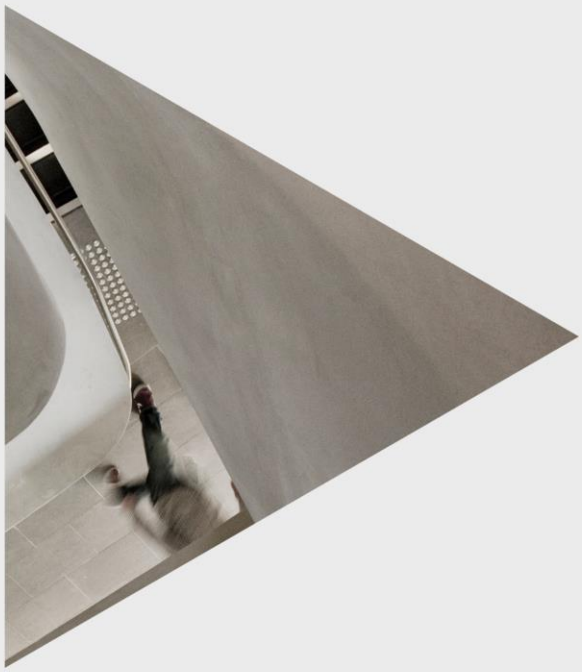
Privacy Management Plan



UTS CRICOS 00099F

Contents

1. Introduction

The University of Technology Sydney's primary governance instrument for managing privacy, and ensuring our functions and activities are meeting privacy obligations, is our Privacy Policy (the policy).

In support of this policy, we have developed this Privacy Management Plan (the plan) (available at Privacy regulations). The plan has been developed in line with section 33 of the Privacy and Personal Information Protection Act 1998 (NSW) (PPIPA).

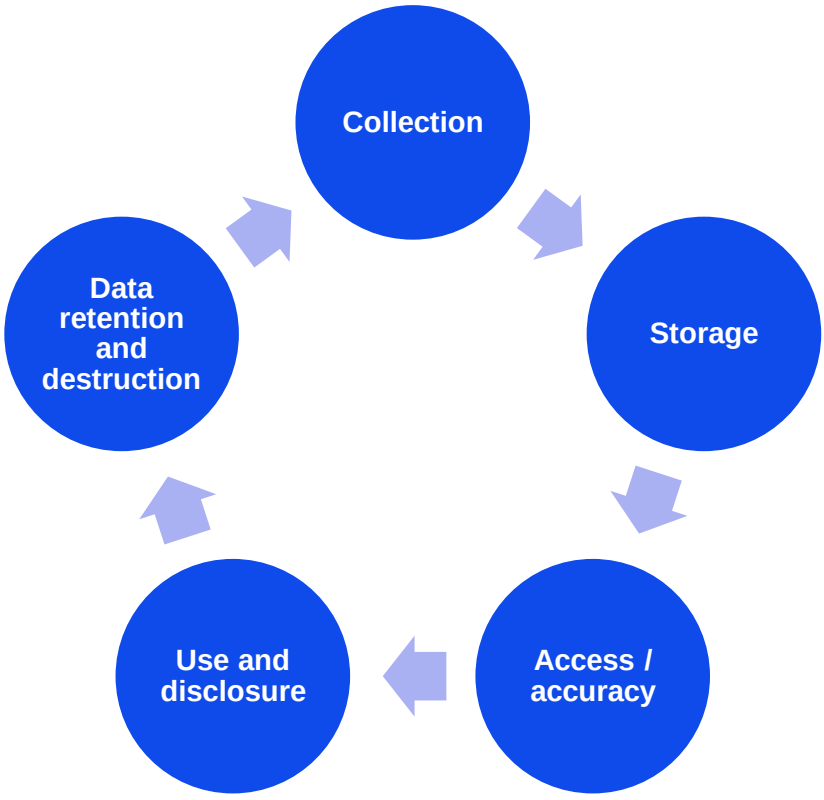
The plan details our approach to handling personal information under the following privacy laws:

- Privacy and Personal Information Protection Act 1998 (NSW) (PPIPA), and the Information Protection Principles (IPPs), and
- Health Records and Information Privacy Act 2002 (NSW) (HRIPA), and the Health Privacy Principles (HPPs).

Our policy, this plan and our processes will also be informed by legislation in other jurisdictions, such as the Privacy Act 1988 (Cwlth) and the European Union's General Data Protection Regulation (GDPR). Legislation in other jurisdictions may apply in certain situations and do not cover all of our activities.

a) How this plan is structured

We have aligned the main sections of this plan and our privacy obligations in line with the following 5 steps in the information lifecycle.



b) Scope of this plan

This plan covers UTS as a public sector agency, including our staff and affiliates (referred to as staff).

Our students and learners are not generally subject to the privacy laws unless they are also staff. Privacy obligations will apply to students if they are involved in research as part of their studies. Our Student Rights and Responsibilities Policy sets out our expectations for the personal and academic conduct of our students. Conduct that may have a negative impact on the privacy of others, or may be contrary to the Student Rights and Responsibilities Policy or our Privacy Policy, may result in misconduct proceedings.

c) Bodies that are not part of the university

Bodies that operate independently of our governance framework are not part of the university and are not covered by our Privacy Policy or this plan. These bodies include:

- controlled and associated entities
- UTS Students' Association

2. Collection

This section describes how and why we collect personal information. This section does not apply to information we receive that is unsolicited.

