UTS Privacy Management Plan

Policy context and introduction

The Privacy Management Plan (the plan) details the university's approach to and provides practical guidance on the protection and management of personal and health information.

This document has been developed to implement the principles and statements outlined in the Privacy Policy and the obligations under both the Privacy and Personal Information Protection Act 1998 (NSW) (PIPPA) and the Health Records and Information Privacy Act 2002 (NSW) (HRIPA) (collectively referred to as the privacy acts).

This plan has been developed in compliance with section 33, PPIPA and applies to all those within the scope of the Privacy Policy.

This plan also considers, where applicable, the requirements of the federal Privacy Act 1988 (Cwlth). While it is acknowledged that this act does not directly apply to UTS, the university may be subject to some of its provisions in meeting obligations outlined some contracts, standards and in other federal legislation (for example, the Higher Education Support Act 2003 (Cwlth).

Although this plan aims to detail how UTS will meet the requirements of the privacy acts, it cannot and does not reference every activity or situation that may arise.

This plan will be published on the privacy at UTS website.

Any queries should be sent to the UTS Privacy Officer.

Contents

1 Managing privacy at UTS

Section 1 covers the implementation of the Privacy Policy (the policy) and the requirements of:

- the information privacy principles (IPP) 1–12 in sections 8–19, PIPPA, and
- the health privacy principles (HPP) 1–15 under schedule 1, HRIPA.

Further guidance is available on the privacy at UTS website. Procedures for staff are available on the university's intranet (staff only).

Unless otherwise specified 'personal information' under this plan includes 'health information'. Both terms are defined by the policy.

This plan is approved by the Deputy Vice-Chancellor (Corporate Services) in line with the Privacy Policy.

Information that is not covered by this plan

Information is *not* considered personal information and is therefore not covered by the policy and this plan where:

- the information relates to an individual who has been dead for more than 30 years
- the information is already available in a publicly available publication, including non-UTS public websites, journals, books, etc., which are openly and freely available to the public.
- the individual cannot be identified by the information or data in question. This is commonly known as de-identified information. However, if the information can be re-identified by being linked to other information, it is viewed as personal information.
- the information relates to an organisation, not an individual. For example, the business contact details for 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.

1.1 Collecting personal information

The following requirements relate to how UTS collects personal information, either directly, indirectly or though automated processes.

The requirements outlined in this section do not apply to unsolicited information provided to UTS.

1.1.1 Purposes that information may be collected for

In line with the policy, IPP1 and HPP1, UTS may collect personal information where it is required for activities in support of the university's functions, including:

- teaching and learning
- research
- the management of staff (including recruitment, performance, development, remuneration, complaints and grievances, disciplinary matters, safety and wellbeing)
- the management of students (including enrolment, progression, assessment, complaints and grievances, disciplinary matters, conferral and graduations)
- community engagement (including with potential staff and students, alumni and donors, community groups, other educational institutions, industry and government)
- marketing of university courses and services and student recruitment
- provision of services, and

- administrative functions (including 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).

1.1.2 Collecting information directly from individuals

In line with the policy, IPP2 and HPP3, personal information will be collected directly from the individual unless an individual provides consent or the collection is required or permitted by law. This allows UTS to ensure that appropriate consent is provided and that information collected is accurate, up to date and complete.

1.1.3 Collection of information from a third party

Some of the university's activities and processes require personal information to be collected from a third party. Where this is required, privacy notices and collection of consent (where relevant) should be incorporated into those activities and processes. Information collected via a third party can include:

- Universities Admissions Centre (UAC). When individuals apply via UAC to study at UTS, UAC is approved by the applicant to liaise with UTS as part of the application process.
- schools, hospitals or other organisations where UTS students undertake field work, practicums and professional experience programs or internships related to their course. Students are advised that information will be shared with their placement provider first through the UTS Student Declaration (as part of enrolment processes), then as part of the placement process.
- other education providers. UTS will verify qualifications or certain details relating to previous study claimed by a prospective student, job applicant or current staff member. Individuals' are informed that information be verified.
- health care providers. This can occur where clients of UTS health services are referred to specialists or for medical tests or where a professional authority is required to support a student's special consideration application.
- contracted UTS security officers who may be required to record details of security incidents for the university's records
- nominated emergency contacts or an immediate family member in the event an individual cannot provide consent or be contacted
- next of kin or a power of attorney in relation to a deceased individual
- parents and legal guardians of a minor under 16 years of age.

Personal information may also be collected from third parties as part of investigations, appeals or other proceedings carried out under legislation, UTS Rules, UTS Code of Conduct, a university policy or other instruments.

1.1.4 Automated collection of personal information

UTS collects information by automated processes, including but not limited to:

- security cameras, which are in use across all campus locations
- video recordings, which are made and used for teaching and assessment purposes (such as assessing clinical practice and moots) or for staff training and development purposes
- capturing details about visits to the UTS website or intranet for quality improvement processes
- logging of details of users signing onto the UTS wireless internet (WiFi) service to facilitate that service, or logging the use of the university's information systems.
- logging attendance at lectures or events where audio, video or images are taken, and from classroom sensors.

