can readily be matched with other information to identify an individual, it may not be considered de-identified information.

De-identify refers to a process of removing information that would identify or reasonably enable an individual to be identified. Unlike collecting information that is considered anonymous, de-identifying information usually occurs after personal or health information is collected, and is usually done for a particular purpose.

Health information is information as defined under section 6 of HRIPA. In summary, health information is a subset of personal information, and refers to personal information that relates to an individual's health.

Health information not only relates to data about the health of research participants or information held in medical records, it also includes but is not limited to medical certificates, mental capacity, references to permanent or temporary disabilities, workers compensation processes or accident reports, sick leave management and arrangements that are a result of or relate to health issues that are put in place for staff as part of work planning or for students to facilitate successful course completion.

For the purposes of this Plan, the use of the term 'personal information' includes health information unless otherwise specified.

HPPs are Health Privacy Principles defined under Schedule 1 of HRIPA.

IPPs are Information Protection Principles defined under sections 8-19 of PPIPA.

Personal information is information as defined under section 4 of the PPIPA. In summary, personal information refers to information or an opinion of any person about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion, irrespective of whether the information is recorded in a material form or not, and including information or an opinion forming part of a database.

Personal information includes but is not limited to:

- information that is about a person, such as names, addresses, contact details, date of birth, marital status, financial information, gender, ethnicity, religious beliefs, photographs
- work performance, successful or unsuccessful applications, subject results
- information relating to personal activities or habits of an individual.

UTS has a responsibility to appropriately manage personal information where it is held by the University. Personal information is considered to be 'held' by the University if:

- the University is in possession or control of the information, or
- the information is in the possession or control of a person employed or engaged by the University in the course of such employment or engagement, including engagement in subject, course or research requirements, or
- the information is contained in an official record for which the University is responsible under the State Records Act 1998.

Information is not considered personal information where:

- the information relates to an individual who has been dead for more than 30 years
- the information is already available in a publically available publication, including non-UTS public websites, journals, books, etc., which are openly available
- the information directly relates to an individual's suitability for appointment or employment to a position in the public sector
- the individual cannot reasonably be identified by the information or data in question. This is commonly known as de-identified data. However, if the information can be readily linked to other identifying information, or the individual's identity can be determined by recipients of such information, it is viewed as personal information.
- the information relates to an organisation, not an individual. For example, the work contact details of an employee undertaking an activity on behalf of UTS, or a staff member signing a letter in their work capacity, is information relating to UTS, not personal information of that employee.

Note: in this Plan, the use of the term 'personal information' includes health information unless specified otherwise.

Surveillance is defined under section 3 of the Workplace Surveillance Act 2005. In summary, it refers to observations that may be made about an employee through the use of cameras, computer use, or other device which may have the ability to track location or movement information.

Surveillance information is defined under section 3 of the Workplace Surveillance Act 2005. In summary, it refers to information obtained, recorded, monitored or observed as a consequence of surveillance of an employee.

Appendix 2. Types of information collected and held

The following list provides an overview of the types of personal or health information collected and held by UTS in relation to its functions as specified under section 4.1.1 of this Plan.

Teaching and learning

- Comments and personal details provided in survey responses
- Assessments and coursework provided by students (see also managing students)
- International English Language Testing System (IELTS) applications, including photograph and finger scans required by Cambridge University and IELTS Australia

Research

- Personal or health information collected as part of research
- Personal information about researchers applying for research or grant funding

Managing staff (including recruitment, performance, remuneration, safety and wellbeing)

- Staff details, including but not limited to date of birth, photograph, contact details, address, emergency contact details, tax file declarations, banking details, contracts of employment, previous employment details, salary details, superannuation information, leave applications and approvals (and medical certificates where applicable), EEO information, training undertaken and results if applicable, information relating to eligibility to work in Australia
- Recruitment information relating to both successful and unsuccessful applicants, including contact details, applications, CVs, previous employment details, referee reports, skills assessments, security and working with children checks where applicable
- Workers compensation, accidents and injury-related information
- Information relating to grievances, complaints and misconduct
- Promotion records, including applications, CVs, qualifications, referee reports and references
- Performance planning, including work plans, probation plans and reports and performance reviews

Managing students (including enrolment, assessment, and graduations)

- Student details, including but not limited to photograph, contact details, address, date of birth, previous education, subjects, courses, qualifications attained, fee payment, bank details, fines and debt information if applicable, ethnicity, indigenous status, language, visa and immigration status, exchange details, and sponsorship details where applicable
- Information relating to applications for enrolment, leave, special consideration or admissions, withdrawals
- Assessment and examination records, including marks comments, final grades

- Supervision of students, including personal details and progress reports
- Information relating to grievances, complaints and misconduct
- Course, subject and timetable information in the context of it being linked to individuals
- Details of internships, clinical placements, practicum or professional experience and fieldwork, including evaluation, results and, where applicable, criminal history checks, evidence of vaccinations, working with children declarations
- Graduands, including names (and mailing address in some instances), faculty, course and qualification
- Applications and receipt of prizes, awards and scholarships
- Details of disabilities, Overseas Student Health Cover (OSHC) details, and medical history in some cases, where relevant

Engaging with potential staff and students, alumni and donors, community groups, other educational institutions, industry and government

- Alumni details, including contact details with graduates of UTS and antecedent institutions, photographs, details of who have attended events or taken up special offers
- Donors, including history, dates, amounts, conditions of gifts, contact details, philanthropic interests and details of their contact with the University
- Names, contact details of prospective students
- Names and professional contact of career advisers, principals and teachers, industry partners, professional bodies
- Attendee information for courses and events, including names, contact details, titles, position details, organisation's details, dietary and access requirements
- Personal and health information about summer school students

Provision of services to staff and students

- Medical records, including personal details, confidential health information in the provision of services, such as health or counselling services
- Personal information relevant to engagement with or requests for services, such as parking applications, career support, disability support, assistance with grievances, financial assistance, study support, support for Aboriginal and Torres Strait Islander students, housing and renting of student accommodation
- Information relating to library use, including contact information, photo identification, borrowing record, items currently on loan, fines

Administrative functions, such as receipt and payment of monies, security and safety of property and individuals

- Financial details, such as creditors, debtors and bank account details
- Security incident reports and CCTV footage
- Personal details of nominated, appointed and elected committee members
- Formal declarations required by Council and committee members

- Personal information relating to individuals requesting access to information
- Access logs and audit trails of staff and student activity in use of information technology
- Personal information relevant to warrants, court orders, subpoenas, contracts or other legal matters