2.1. How we collect personal information

Relevant privacy principles: IPP1 and HPP1 require that information collected is for a lawful purpose and collected by lawful means.

a) How we collect personal information

Information will not be collected by unlawful means or processes. We collect personal information through a variety of methods. For example:

- online or manual forms, chat bots that people engage with, physical mail or emails
- verbally, in person, over the phone or through online meetings
- automatically, for example, via audit logs, website cookies, CCTV and access cards (refer also to our Surveillance Policy)
- social media and public sources of information
- from third parties where this is required.

b) Why we collect personal information

Our object and functions are defined in section 6 of the University of Technology Sydney Act 1989 NSW. Our object is to promote scholarship, research, free inquiry, the interaction of research and teaching, and academic excellence. Our functions in support of this object include:

- providing facilities for education and research
- encouraging the dissemination, advancement, development and application of knowledge informed by free inquiry
- providing courses of study, teaching and learning
- carrying out research
- participating in public discourse
- conferring degrees
- developing governance, rules, policies, procedures and quality assurance
- undertaking commercial functions and generating revenue
- developing and providing cultural, sporting, professional, technical and vocational services to the community
- general and ancillary functions that promote our object and interests
- functions conferred or imposed on us by other legislation (for example, work health and safety legislation).

We deal with various types of personal information in support of our object and functions, which may include sensitive personal information or health information.

Refer to Appendix 2 of this plan for further details about the types of personal information we deal with.

In some cases, the information we collect may be required by law. For example, where we collect certain demographic information to meet our government reporting obligations or require evidence to support a staff member's right to work. We endeavour to ensure this is clear in our collection processes.

2.2. Who we collect personal information from

Relevant privacy principles: IPP2 and HPP3 require that information is collected directly from the individual it relates to unless we have consent to collect information from other parties.

We collect information from prospective and current staff and students, alumni, donors, members of the public who we engage with, and research participants.

a) When we need to collect information from others

Sometimes we need to collect information from others if it is not possible or practical to collect the information from an individual directly. For example:

- Universities Admissions Centre, student recruitment agents or partners, collaborative institutions and sponsors
- pathway providers to UTS, including UTS College
- student practicums, professional placements or internship providers
- other education providers or employers to verify qualifications
- student exchange partners to facilitate exchange arrangements
- health care providers who may provide test results, certifications or professional authorities
- staff recruitment agents
- nominated emergency contacts, power of attorney or next of kin
- parents and legal guardians where a minor is under 16 years of age
- regulators and investigative agencies in performing their complaint handling and investigative functions (e.g. IPC, ICAC or AHPRA)

b) When information is collected or generated automatically

We may collect information by automated processes and not directly from someone. This may be the case when someone engages with a process or system, or physically attends our campus. For example:

- audio and/or visual recordings created for teaching, assessment purposes or staff training
- information collected when using our Wi-Fi or our website
- security cameras/CCTV that is in use across our campus, and body worn devices that may be used by UTS Security in certain situations (refer also to our Surveillance Policy)
- logs of physical access to our facilities through use of security passes
- logs of activity on our network, devices and information systems, or using our Wi-Fi or website
- logs generated from use of UTS-provided fleet vehicles or machinery

Some of this information when related to staff may be viewed as surveillance information and staff will be advised of this purpose under the Workplace Surveillance Act 2005 (NSW). Refer also to our Surveillance Policy.

2.3. How we are open and transparent when collecting information

Relevant privacy principles: IPP3 and HPP4 require that information is collected in an open and transparent way.

We achieve openness and transparency by ensuring that individuals are provided with a relevant and up-to-date privacy notice when their information is collected.

There is no one single privacy notice covering the whole of UTS and all of its activities. Instead, we have privacy notices covering key functions, and develop bespoke notices where they are required. Our key privacy notices cover our:

- students
- learners
- website users
- staff
- philanthropy, covering our donor-related activities
- marketing activities.

Our key notices are provided when we collect information but are also available from the privacy page in the footer of any of our main website pages.

2.4. How we ensure information collection is relevant and necessary

Relevant privacy principles: IPP4 and HPP2 require that information which is collected is relevant and necessary for our intended purposes, and not excessive or unreasonably intrusive.

a) Minimising data collection

We take steps to ensure we only collect what is relevant and necessary for the particular activity, and that what is collected is not excessive or intrusive. For example:

- we minimise data collected by reviewing each data element that is required
- for new activities, a privacy impact assessment is undertaken and data collection is reviewed.

b) Engaging with us anonymously

Relevant privacy principles: HPP13 provides that, where lawful and practical, an individual must have the opportunity to not identify themselves when engaging with or receiving health services.

Someone's identity is also considered when minimising data collection (see section 2.4(a) above).

The NSW privacy laws provide the opportunity for someone to remain anonymous when receiving health services if it is lawful and practical. Our faculty clinics require an individual's identity when collecting consent. Our health services are established to provide health services specifically to our staff and student community. We need to know the identity of an individual to verify their eligibility for these services.

3. Storing and protecting personal information

This section explains how we store and protect personal information.

Relevant privacy principles: IPP5 and HPP5 require that reasonable steps are taken to protect personal information from loss, unauthorised access, use, modification or disclosure, and other misuses.

a) Where personal information is stored

Personal information we hold is required to be stored in our university-controlled information systems. Some information systems are cloud-based and hosted with contracted service providers (refer to section 5.5).

b) How information is secured

We protect personal information using a range of technical and non-technical controls. For example:

- passwords, multi-factor authentication (MFA) and access controls
- encryption and data segregation
- policies and other governance instruments, including our Privacy Policy, Records Management Policy, Data Governance Policy and Information Security Policy, and related procedures
- our information security classification standard, which classifies information as 'public', 'internal', 'sensitive' or 'confidential'. Sensitive personal information and health information are classified as confidential and will have tighter security controls and protections applied
- physical storage assessments covering storage and transportation of physical records
- cloud security assessments for our cloud-based service providers
- confidentiality agreements, contracts and/or data sharing agreements
- privacy impact assessments
- staff training and education
- archiving and destruction procedures (refer section 6).

c) How access to information is controlled

Access controls are applied to our information systems to manage access to those who require it as part of their role. Staff are covered by the Code of Conduct, employment contracts and relevant governance instruments and procedures governing appropriate access and use of information.