UTS will endeavour to make automatic collection processes open and transparent by providing privacy notices, terms and conditions, user manuals, or by using other methods to communicate to individuals.

1.1.5 Privacy notices

In line with the policy, IPP3 and HPP4, a relevant privacy notice must be included when personal information is being collected. Not all activities can or should be covered by one whole-of-university privacy notice[1].

When and how to provide a privacy notice

A privacy notice must be provided to individuals before information is collected. If this is not possible, the privacy notice must be provided as soon as possible after the informing is collected.

A privacy notice may be provided in a variety of ways, including:

- on a form where personal information is being collected
- on a consent or other form
- on a web page
- in terms and conditions for an app, information system or service
- in a local privacy policy.

The method chosen to provide access to the privacy notice should be one that ensures it is readily accessible to the individuals' concerned.

Where privacy notice details are provided in conjunction with other rights and responsibilities, the details should be clearly distinguishable from the other information provided.

Privacy notice content

A privacy notice must be relevant to the collection process and include:

- that personal information is being collected and what information is being collected. (This may not always be obvious, such as where information is collected automatically.)
- who is collecting the information, and their contact details and address
- why this information is being collected and how it will be used, including the primary purposes and any known secondary purposes for the information in question
- whether the information will be disclosed, to whom and for what reason
- how an individual can request access to their personal information or amend/update it
- whether the supply of the information is voluntary or required by law, and any consequences if the information requested is not provided. In some cases, if information is not provided, certain actions may not be possible and may disadvantage the individual concerned. This may also be the case if consent is withdrawn.

The following additional details may also be included where relevant to the activity:

- that data is being disclosed or transferred outside NSW or to a Commonwealth agency, and where
- how consent can be withdrawn in cases where the privacy notice has been provided as part of consent. For example, the ability to unsubscribe from certain communications or who to contact to withdraw consent.

Where information is being collected verbally or automatically, the same privacy notice details should be provided.

1.1.6 Collecting only relevant personal information

In line with the policy, IPP4 and HPP2, collection processes should be designed to ensure that only relevant, accurate, up-to-date and complete information is collected.

[1] For example, the tailored privacy notice on the UTS website that covers information collected by virtue of someone using the website does not cover the collection of specific information via an online enrolment form. Similarly, the privacy elements in the UTS Student Declaration are for specific purposes and do not cover all activities involving use and disclosure of a student's personal information.

This may be achieved using automated fill-in boxes, data validation and mandatory fields where appropriate.

Whether information is relevant (and the level of detail collected) will depend on the collection purposes. For example, the level of personal information required for a staff member's sick leave application will differ depending on how long they are off work and whether the leave relates to a workers compensation claim.

Names, ID numbers or other identifying information should not be collected if the individual's identity is not required for the purpose the information will be used for. Separate information elements may still identify an individual when put together.

Privacy impacts need to be assessed when developing or changing a collection activity. This will assist business units to meet collection requirements.

1.2 Security of personal information

The following requirements apply to the protection of personal information. See also provisions outlined in the Information Technology Security Vice-Chancellor's Directive and the Information Technology Security Standards (PDF), which provide further information about security of information systems.

1.2.1 Secure storage

In line with the policy, IPP5 and HPP5, personal information is protected through a combination of practices, including:

- university-level policies (and other instruments) as outlined in this plan, including the classification of information in line with the Information Security Classification Standard (PDF, Staff Connect).
- local-level procedures in relation to the access, use and disclosure of personal information held by business units
- requirements of the Records Management Program, which includes the capture, accessibility, storage, retention and destruction of records
- secure storage, transportation and destruction of paper and digital records, computers and portable devices
- protection of information systems and data through design, passwords, security testing and monitoring, and the implementation of user rights and access controls
- enforceable contracts with third-party providers that host systems or collect, store, and/or process information on behalf of UTS
- privacy impact assessments
- staff education and training.

1.2.2 Retaining and destroying personal information

In line with the policy, IPP5 and HPP5, personal information will only be retained by UTS for as long as it may be used for legitimate purposes, and to satisfy legal minimum retention requirements.

For records containing personal information (including where held in paper or digital formats), staff are required to follow the requirements of the Records Management Policy and the university's procedures for archiving and destroying records.

Where it may be useful to keep personal information for a longer period than required, the information may be de-identified rather than destroyed. In such cases, destruction of identifying elements must be in line with the university's procedures for archiving and destroying records.

Personal information will not be destroyed early where there is a legal requirement to retain it.

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

Destroying paper records

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

Destroying digital records

Where personal information is stored on UTS-owned or leased IT equipment (including hard-drives and USBs), the equipment must be reformatted before it is disposed of to ensure the irreversible permanent deletion of all data. For other storage devices, such as DVDs or tapes, advice on appropriate destruction methods is provided by University Records.

1.2.3 Disclosing, transferring, or storing personal information outside UTS

In line with the policy, IPP5, IPP12, HPP5 and HPP14, the university may at times need to disclose, transfer or store personal information outside UTS.

Where this is at the instigation of an individual, any action taken will be based on that individuals' consent.

Other activities may involve UTS engaging a third party. For example, UTS may contract a commercial storage company to store paper records, or a third party to host an information system or store data in the cloud.