Some administrative functions also require certain staff to have access to information. For example:

- administration, records and IT support staff and systems administrators
- subject matter experts where advice or support is required, including potential or actual litigation
- staff managing and investigating complaints or alleged breaches of policy, rules or legislation
- staff managing audit functions.

4. Accessing or amending personal information

This section explains how individuals can access or amend their personal information.

4.1. Understanding what information we hold

> Relevant privacy principles: IPP6 and HPP6 require that reasonable steps be taken to enable an individual to know if information is held about them, the nature of the information and the purpose of its use, and how the individual may access their information.

Appendix 2 summarises the types of personal information and health information that we hold and the purposes for which it is collected.

Privacy notices are also provided to individuals when their information is collected, which will also include what is collected and its intended purposes, as covered under section 2.3.

4.2. How to access or amend personal information

> Relevant privacy principles: IPP7 and HPP7 require that an individual be provided access to their information without excessive delay or expense.
>
> IPP8 and HPP8 require that, at the request of the individual, appropriate amendments (corrections, deletions or additions) be made to their personal information to ensure it is accurate, and that it is relevant, up-to-date and not misleading for the purpose it is to be used.

An individual will need to confirm their identity before we will provide access or amend their information. Refer to Providing proof of identity.

The following systems and processes are in place for individuals to access and/or amend their personal information. Refer also to section 11.1 for internal contacts if further help is required.

a) For staff

Current staff can access some of their personal information directly, including their personal and contact details, timesheets, contract details, leave and pay information, training records through NEO and Ascender Pay, and their travel and expense claims through Concur.

Some information can also be amended via these systems. For example, contact details, emergency contacts, qualifications and EEO data.

Who to contact for help

Where information cannot be accessed or amended directly, an individual can lodge a request with Client Services in the People Unit, or Payroll in the Finance Unit for pay-related information. They can also request information held by their faculty/unit by asking their supervisor.

b) For students

Current students can access some of their personal information directly, including their personal details and study information, through their UTS Student Portal and My Student Admin (student system portals), My Subject Admin (class timetables portal), and Canvas (course and learning delivery systems portal).

Some information can also be amended directly via My Student Admin. For example, contact details, emergency contacts and bank account details.

Requests for academic records

Refer to Academic record for details on how an individual can request a copy of their academic records.

Specific change requests for students

To change personal details, such as name, date of birth or gender, submit a Change of Student Detail Application with supporting documentation. Refer to Personal details.

To correct a student email address or username in Salesforce submit an IT ticket. Refer to IT Support.

Who to contact for help

Where information cannot be accessed or amended directly, or is not covered by the above, a student should lodge an online enquiry via ask UTS, which will be forwarded to the right team for consideration.

c) For clients of our clinics or related services

Who to contact for help

Patients, health/clinical clients, or clients of other support services such as accessibility or counselling, need to contact the relevant clinic or service directly to request access to or correction of their personal information or health information.

Further information on accessing health information is available from the NSW Information and Privacy Commission: Fact sheet — accessing your health information in NSW (PDF).

d) For research participants

Who to contact for help

Where an individual has been involved in a research project, they will need to contact the relevant academic contact or faculty that undertook the research project.

e) Other requests

Who to contact for help

A request from any individual to access their own personal information should be made under these provisions and made to the relevant area of UTS in the first instance.

If you are not sure who to contact, reach out to the UTS Privacy Officer who can assist.

4.3. How requests are managed

Access requests are managed in line with our requests to access to information procedures (refer Requests for access to information (SharePoint, staff only)).

Amendment requests are managed in line with our requests to correct/delete information procedures (refer Requests to correct or delete information (SharePoint, staff only)). Evidence may be required to prove that information is incorrect. For example, change of name or change of date of birth information.

These procedures are summarised below.

a) Timelines

Requests will usually be actioned as soon as practical and within 30 days. This may however depend on the complexity of a request. If longer is required UTS will liaise with the person making the request.

b) Fees and charges

There are no fees applied to amending personal information. For access requests, a fee may be charged in some cases. For example, where information is already available for purchase or to cover reasonable copying costs.

c) Decisions on providing access or amending personal information

In most cases, an individual will receive their information or amendments will be made. However, there may be a valid reason for a request to be refused.

Examples of where access may be refused include:

- providing the information may breach the privacy or others, or
- the information requests may be covered by legal professional privilege.

Examples of when amendment requests may be refused include where:

- we cannot alter or delete a state record (refer also section 6.1)
- there may not be sufficient evidence to claim the information is incorrect.

d) What an individual can do if a request is refused

Where a request has been refused, an individual should consult the UTS Privacy Officer. A formal request may also be sent to the UTS Privacy Officer to access or amend personal information, although this will not necessarily result in a different outcome.

If a request has been refused, an individual can lodge a complaint about the decision, or request a privacy internal review of the decision. Refer to section 9.

For amendment requests, an individual may also request a note be applied to the record if a change was not made.

e) Requesting access under the GIPA Act

An access application under the Government Information (Public Access) Act 2009 (NSW) (GIPA Act) (NSW's freedom of information law) is not usually required when someone wants to access their own personal information. However, it is an option if someone is also requesting other information, or a previous informal request has been refused.

Any individual may request information held by UTS under the GIPA Act. An application may include the personal information of others. We consider privacy requirements and provisions of the GIPA Act when deciding whether access will be provided. Where relevant, affected individuals are consulted.

For further information, refer to Right to information.

5. Using and disclosing personal information

This section explains how we limit and manage the use and disclosure of personal information.

5.1. How we ensure information is accurate before we use it

Relevant privacy principles: IPP9 and HPP9 require that reasonable steps are taken to ensure information is relevant, accurate, up to date, complete and not misleading before it is used.

There are several methods used to ensure information we rely on is relevant, accurate, up-to-date, complete and not misleading. For example:

- processes for individuals to access and amend their information (as covered in section 2)
- using single reliable sources of information to support our activities where we can (for example, ensuring appropriate integrations between our information systems)
- requesting individuals update their information (for example, at enrolment each year)
- verifying the authenticity of information provided to us (for example, other qualifications)
- reporting mechanisms to address data quality issues that are identified.

5.2. Limits on use and disclosure of personal information

Relevant privacy principles: IPP10 and HPP10 specify limits on the use of personal information; and IPP11 and HPP11 specify limits on the disclosure of personal information.

Limits on the use and disclosure of personal information include the following:

- We use and disclose personal information for the purposes we collected it for or purposes that are directly related to those main purposes. We include how information will be used or disclosed in our privacy notices as covered in section 2.3.
- Where we have an individual's consent. For example, someone may consent for us to provide their personal information to someone else.
- Where we are permitted or required to by law. For example, to meet our mandatory reporting obligations under the Higher Education Support Act 2003 (Cwlth) or the Health Practitioner Regulation National Law (NSW) No 86a, or for investigations, such as ICAC or NSW Ombudsman.
- Where it is necessary in an emergency situation. For example, to lessen or prevent serious and imminent harm to someone.
- To support our quality improvement and planning activities. For example, to manage the use of space, improve services, or to improve our course offerings, student retention, and to plan our curriculum. This may involve using various data sets and visualisation and analytics software, and business intelligence systems. The appropriate capture, access and use of data held in such systems is governed by this plan and relevant policies, including the Data Governance Policy.

a) Research

Research that involves personal information is approved by our Human Research Ethics Committee (HREC) in accordance with our Research Policy and Research Data Management Procedure.

If a proposed research project cannot meet privacy principles under the NSW privacy laws, but is considered to be in the public interest, the project will be required to meet the following statutory guidelines:

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

b) Information relating to minors

The maturity and capacity of a minor will be taken into account before dealing with or disclosing personal information to a parent or legal guardian. We will only deal with a parent or legal guardian where a minor is not considered to have capacity to understand their rights and responsibilities.

c) Information relating to deceased individuals

An individual's personal information remains protected as personal information for 30 years after they die. However, we may disclose health information in limited cases. For example:

- disclosing genetic information to a genetic relative in an emergency situation
- disclosing limited health information to an immediate family member on compassionate grounds.

For further guidance, see the IPC's Fact Sheet: Access to a deceased person's health information.

d) Referring individuals to other public sector agencies

UTS does not have any referral arrangements or memorandum of understanding with other public sector agencies for the purpose of referring an individual or their matter to that other agency.

e) Public registers

A public register is an official list of names, events and transactions that is required by law to be made available to the public. We do not have a public register under the NSW privacy laws.

5.3. Limits for health information

Health information is classified as confidential. Providing staff access to health information is tightly controlled and limited to areas that require access as part of the business process the information relates to.

In addition to section 5.2, we may also use or disclose health information where it is necessary:

- to manage our health services or for relevant training purposes
- for research that it is approved by a human research ethics committee
- for genetic information to be disclosed to a genetic relative to lessen or prevent a serious threat to the life, health or safety of the genetic relative concerned.

These above additional purposes are governed by the HRIPA statutory guidelines and the NSW Genetic Health Guidelines issued by the NSW Privacy Commissioner.

a) Using identifiers

Relevant privacy principles: HPP12 specifies limits on the use of identifiers to control health information.

We will generally use unique identifiers (such as ID numbers or codes) to control records. This allows us to ensure data accuracy and increase an individual's privacy through the application of a pseudonym.

b) Including information in health records linkage systems

Relevant privacy principles: HPP15 requires consent from individuals before including an individual's health information in a health records linkage system.

UTS's health service does not use health records linkage systems or provide information to them, including My Health Record. If we sign up in future, information will only be included with a patient's consent.

5.4. Limits for sensitive personal information

Relevant privacy principles: IPP12 specifies limits on disclosure of sensitive personal information, being information relating to ethnic or racial origin, sexual activities, religious or philosophical beliefs, political opinions or trade union membership.

Sensitive personal information has specific requirements when it comes to disclosure. It will only be disclosed when in line with the purpose it was collected or with consent. For example, we may use information relating to trade union membership where someone has requested their membership fees be paid from their salary.

Sensitive personal information is classified as confidential and has tighter security controls and protections applied. Providing staff access to sensitive personal information within UTS is tightly controlled and limited to areas that require access as part of the business process the information relates to.

5.5. Our use of service providers

We engage various service providers to provide services to us or on our behalf. For example:

- hosting information systems and platforms, including cloud providers
- supporting webinars, communications, events and learning activities
- supporting student recruitment, exchange, engagement and welfare.

Where personal information is collected by or provided to a service provider, we maintain control of the information through appropriate licence or contract controls. The contracted service provider may only access or use information to provide the contracted services. This is not generally considered a 'disclosure' of information, but a 'use' of information on our behalf.

5.6. Limits on disclosure or transfer of information outside NSW

Relevant privacy principles: IPP12 and HPP14 specifies limits on the disclosure or transfer of data outside NSW.

Some of our activities require us to disclose or transfer personal information outside NSW. For example, when we report to a Commonwealth agency or provide information to a student exchange partner overseas.