When engaging a third party, privacy obligations must be included in an enforceable contract. Reasonable steps must be taken to make sure information being disclosed, transferred or stored externally to UTS will not be held, used, disclosed or accessed further by the recipient without the express written permission of UTS.

Some university activities require that information be transferred or disclosed outside the jurisdiction of NSW or to a Commonwealth agency. Where possible, UTS will request consent from the individuals concerned. Where it is impractical to obtain consent, privacy will be managed through an enforceable contract with the third party concerned.

Other exemptions may also apply to disclosing or transferring data outside NSW under the privacy acts.

1.3 Access to information

In line with the policy, IPP6, IPP7, HPP6 and HPP7, UTS, where practical, must allow for a person to know:

- whether information is held about them
- what information is held about them, and
- how they can access (or apply for access to) this information.

These details may be provided on request or included in a relevant privacy notice.

Requests to access personal information are to be actioned without unreasonable delay. The volume and nature of personal information requested by an individual will affect how long it will take to action a request. An appropriate timeframe may need to be negotiated with the individual to ensure requests are processed efficiently and expectations are managed, in particular, if a request can't be actioned within 30 days.

1.3.1 How information can be accessed

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

- **UTS staff** can access their contact details, pay, leave and staff development records directly through the online NEO HR and finance system. Further to this, both current and past staff can request access to other personnel records by contacting Client Services in the Human Resources Unit (HRU).
- **UTS students** can access their contact details and study information directly through the online My Student Admin (student system portal) and My Subject Admin (class timetables portal), as well as through UTSOnline and Canvas (course and learning delivery systems portal). Further to this, both current and past students can request access to their student record by contacting Student Records (via student.records@uts.edu.au) in the Student Administration Unit, or the relevant faculty or unit.

- **patients or health/clinical clients** — where an individual wishes to access medical records held by UTS, requests must be referred directly to the relevant area in the first instance (eg Health Services in Students Services Unit or the Traditional Chinese Medicine Clinic in the Faculty of Science). Further information is available in the NSW Information and Privacy Commission (IPC) fact sheet accessing your health information in NSW (PDF).
- **other individuals** — all other individuals should forward initial requests to the relevant faculty or unit they believe holds their information. The UTS Privacy Officer can provide assistance in locating relevant areas and information if required.

In the event access to information is not provided on initial request, additional avenues that can be used to access personal information include:

- a formal request 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)[2].

See also privacy complaints in this plan.

1.3.2 Fees and charges

Fees to access information may only be charged where:

- information is available for purchase in a particular format (for example, production of transcripts, testamurs or statement letters of course completion or enrolment)
- access is requested to health information, or
- access is requested under the GIPA Act.

In some cases, information may not be released until outstanding debts or fines have been paid. For example, a student's results may be withheld if sanctions have been applied under UTS Rules based on money being owed to the university. The request for payment of outstanding debts or fines is not considered an expense imposed under privacy legislation.

1.3.3 Refusing to provide access to information

In some cases, a request to access information may be refused. Examples of when access may be refused include where:

- the information is already available through other standard business processes. For example, where the information is available for purchase, such as the production of an original document.
- access will disclose another individual's personal information. Attempts to remove the other individual's information should be made before access is provided or refused,
- the information is subject to legal professional privilege. Attempts to remove the affected information should be made before access is provided or refused.
- it is believed that providing access would pose a serious threat to the life or health of any individual
- refusal to provide access is permitted or required by law
- access would negatively affect law enforcement activities, or
- access would prejudice any pending investigation or dispute resolution process.

Where access has been refused, the following details must be provided to the individual in writing:

- the decision to refuse access and why this decision was made, and
- how the individual can appeal the decision.

All relevant documents in relation to the refusal must be captured as an official record.

[2] For further information about accessing information under the GIPA Act, see right to information (GIPA).

1.4 Accuracy and correcting information

In line with the policy, IPP8 and HPP8, inaccurate information must be corrected where it is possible and practical to do so. Relevant documents that support a request for a change may be requested and held as evidence (for example, change of name certificates or birth certificates).

Individuals can correct some information held about themselves or request information be corrected through the same processes that apply to accessing information (see section 1.3.1 above).

1.4.1 Refusal to correct information

In some cases, a request to correct information may be refused by UTS.

Examples where a request 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. For example, UTS will not retrospectively change records of decisions where the old information was up to date at the time it was used in making decisions.
- the question of accuracy is contentious. For example, where the information is a university business decision and is not deemed inaccurate by UTS.
- insufficient evidence has been provided to support the change.

Where a correction is refused, the following information must be provided in writing to the individual:

- the decision not to change the information and why this decision was made, and
- any appeal rights.

All relevant documents in relation to the refusal must be captured as an official record. If requested, a note about the requested change or viewpoint of the individual must be recorded so that it can be accessed and read with the original information in question.

1.5 Using personal information

In line with the policy, IPP9 and HPP9, reasonable steps will be taken to ensure information is relevant, accurate, up to date, complete and not misleading before it is used. The nature of such steps will depend on the information in question and the intended use.