Where personal information is required to be disclosed outside NSW, or health information is transferred outside NSW, additional obligations apply. We mainly rely on one of the following to support a disclosure or transfer outside NSW (other grounds may also be applied if relevant on a case-by-case basis):

- A contract with the relevant recipient. For example, where we may have a contracted service provider (as covered in section 5.5).
- Where a disclosure is permitted or required by law. For example, to meet our mandatory reporting obligations to the Commonwealth government agency (as covered in section 5.2).
- Where the disclosure is required to support a contract with an individual. For example, a student exchange agreement between UTS, the individual and a university in another country.
- Where express consent has been received from the individual.

Where a third party is outside Australia, other privacy laws may also apply or be included in a contract. For example, where a vendor or university is processing data in the European Union (EU), additional provisions under the EU's General Data Protection Regulation (the GDPR) may also apply.

5.7. How we ensure our use or disclosure of information is relevant and appropriate

We have systems and processes to ensure our use or disclosure of personal information is appropriate. For example:

- assessing planned uses or disclosures of information when it is collected to ensure it is appropriate
- having controls for internal sharing of personal information to ensure intended uses are appropriate in the circumstances. Providing information to different business units for legitimate purposes is considered to be a 'use' of information. Data sharing within UTS is approved by the relevant data steward
- basing access to many of our information systems on access controls so that access to data is only provided to those staff who need to have access for their roles
- ensuring the disclosure of information is approved by the relevant data steward (or a delegated staff member).

6. Data retention and destroying personal information

This section explains how we manage data retention and the disposal of personal information.

6.1. How long personal information is kept

Relevant privacy principles: IPP5 and HPP5 require that personal information is only retained for as long as it can be legally used.

How long we keep personal information will depend on the following factors:

- The purpose information was collected for and is being used
- Any consent we have about how information can be used
- Minimum legal retention requirements under the State Records Act 1998 (NSW) or any other legislation that applies us
- Any contractual requirement (e.g. research contracts) where we receive data from another body
- Any pending or actual investigations or litigation if relevant
- Historical value to UTS and higher education.

We will dispose of health information and sensitive personal information under the same obligations.

Under our Records Management Policy, a data retention plan will be developed and implemented for our information systems. Data retention plans will define responsibilities and how data retention will be managed.

The destruction of our records requires approval under our Records Management Policy.

6.2. Requests for information to be deleted

An individual may request their information be deleted. A decision to delete information will consider any requirement to retain information under section 5.1.

A deletion request will be managed in a similar way to an amendment request. Refer to section 4.

De-identification/anonymisation of information may be used as a method of deleting personal information where it is appropriate to do so.

7. Incidents and data breaches

Cybersecurity incidents will be managed in line with our Cybersecurity incident response plan.

If a data breach is suspected or known to have occurred, our Data Breach Policy and our Data breach response plan (DBRP) (available at Data breaches (SharePoint)) will apply. These documents have been developed to meet the requirements of the NSW mandatory notification of data breach (MNDB) scheme[1] as well as other data breach notification obligations that may apply to us under other privacy laws.

7.1. How we will respond to a suspected data breach

A data breach is the unauthorised access or disclosure of person information, or the loss of personal information that may result in unauthorised access or disclosure.

Our approach to deal with a data breach under our Data Breach Policy is to:

- have a mechanism for staff to report suspected data breaches as soon as possible (via email to data.breach@uts.edu.au)
- take immediate steps to contain the breach or lessen its impact
- assess whether an eligible data breach has occurred. An eligible data breach is a data breach that may result in serious harm to affected individuals
- notify the NSW Privacy Commissioner and affected individuals where an eligible data breach has been decided, unless valid exemptions apply under the MNDB scheme. If a data breach falls within a different jurisdiction's privacy law, other regulators may also be notified, for example, the Australian Information Commissioner
- undertake a post-breach review and determine any ongoing actions to improve privacy protections.

Other parties may also be informed of suspected or actual data breaches depending on the incident, including the Australian Cyber Security Centre (ACSC) and/or contracted parties or other government agencies if a breach involves their data.

7.2. How we ensure we meet our notification obligations

We have various ways to ensure we handle any suspected or actual data breaches in line with both our legislative obligations and to support the privacy of the individuals we deal with. For example:

- implementing our Data Breach Policy
- including data breach responsibilities in key training for staff and in contracts with service providers
- linking our data breach response plan into our cybersecurity incident response plan.
- providing staff clear guidance on data breaches (available at Data breaches (SharePoint)).

7.3. Offences under NSW privacy laws

The NSW privacy laws include offences for certain conduct of public sector officials and other people[2]. For example:

- corrupt disclosure and use of personal and health information
- inappropriately offering to supply personal or health information that has been disclosed unlawfully.

The following steps are taken to inform staff of offences and minimise the risk of a staff member committing an offence:

- We cover offences in our online privacy training.

[1] The MDBN Scheme is covered in Part 6A of the Privacy and Personal Information Protection Act NSW.

[2] Offences are covered under Part 8 of PPIPA and HRIPA.

- We include action that will be undertaken for identified breaches of our policies by a staff member, including the Privacy Policy and the Data Breach Policy. Breaches of a policy are handled in line with our Code of Conduct that all staff accept when they sign their employment contract.

8. Exemptions

This section explains how we may apply exemptions to the privacy obligations in the NSW privacy laws as covered in sections 2 to 6 in this plan.

a) How we apply exemptions under the NSW privacy laws

There are exemptions to the IPPs and HPPs in the NSW privacy laws[3]. Examples that may apply include where:

- we are required to disclose information as part of an investigation or to an investigative agency. For example, ICAC or the NSW Ombudsman
- information is requested by a law enforcement agency. For example, police requests for information
- we may use or disclose information under the obligations in another law, such as our mandatory reporting (as covered in section 5.2)
- information is required to respond to an emergency situation (as noted in section 5.2). This includes any response required under the NSW State Emergency and Rescue Management Act 1989 (SERM Act)[4]
- personal information may be used for the purpose of research that is in the public interest (as covered under section 5.2(a).