Where practical, maintaining multiple sources of the same information will be limited in favour of having one authoritative source that can be more easily maintained. Alternatively, information held in various specific information systems will be drawn from one authoritative source where practical and reasonable to do so.

In addition, certain types of information should be maintained directly by individuals, such as staff and student contact details (see how information can be accessed under section 1.3.1 above).

1.5.1 How personal information may be used

In line with the policy, IPP10 and HPP10, personal information may only be used:

- for the purposes it was collected for, including the primary purpose and any secondary purposes identified in the privacy notice at the point of collection
- for a directly related purpose
- where an individual has provided consent
- where required or permitted by law, or
- in the event of an emergency situation as outlined under section 1.8 below.

UTS may also use information it holds for administrative processes, including:

- internal quality improvement processes and planning activities. Any personal information used for quality improvement processes and planning activities will be de-identified where possible and practical to do so. (See quality improvement and planning in section 1.5.4 below.)
- handling of complaints, investigations, appeal processes or litigation.

Where a new use is identified for personal information collected in the past, consent needs to be obtained unless the additional use is covered by this plan or a relevant exemption in the privacy acts.

In the event that an individual withdraws consent for their information to be used, the university will take reasonable steps to comply with the request as soon as practical. Action taken will depend on the context of the request and when it is received. 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 to be sent by law. Similarly, there may be a small delay between when a withdrawal is received and when it can be actioned.

1.5.2 Using personal information for research

Where personal information is collected or otherwise obtained for the purpose of undertaking research (including research involving the compilation or analysis of statistics), this will be done with the approval of a Human Research Ethics Committee. Privacy requirements and public interest considerations will be considered when approving research that requires the collection and use of personal information.

Where research is in the public interest and cannot meet the relevant privacy principles under the privacy acts, the research will be covered by the following statutory guidelines issued by the NSW Privacy Commissioner.

- Research involving personal information is covered by the Statutory Guidelines on Research — section 27B, Privacy and Personal Information Protection Act 1998 (NSW) (PDF).
- Research involving health information is covered by the Statutory Guidelines on Research, Health Records and Information Privacy Act 2002 (NSW) (PDF).

See also quality improvement and planning below.

1.5.3 Surveillance

Surveillance information relating to staff will be used in accordance with the Workplace Surveillance Act 2005 (NSW). Staff must be informed about surveillance activities. Any convert surveillance is only permitted without the knowledge of staff by court order .

Security activities that may generate surveillance information include:

- security surveillance through CCTV footage, which is undertaken for the protection of staff, students, members of the public and property. Signs are posted at various campus entries points identifying that cameras are in use.
- access to the university's physical locations via security passes.

Surveillance information generated from security activities may be used in the event an alleged incident occurs, including as evidence in an internal investigation. If required, surveillance information may also be provided to the police.

Other activities that may generate surveillance information include but are not limited to:

- access and use of information held in information systems, networks and other IT facilities. Information generated may be used to monitor appropriate use, as evidence of the authenticity of information and when actions were taken. Audit information is collected in line with the university's Code of Conduct and the Acceptable Use of Information Technology Facilities Policy.
- a record of use of UTS-provided fleet vehicles. Destination and mileage is recorded manually by users when fleet vehicles are booked.

1.5.4 Quality improvement and planning

The university uses information to improve the quality of its functions, activities and services. This may involve the use of statistical information, but at times may also involve the use of personal information. Where personal information will be used this way, it will be referenced in relevant privacy notices and consent collection as appropriate.

The university is implementing a system to analyse student data for quality and planning purposes. The appropriate use of data held in the Student Datamart,and the capture of data within that system will be governed by a data governance and use protocol. The objectives of this protocol are to ensure that:

- the use of student data complies with the university's policies, including the Privacy Policy and research policies, procedures and guidelines, and

  student personal information is used in line with privacy notices and consent provided by students, including consent provided under the university's Student Declaration.

The protocol will define all reporting, analysis, evaluation and improvement of teaching and learning activities that are sourced from the Student Datamart. It will also define the procedures by which staff will be provided access to the datasets.

Any research performed using data from the Student Datamart will be managed in accordance with the university's research policies, procedures and guidelines (see using personal information for research in section 1.5.2 above).

1.6 Disclosing personal information

1.6.1 When personal information may be disclosed

In line with the policy, IPP11 and HPP12, personal information may only be disclosed:

- for the purposes it was collected for, including the primary purpose and any secondary purposes identified in the privacy notice at the point of collection
- where an individual has provided consent, or where the individual should be aware based on the university's privacy notice that such a disclosure would occur
- for a directly related purpose[3] and where there is no reason to believe the individual concerned would object to the disclosure, or
- where this disclosure is necessary in an emergency situation, as outlined under section 1.8 below.

Some exemptions under the privacy acts to these limits on disclosure may apply. For example, where disclosure is required or permitted by law.

Examples where information may be disclosed include but are not limited to:

- verification of authenticity of an academic record, or that an individual has gained a qualification from UTS or an antecedent institution, in line with provisions of the Academic Records Vice-Chancellor's Directive (see also section 1.3.1 of this plan)
- where a company is undertaking an activity on behalf of UTS and where the third party is bound by the same privacy requirements. For example, where an IT company is contracted to provide support for a business system that holds personal information.
- where it is necessary for UTS to manage investigations, appeals or complaint handling processes, litigation or insurance matter. For example, information is required by the NSW Privacy Commissioner in relation to internal privacy reviews under PPIPA.
- where disclosure is required or permitted by law or for mandatory reporting obligation. For example, where information must 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 Act, or for mandatory reporting obligations under the Health Practitioners Regulation National Law (NSW) No 86a[4].
- where information is requested by a valid subpoena, warrant or court order. In such cases, requests will be actioned by UTS Legal Services.
- where disclosure 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

[3] For health information, a directly related purpose must be one that an individual would reasonably expect. For sensitive personal information, information may not be disclosed for a directly related purpose.

[4] See also the university's Course Related Work Experience: Procedures for Reporting Obligations to the Australian Health Practitioner Regulation Agency (AHPRA).

act. The university has specific procedures covering the release of information to law enforcement agencies, including the police, that detail authorisation to release under the NSW privacy acts or where a warrant will be required.

Where disclosure of information under legislation is a regular and routine process, it should be included in relevant privacy notice.

Where information has been disclosed beyond its primary purposes (including any directly related purposes, where consent was provided or where information has been disclosed under any exemptions), details of the decision and process involved must be capture as an official record.

1.6.2 Approving the disclosure of personal information

In line with the policy, disclosure of personal information must be approved by the relevant dean, director or head of area, or by the appropriate staff member who has been properly delegated this responsibility.

This delegation must be identified in relevant position descriptions, employment contracts, governance instruments and/or operating procedures as appropriate in the circumstances.

1.6.3 Access to personal information internally at UTS

Providing information to different business units for legitimate purposes is not considered a disclosure, however, information will only be accessed or provided to other internal parties who require the information for a legitimate use.

Provision of health information, in particular, is tightly controlled and is generally limited to areas that require access as part of the business process to which it relates.

Generally, some administrative functions require staff in certain areas to have access to files and documents that may contain personal information, such as an area's administrative support staff, IT support and systems administrators, and records management staff. Staff in these areas are governed by the university's Code of Conduct and relevant governance instruments and procedures governing appropriate access and use of information.

Some staff or areas of UTS may be consulted in relation to specific matters concerning a particular individual, due to their specific subject matter expertise. An individual's identify may be shared as part of this process where it is necessary to ensure accuracy of the advice requested.

Information may also be provided to relevant UTS staff where it is necessary for:

- handling of complaints
- management of potential or actual litigation
- internal audit and investigation functions, or
- reviews or investigations into alleged breaches of policy, rules or legislation.

1.6.4 Disclosure of personal information held in archives

Records of UTS that still exist after 30 years are generally considered to be open to the public under the State Records Act 1998 (NSW). UTS issues access directions under the State Records Act to limit access to archival records which contain personal information. This process is governed by the Records Management Policy.

1.7 Additional privacy requirements covering use and disclosure of health information

Further to section 1.6, and in line with the policy, HPP10 and HPP11, UTS may also use or disclose health information where it is deemed necessary for:

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

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

1.7.1 Use and disclosure of genetic information

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

1.7.2 Use of codes to manage an individual's health information

In line with the policy and HPP12, unique identifiers (such as ID numbers or other codes) may be used where it is necessary for the university to carry out its activities. For example, unique identifiers may be used to help identify individuals with similar names, increase privacy through the application of pseudonyms. Unique identifiers may be used for recordkeeping purposes. The use of unique identifiers will often assist in enhancing an individual's privacy.

External identifiers, such as Medicare numbers, may still be recorded. However, identifiers used by UTS will be generated by the university unless the individual concerned has agreed for UTS to use an external identifier for this purpose.

1.7.3 Anonymous health services

In line with the policy and HPP13, health-related services may be provided anonymously where lawful or practical to do so.

Anonymous provision is not normally practical in the context of the types of health services the university provides.

The relevant dean or director responsible for the provision of a health service may decide whether to provide anonymous health services on a case-by-case basis.

1.7.4 Linking health records with other agencies

In line with the policy and HPP15, the university will not link an individual's health record with those of another organisation without the individual's express written consent.

1.8 Use or disclosure of information in emergency situations

Personal information may be used or disclosed where it is considered necessary to lessen or prevent an imminent and serious threat to the life or health of any individual. With regards to health information, this includes a serious threat to public health and safety.

Where information is required in an emergency, it may often be based on verbal requests. Approval for the immediate use or disclosure of information in emergency situations must be obtained from one of the following staff members as appropriate in the circumstances:

- Vice-Chancellor, Provost or Deputy Vice-Chancellor (Corporate Services)
- Director, Student Administration Unit; Director, Student Services Unit or Deputy Vice-Chancellor (Education and Students) in relation to information about current, past or prospective students
- Director, Human Resources in relation to information about current, past or prospective staff, contractors or volunteers
- relevant member of the Senior Executive in relation to information that falls under their portfolio
- a registered medical professional in relation to a patient's information (eg a registered general practitioner or psychologist or a counsellor undertaking clinical supervision), or
- Manager, Security Services, where personal information is required to be released to the police. (Usually this will apply after hours where approval from the above staff members is unavailable.)