We will only rely on an exemption where it is considered appropriate in the circumstances.

b) Privacy Code and Public Interest Directions

The NSW Privacy Commissioner may make public interest directions or a privacy code of practice to modify how privacy principles apply. We do not have a specific public interest direction or code of practice in place.

[3] Under PPIPA, these exemptions are included as specific exemptions in Division 3 of PPIPA. Under HRIPA, these exemptions are incorporated in the privacy principles themselves in Schedule 1 of HRIPA.

[4] A emergency under section 4(1) of the SERM Act includes 'fire, flood, storm, earthquake, explosion, terrorist act, accident, epidemic or warlike action'.

9. Complaints

9.1. Making a complaint

We will receive and address any complaints informally where possible. An informal complaint can result in quicker outcomes for those concerned. An informal complaint can be raised with the relevant faculty or unit involved. Students can also complain to our Student Complaints Resolution Office (refer to section 11.1).

An individual has the right to make a formal privacy complaint if they prefer. This is referred to as a privacy internal review request under section 53 of PPIPA. Refer to section 9.2. Unlike an informal complaint, a privacy internal review will have external appeal rights and is an option if an individual is not satisfied with the outcome of an informal complaint.

Informal complaints are addressed under our Staff Complaints Policy or the Student Complaints Policy as appropriate. Further information is available at Privacy complaints. The UTS Privacy Officer can also provide advice and guidance.

a) Research-related complaints

Where a complaint relates to research, such as handling of research data, it will be referred to the Executive Manager, Research Stewardship in the Research Office and to the Deputy Vice-Chancellor (Research). The complaint may also be investigated by those areas in relation to research integrity or a potential breach of research ethics.

b) Other complaint avenues

Individuals may complain directly to the NSW Privacy Commissioner at the NSW Information and Privacy Commission (IPC). Further information is available from IPC's How do I make a complaint?.

If an individual is in the EU, and believes their information is subject to GDPR, they may complain directly to the relevant EU Data Protection Authority in their member state. Given GDPR has limited application at UTS, it is recommended that an individual consult with the UTS Privacy Officer in the first instance.

9.2. Privacy internal reviews

a) Requesting a privacy internal review

A complaint that meets all of the following criteria will be dealt with as an internal review under the NSW privacy laws:

- The complaint is in writing and addressed to UTS
- It includes an Australian address for the receipt of correspondence
- It is lodged with UTS within 6 months from when the complainant first became aware of the conduct in question
- It includes enough detail about the conduct so that it can be investigated.

If a complaint meets these criteria, but an individual wishes their complaint to be treated informally, they can advise us of this when making their complaint (refer to section 9.1).

An applicant for an internal review can use our request for internal review form (available at Privacy forms) to assist them in lodging their request. This form is not mandatory so long as the above criteria is met.

b) Internal review officer and decision-maker

An internal review officer will be appointed by the University Secretary to investigate the complaint. This role is usually assigned to the UTS Privacy Officer unless they are unavailable or there is a conflict of interest.

The outcome of an internal review is decided by the University Secretary.

c) Role of the NSW Privacy Commissioner

We are required to report all internal review requests to the NSW Privacy Commissioner, including details of the complaint, the conduct in question, and the findings of the internal review. The Commissioner has the right to make a submission on the draft findings of an internal review before it is completed.

d) Internal review processes and outcomes

When investigating a complaint, we consider:

- information provided by the applicant or held in our records
- privacy principles or exemptions under the NSW privacy laws, other relevant laws or case law
- our rules, policies and procedures
- interviews with relevant parties
- any submission or response from the NSW Privacy Commissioner.

e) Timelines and outcomes

A privacy internal review needs to be completed within 60 days from when we received the application unless an extension is negotiated with the applicant. The applicant will then be advised of the outcome of the internal review within 14 days of its completion.

The NSW Privacy Commissioner will also be advised of the final outcomes.

f) Appeal rights

If an applicant is not satisfied with the outcome of the internal review, or we have not completed the review on time, they can appeal by lodging an application with the Administrative and Equal Opportunity Division of the NSW Civil and Administrative Tribunal (NCAT). Refer to external contacts in section 11.2.

To lodge an appeal the applicant has:

- 28 days from when they were provided the outcomes of their internal review
- if the internal review was not completed on time, 28 days from the date the internal review was due.

For further information, refer to NCAT's Privacy of personal information.

10. Communication and awareness

10.1. How we communicate with individuals about their privacy

We provide information to individuals about their privacy:

- by publishing this plan on the UTS website and through our Privacy Policy
- through our public Privacy at UTS website, which provides additional privacy related content
- through our privacy notices or consent forms as covered in section 2.3.

10.2. How we communicate to staff about their obligations

a) Our policies and procedures

Our Privacy Policy is our primary governance instrument covering privacy. Privacy requirements are also considered and included where relevant in other governance instruments as part of our policy development and review practices. This is achieved through collaboration between key stakeholders, including the policy owners, the policy team in the Governance Support Unit (GSU), and the UTS Privacy Officer.

Procedures and guidance about privacy-related matters are provided for staff on our Privacy hub (SharePoint, staff only).

Our key privacy and information management resources are listed in Appendix 3 of this plan.

b) Staff orientation and induction

Privacy requirements and responsibilities are included in the UTS staff induction program and staff welcomes. Supervisors are responsible for ensuring staff, including contractors and casual staff, are informed of their privacy responsibilities and undertake appropriate training.

Relevant data stewards and information system stewards are responsible under the Data Governance Policy for ensuring staff undertaking business processes or accessing information systems understand the specific privacy requirements regarding the appropriate collection, storage, retention, use and disclosure of information.

c) Privacy training

We provide online privacy training for staff. Staff can access privacy training through our Online Learning Management system (OLM) in NEO. Customised face-to-face (either in person or via MS Teams or Zoom) are also developed and provided to groups of staff on request.