This process applies to immediate responses to verbal requests. This is not applicable to disclosures generally, which are covered under sections 1.6 and 1.7 of this plan.

1.9 Third parties acting on behalf of an individual

Unless permitted under this plan and the privacy acts and the exemptions outlined within, consent must be provided by an individual before UTS will deal with a third party on the individual's behalf in relation to their personal information or personal affairs. An individual can provide consent using the third party authority form (PDF) or in writing by other means.

Where an individual is either unable to provide consent or is otherwise incapable of providing consent, UTS may interact with a power of attorney or nominated emergency contact in a limited capacity. For example, assisting with student special considerations or staff leave arrangements as appropriate in cases where the individual is in hospital and unable to liaise with UTS themselves.

1.9.1 Deceased individuals

For deceased individuals, the authority to provide consent or otherwise deal with UTS in relation to an individual lies with the individual's power of attorney or next of kin.

1.9.2 Minors

UTS can collect personal information about a minor (under 16 years of age) from a parent or legal guardian.

The maturity of a minor will be taken into account before liaising with a parent or legal guardian about specific personal information, or disclosing personal information to the parent or legal guardian.

If disclosure of information to a parent or legal guardian is considered in the best interests of the minor in the circumstances, and the minor is not deemed mature enough to make an informed decision, information may be disclosed with the approval of the relevant dean or director (or a staff member delegated by them in procedures, position description or employment contracts to make such decisions).

In relation to health information in medical records of a university 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 clinic or practice manager.

1.10 Exemptions to privacy requirements

1.10.1 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 required or permitted under another law. Some examples of these are covered under the specific sections in this plan. UTS will only rely on exemptions to privacy principles where it is considered appropriate in the circumstances.

1.10.2 Public interest directions

The NSW Privacy Commissioner may make public interest directions to modify the application of privacy principles in certain circumstances. The Information and Privacy Commission NSW publishes current public interest directions issued by the Commissioner. UTS will only apply public interest directions if applicable in the circumstances.

1.10.3 Public registers

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

1.10.4 Assessing privacy impacts

A privacy impact assessment is required when a proposed activity or change to an existing activity is likely to affect an individual's privacy or involve personal information. This includes the development and implementation of information systems.

An assessment tool is available to help staff undertake the assessment process. An assessment will review the activity against the relevant IPPs and HPPs in the privacy acts as covered in section 1 of this plan.

The Australian Privacy Principles (APPs) in Schedule 1 of the federal Privacy Act will also be considered if an activity is governed by federal legislation that requires compliance with the APPs.

Consultation with different areas of UTS (such as UTS Legal Services, Information Technology Division (ITD), University Records or the UTS Privacy Officer) is recommended 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 hosted externally to UTS, the IT Security team will be consulted.

In certain circumstances, an external privacy expert may be engaged to undertake a privacy impact assessment. External experts should also be consulted if an independent review is required.

Approval to undertake an activity will generally sit with a dean, director, head of area, university committee or relevant project board; however the relevant dean, director or head of area responsible for the activity (or the information systems steward, if relevant) must ensure a privacy impact assessment is completed if required.

1.11 Reporting on privacy matters

The university's requirements in relation to reporting on privacy matters are outlined in the Privacy Policy.

1.12 Data breach reporting

Although processes are in place to protect personal information, if information has been lost, or subject to unauthorised access, modification or disclosure, a data breach will have occurred and will be managed in line with the university's data breach response procedures.

In the event of a data breach, the relevant business unit or information system owner is required to:

- respond immediately by taking necessary action to prevent any further data beach from occurring, or to lessen the impact. This may involve shutting down a system, changing security or halting a business process.
- inform the UTS Privacy Officer as soon as possible, detailing what 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 the incident.

Other internal reporting is required where a breach involves:

- data held in an information system, inform the relevant information system owner, the Chief Information Officer (CIO) in ITD and the Deputy Vice-Chancellor (Corporate Services)
- research data or associated information, inform the Deputy Vice-Chancellor (Research)
- a contract with a third party, inform the Deputy Vice-Chancellor (Corporate Services) and Director, UTS Legal Services
- deliberate or potential corrupt behaviour, inform the Deputy Vice-Chancellor (Corporate Services) or a nominated public interest disclosures officer under the Fraud and Corruption Prevention and Public Interest Disclosures Policy.

Where it is believed that the data breach poses a serious risk to an individual the information relates to, the individual may be informed of the data breach. Informing affected individuals, or regulatory bodies if required by law, will be decided on a case-by-case basis by the Deputy-Vice Chancellor (Corporate Services) in line with the university's data breach response procedures.

2 Education and training

2.1.1 UTS policy and governance

The Privacy Policy (the policy) is the primary UTS instrument covering privacy requirements and is supported by this plan. Privacy requirements will be included in other governance instruments, or otherwise cross-referenced, where appropriate.

Other governance instruments that facilitate privacy are listed in appendix 3 of this plan.