Privacy requirements are be incorporated into other training programs for systems and processes where privacy considerations apply. Additional training for stewards is also provided.

d) Privacy Contact Network

We have a Privacy Contact Network that includes select representatives from faculties, centres, institutes and units. The network's key focus is developing and maintaining a level of knowledge and understanding of privacy obligations across the university.

e) Advice and guidance

Further advice and guidance are available from the UTS Privacy Officer where specific privacy requirements need to be included in other university-wide documents or local procedures and processes.

11. Privacy contacts

11.1. Internal contacts

a) UTS Privacy Officer

Privacy inquiries can be referred to the UTS Privacy Officer in the Governance Support Unit (GSU):

telephone	+61 2 9514 1245
email	privacy@uts.edu.au
post	PO Box 123 Broadway 2007 NSW

b) Cybersecurity issues (for UTS or our service providers that may impact on UTS)

Report a suspected or actual cybersecurity risk or incident, including a potential data breach that impacts one of our information systems, to our UTS Cybersecurity Information Office:

telephone	+61 2 9514 9009 (UTS Cybersecurity Information Office)
telephone	+61 2 9514 2222 (UTS IT Support Centre (if the cybersecurity office is unavailable))

c) Student complaints

Students can make a complaint to our Student Complaints Resolution Office

email	student.complaints@uts.edu.au.
online form	complaints form (via our student portal, student login required).

d) Data Protection Officer (DPO)

A DPO role under the EU's GDPR. The UTS Privacy Officer is not a delegated DPO, however many of the tasks and activities associated with the DPO role are part of the UTS Privacy Officer's role.

Any communication for the DPO should be referred to the UTS Privacy Officer in the first instance.

11.2. External contacts

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

telephone	1800 472 679 (free call)
email	ipcinfo@ipc.nsw.gov.au
postal mail	GPO Box 7011, Sydney NSW 2001
website	ipc.nsw.gov.au

b) NSW Civil and Administrative Tribunal (NCAT)

Privacy internal review appeals are dealt with by the Administrative and Equal Opportunity Division of NCAT. Refer also to section 9.

telephone	1300 006 228
website	NSW Civil and Administrative Tribunal

c) European Union Data Protection Authorities

website	EU national data protection authorities

12. Version control

Plan contact	UTS Privacy Officer
Approval authority	University Secretary
Approved	09/11/2023
Review date	2028
File number	UR23/574
Superseded documents	None

Version history

Version	Approved by	Approval date	Effective date	Sections modified
1.0	Deputy Vice-Chancellor (Corporate Services)	20/12/2017	03/04/2018	New plan.
1.1	Director, Governance Support Unit	29/01/2020	29/01/2020	Minor correction to statement 1.8.4 re linking health records with other agencies.
1.2	A/Director, Governance Support Unit	18/11/2020	18/11/2020	Title change for Director, Legal Services, to General Counsel.
2.0	Director, Governance Support Unit	20/05/2021	28/05/2021	Updates and corrections and minor changes resulting from the review of the Privacy Policy.
2.1	Director, Governance Support Unit	27/10/2021	27/10/2021	Updates as a result of Fit for 2027 key portfolio changes and in response to the Information and Privacy Commission (NSW) review.
2.2	Director, Governance Support Unit	9/3/2022	9/3/2022	Amendment of section 1.9, and 1.12.1, relating to emergencies following structural changes and updates to PPIPA in Nov 2021. Minor changes to reflect changes in organisational structure.
3	Director, Governance Support Unit	09/11/2023	28/11/2023	Changes following a full review and the development of the new Data Breach Policy.

Appendix 1: Definitions

Affiliate is defined in the Code of Conduct.

Anonymous means a situation where an individual being provided a service is not identified or identifiable.

Consent is defined in the Privacy Policy.

Data breach is defined in the Data Breach Policy.

Data steward is defined in the Data Governance Policy.

De-identified information (also **anonymised)** means information that no longer identifies the individual it relates to. 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. Where information can readily be matched with other information to identify an individual, it should not be considered de-identified information.

Disclosure is defined in the Privacy Policy.

Emergency situation is defined in the Privacy Policy.

Health information is defined under section 6, HRIPA and is a subset of personal information that relates specifically 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 may also include information that relates to permanent or temporary physical or mental disabilities, workers compensation processes or accident reports, sick leave management, special considerations and other arrangements that relate to health issues.

Health service is defined under section 4, HRIPA. For UTS, this includes the UTS Health Service, as well as faculty clinics.

Health privacy principles (HPPs) are defined under Schedule 1 of HRIPA.

Internal review is a formal review undertaken internally by UTS under the provisions of PPIPA into a complaint regarding an alleged breach of privacy.

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

Learner, for the purposes of this plan, includes individuals undertaking, for example, short courses, tasters, bridging courses and microcredentials.

Minor means an individual under the age of 18.

Personal information is information as defined under section 4, PPIPA. Personal information refers to information or an opinion 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.

For the purposes of this plan 'personal information' includes 'health information' unless otherwise specified.

Privacy notice means a collection notice or statement that 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.

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

Student is defined in Schedule 1, Student Rules.

Surveillance and **Surveillance information** are defined under section 3 of the Workplace Surveillance Act 2005 (NSW). Refer also to the Surveillance Policy.

Unsolicited information means personal information received by UTS as a by-product of a process or an automated system. It is information that is not actively collected or received.