2.1.2 Staff orientation and induction

Privacy requirements and responsibilities 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 part of staff orientation, and details of information resources and training is provided to all new staff attending Vice-Chancellor's Welcome to New Staff events.

Supervisors are responsible for ensuring staff under their supervision, including contractors and casual staff, are informed of their privacy responsibilities and undertake appropriate training. This may involve both general privacy training as well as local induction into management of information locally.

2.1.3 Privacy training program

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

Privacy requirements should be incorporated into other 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.

2.1.4 University procedures and guidance

Procedures and information about privacy-related matters are provided to staff through the university's privacy topic on Staff Connect (intranet).

Procedures cover requirements for collecting, storing, retaining and destroying, providing access to or correcting, using and disclosing personal information, as well as details regarding privacy notices, consent, privacy impact assessments and research activities. These procedures are mostly high-level and need to be customised for specific business and information system processes as appropriate.

Advice is available from the UTS Privacy Officer where specific privacy requirements need to be included in other university-wide procedures.

2.1.5 Local training and procedures

Relevant business process owners and information system owners are responsible for ensuring staff undertaking business processes or accessing information systems understand the specific privacy requirements and commitments regarding the appropriate collection, storage, retention, use and disclosure of information relevant to the specific business processes or access information systems.

Advice is available from the UTS Privacy Officer where specific privacy requirements need to be included in local or system based procedures.

3 Communication with individuals

Information about how UTS deals with the personal and health information of students, staff and members of the public is covered in this plan and your privacy at UTS on the privacy at UTS website.

This website includes information and guidance on:

- how an individual can access or correct their information
- how UTS will deal with requests from others to access their information
- identity verification (see also section 3.1 below)
- surveillance activities at UTS, and
- how an individual can make a privacy complaint.

UTS also communicates with individuals through the use of privacy notices and/or consent forms at points where personal information is collected (see section 1.1.3 in this plan).

3.1 Identity verification

When dealing with an individual about their personal information, UTS will require that the individual confirm their identity. This also applies to third parties in cases where they have been given authority to act on an individual's behalf. UTS may need to collect or confirm information held where necessary to prove someone's identity to ensure UTS is not breaching an individual's privacy by dealing with the wrong person.

Identity may be verified through one or more of the following:

- staff or student ID number and date of birth
- use of student, alumni or staff official email accounts. Emails received from these email accounts are considered to be from the individual concerned and no additional identification is usually required.[5]
- photo identification, such as a current staff or student card, valid passport or driver's licence. For inquiries made in person, photo identification may only need to be sighted. For written or emailed inquiries, a copy of identification may be required. Communication via any non-UTS-provided email account will require that appropriate identification is provided.

The university also has procedures for providing certified documents to UTS, which should be referred to where relevant.

[5] Note that under Student Rules section 2.3, official communication between UTS and a student is to be via their official UTS student email account

4 Complaints

4.1 Making a complaint

If an individual believes that UTS has breached their privacy they should contact the faculty or unit responsible for the conduct in question as soon as possible. In many cases, these matters can be dealt with quickly by the faculty or unit concerned.

An individual may contact the UTS Privacy Officer for assistance, particularly where they do not know who they should be contacting.

If an individual is not satisfied with the response received by the faculty or unit in question, the individual may make a formal complaint about the alleged privacy breach. Formal complaints will be dealt with as a privacy internal review.

Any privacy complaint that relates to research activities, such as handling of research data, are referred to the Ethics Secretariat in the university's Research and Innovation Office (RIO) and to the Deputy Vice-Chancellor (Research). The complaint may be investigated by those areas in relation to research integrity or breaches of research ethics approvals. Where such complaints also meet the criteria for a privacy internal review, an internal review will also be undertaken.

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

4.1.1 Complaints not related to privacy

Complaints (or elements of a complaint) that do not relate to privacy will not be dealt with as part of a privacy internal review. These complaints must be referred to the appropriate part of UTS for action in line with the Code of Conduct or relevant policy.

4.2 A privacy internal review

Any complaint received by UTS relating to privacy that meets the criteria for an 'internal review' under PPIPA, will be dealt with as such regardless of whether the complaint specifically requests an internal review.

4.2.1 Applying for an internal review

An application for an internal review must:

- be made in writing and addressed to UTS
- include an Australian address for the receipt of correspondence
- be lodged with UTS within six months from when the complainant first became aware of the conduct the complaint relates to, and
- include enough information about the conduct so that it can be investigated.

UTS has developed a request for an internal review form (PDF); however, internal review applications may be lodged in other written formats as long as they meet the above requirements.

UTS is required to inform the NSW Privacy Commissioner of any internal review applications it receives and provide all correspondence with the applicant and any other relevant documents. The Commissioner is provided the opportunity to make a submission to UTS before an internal review is finalised.

For further information about how to apply for an internal review, see privacy complaints. The UTS Privacy Officer can provide further advice.

4.2.2 Internal review process

An internal review must be completed by UTS within 60 days of receiving a valid application, 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 requires UTS to investigate the conduct in question. This will include discussion with any key parties (whether internal or external to UTS) who were allegedly involved or who may have information about the alleged conduct.

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
- information obtained from the university's records and information systems
- UTS Rules, governance instruments or other relevant UTS documents
- requirements of PPIPA and HRIPA, any statutory guidelines or other relevant external documents
- any NSW Civil and Administrative Tribunal decisions or relevant case law, and
- any submission received from the NSW Privacy Commissioner before the review is completed.

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

4.2.3 Internal review outcomes

The draft findings of an internal review will be submitted by the internal review officer to the Director, Governance Support Unit or, in their absence, the Deputy Vice-Chancellor (Corporate Services), who will be responsible for deciding the outcome of the review. This may include approving any resulting recommendations.

An applicant will be advised of the findings of the internal review and the reasons for those findings within 14 days of the review being finalised.

The NSW Privacy Commissioner will also be advised about the final outcomes of an internal review.

An internal review may have either or both of the following outcomes:

- Where a breach of privacy is identified, UTS may offer a formal apology, take 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 expected outcome of the applicant and the nature of the breach.
- Where no breach of privacy is identified, no further action will be taken. However, depending on the circumstances, additional training or a review of procedures may 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.

4.2.4 External reviews and appeal rights

If an applicant is not satisfied with the outcome or handling of an internal review, they can apply for an external review of the decisions made with the NSW Civil and Administrative Tribunal (NCAT).

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

Where an internal review is not completed within the required 60-day period, this 28-calendar-day time limit starts when the 60-day period has expired.

Further information on reviews by the NCAT is available on the NCAT website under privacy of personal information.

4.3 Policy breaches and misconduct

Breaches of this plan will be managed in line with the statements outlined in the policy.

Individuals who deliberately breach privacy legislation may be personally liable for that action and attract legislative penalties under PPIPA or HRIPA, or criminal prosecution under the Crimes Act 1900 (NSW).

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.

5 Privacy contacts

5.1 Internal contacts

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

Prospective, current and past students who wish to inquire about information held about them centrally, should contact their relevant UTS Student Centre in the first instance.

Prospective, current and past staff can inquire about information held about them centrally by contacting the Human Resources Unit in the first instance.

See also accessing information under section 1.3.1 of this plan.

UTS Privacy Officer

Other inquiries should be referred to the UTS Privacy Officer:

telephone: +61 2 9514 1245
email: privacy@uts.edu.au
website: Privacy at UTS

5.2 External contacts

NSW Privacy Commissioner, Information and Privacy Commission NSW (IPC)

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

These definitions outlined in the Privacy Policy (the policy) are applicable for this plan. The following additional definitions are also applicable.

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

De-identified information means information that no longer identifies the individual to which it relates. Identifying information, in addition to an individual's name or ID number, may include any data elements that, when put together, can be used to identify an individual[6].

De-identify means 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 identifiable personal or health information is collected, and is usually done for a particular purpose.

Health service is defined under section 4, HRIPA. For UTS, this includes the UTS Medical Service, as well as faculty clinics such as the UTS Chinese Medicine Clinic, UTS Psychology Clinic and the UTS Orthoptics Clinic.

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

Internal review is a formal 'internal review' undertaken under the provisions of PPIPA into a complaint regarding an alleged breach of privacy.

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

Minor means an individual under the age of 18.

Primary purpose refers to the main reason for which information has been collected.

Privacy notice means a notice or statement which explains what personal information is being collected, its purpose, how it will be used, whether it will be disclosed and to whom, and how it can be accessed.

Secondary purpose refers to any purpose other than the primary purpose for information collection.

Sensitive personal information means a subset of personal information defined under section 19, PPIPA (and the policy), and includes information about a person's ethnic or racial origin, sexual activities, religious or philosophical beliefs, political opinions or trade union membership.

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

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

Unsolicited information means personal information received by UTS that was not actively collected or received as a byproduct of a process or an automated system.

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

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 1.1.1 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 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, etc.
- Assessment and examination records, including marks comments, final grades
- Supervision of students, including personal details and progress reports, attendance records
- Information relating to grievances, complaints and misconduct, and any appeals
- 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 attended events or who took 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 some information held in 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 some information technology
- Personal information relevant to warrants, court orders, subpoenas, contracts or other legal matters

Appendix 3: Related reading

University governance instruments

Privacy Policy

Data Governance Policy

Records Management Policy

Handling Student Complaints Policy

Handling Staff Grievances Vice-Chancellor's Directive

Fraud and Corruption Prevention and Public Interest Disclosures Policy

Code of Conduct

Information Technology Security Vice-Chancellor's Directive

Other university privacy resources

Privacy at UTS (public website)

Privacy (on staff-only intranet)

External resources

University of Technology Sydney Act 1989 (NSW)

Privacy and Personal Information Protection Act 1998 (NSW) (PPIPA)

Health Records and Information Privacy Act 2002 (NSW) (HRIPA)

Government Information (Public Access) Act 2009 (NSW) (GIPA Act)

State Records Act 1998 (NSW)

Workplace Surveillance Act 2005 (NSW)

Privacy Act 1988 (Cwlth)

HRIPA statutory guidelines (Information and Privacy Commission NSW)

General retention and disposal authorities (State Archives and Records Authority NSW)