Appendix 2: Types of personal information we handle

The following details the types of personal information and health information that we collect and hold in support of our functions (as covered in section 2.1).

a) Students and learners

- Student details, including photograph, contact details, address, date of birth, previous education, subjects, courses, qualifications attained, fee payment, bank details, fines and debt information if applicable, language, visa and immigration status, exchange details, and sponsorship details where applicable.
- Admissions and enrolment, leave of absence or withdrawals, or special consideration requests, which may include health information if relevant.
- Course progression, study plans, variations, supervision records, progress reports, attendance, assessment and examination records, including marks, comments, final grades.
- Applications, management and receipt of prizes, awards and scholarships.
- Reports of hazards and incidents, which may include health information.
- Grievances, complaints and misconduct, appeals and resulting outcomes, including any investigation. This may include health information or sensitive personal information if relevant.
- Completion of mandatory or optional training.
- 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. This may include health information where relevant.
- Graduation and course completion, including names and contact details, course and qualifications, employment status and credentials.
- Sensitive personal information relating to ethnicity and Indigenous status.
- Health information relating to disabilities and/or accessibility requirements, Overseas Student Health Cover (OSHC) details and medical history in some cases where relevant. Health information may also exist in relation to special consideration, leave of absence or withdrawal requests if relevant.

b) Teaching and learning

- Comments and personal details provided in survey responses.
- Assessments and coursework of students, including audio-visual components, tutorial and online subject participation, records of online or in-person examinations.

c) Research

- Research management related records such as ethics committee minutes, participant consent and information forms, intellectual property agreements and licences, and grant applications.
- Data collected as part of approved research activities, which may include personal information, sensitive personal information or health information depending on the research.
- Clinical patient records held by our research clinics, which will include health information.

d) Staff and affiliates

- Recruitment information relating to potential candidates, as well as applicants. Including contact details, results from internet or social media searches, job search or professional networking websites, applications, CVs, candidate databases (which could include salary), previous employment

details, referee reports, skills assessments, psychometric and personality profiles, interviews, security and working with children checks where applicable, credit, criminal background checks if appropriate for the role, qualification checks for academic credentials.

- Eligibility to work in Australia checks, including visa information and information collected in relation to sponsored visas.
- Staff details, including date of birth, photograph, contact details, address, emergency contact details, tax declarations, banking details, contracts of employment, previous employment details, salary details, superannuation information, EEO information, training undertaken and results if applicable, changes in contract, including work arrangements, acting roles; promotions, including applications, CVs, qualifications, referee reports and references.
- Sensitive personal information relating to ethnicity and indigenous status, and gender identity. Trade union membership may be held if payments are being made on a staff member's behalf.
- Leave requests, approvals and related documents. This may include health information for some types of leave, such as sick or carers leave.
- Work planning and performance reviews, including 360 leadership diagnostic assessments and comprehensive assessment reports, probation plans and performance management.
- Reports of hazards and incidents, which may include health information.
- Grievances, complaints and misconduct, appeals and resulting outcomes, including any investigation. This may include health information or sensitive personal information if relevant.
- Completion of mandatory or optional training.
- Health information relating to workers compensation, accidents and injury-related information, medical certificates, health reports and questionnaires.
- Resignations or retirements, or other forms of separation, including exit interviews and surveys.
- Personal details of nominated, appointed and elected committee members.

e) Provision of services to staff and students

- Medical records, including personal details, confidential health information or sensitive personal information required for the provision of services, such as health or counselling services.
- Wellbeing services and support (for example, the Employee Assistance Program (EAP)), health case management, where access to coaching services is funded by the faculty, or in other cases where express consent is provided by the staff member for any other EAP provided service.
- Other student services and support, including accessibility support, financial assistance, housing, mentoring, career support and internships, language and other support services.
- Support services of Jumbunna supporting Indigenous students, and our Centre for Social Justice and Inclusion. Some sensitive personal information may be held to support students in using these services.

f) Alumni

- Alumni details, including contact details of graduates of UTS and its antecedent institutions and photographs, details of who attended events or who took up special offers.

g) Community and industry engagement and partnerships

- Philanthropy activities and engaging with our donors, including history, dates, amounts, conditions of gifts, contact details, philanthropic interests and details of their contact with UTS.
- Names and contact details of prospective students or partners.

- Names and contact details of volunteers including volunteer mentors.
- Incursion programs into schools, or excursions to UTS and associated programs, including names and professional contact of career advisers, principals and teachers, and names and contact details of participants.
- Event management, including attendee information, contact details, titles, position details, organisation's details, dietary and access requirements. This may include health information where relevant, and may also include staff and students.
- Library, Art Gallery and Archive records of donors and users of these services. Library services include photo identification, borrowing record, items currently on loan, fines.
- Community surveys and engagement in the university's activities, such as consultation broadly on our strategy.

h) Administrative and governance functions

- Financial details, such as creditors, debtors and bank account details.
- Security incident reports, including CCTV or other security video footage.
- Declarations of conflicts of interests.
- Protected disclosures.
- Information access request, such as under privacy laws or the GIPA Act.
- Access logs and audit trails of staff and student activity in their use of information systems, technologies, and physical locations.
- Personal information relevant to warrants, court orders, subpoenas, contracts or other legal matters.
- Administrative records dealing with governance, finance, property (land and buildings), security (including CCTV), procurement.
- Information and communication technologies records such as email and other account information, websites and cookies.

Appendix 3: References

a) Our governance instruments

Policies by classification

University of Technology Sydney Act 1989 (NSW)

b) Our privacy resources

Privacy hub (SharePoint, staff only)

Privacy at UTS (public website)

c) Key privacy legislation

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

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

d) Other relevant legislation

Data Availability and Transparency Act 2022 (Cwlth)

General Data Protection Regulation (EU) (GDPR)

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

Privacy Act 1988 (Cwlth)

State Records Act 1998 (NSW)

Workplace Surveillance Act 2005 (NSW)

e) Other external resources

Information and Privacy Commission NSW

NSW Civil and Administrative Tribunal

State Records NSW: Retention and disposal overview