Privacy Policy

1. Purpose

1.1 The Privacy Policy (the policy) provides a framework to protect the privacy of all individuals at UTS in compliance with relevant privacy acts, including the establishment of the Privacy Management Plan (the plan) (available at Privacy regulations).

2. Scope

2.1 This policy and the plan apply to all staff, students and affiliates.

2.2 This policy does not cover bodies that operate independently of the university's governance framework, including controlled or associated entities of UTS.

3. Principles

3.1 The university will:

- strive to create, promote and maintain a culture of respect for the privacy of all individuals, and
- incorporate privacy requirements into processes, procedures and information systems.

4. Policy statements

Privacy Management Plan

4.1 The plan implements the provisions outlined in this policy, further outlining the university's approach to the protection of personal and health information (hereafter personal information[1]) under:

- the Privacy and Personal Information Protection Act 1998 (NSW) (PPIPA)
- the Health Records and Information Privacy Act 2002 (NSW) (HRIPA), and
- where applicable the requirements of the Privacy Act 1988 (Cwlth) and the European Union's General Data Protection Regulation (GDPR).

Managing personal information

4.2 UTS will establish systems and provide guidance to appropriately manage personal information where it is held by the university.

[1] Unless otherwise indicated, references to 'personal information' will include 'health information'.

4.3 Personal information is considered to be ‘held’ by the university if:

- the university is in possession or control of the information, or
- the information is in the possession or control of staff or affiliates of the university in the course of their duties, regardless of their physical location.

Collecting personal information

4.4 Personal information (including sensitive personal information) must be collected in line with the requirements of the plan. Collection of any personal information must be:

- approved by the relevant data steward
- accompanied by a privacy notice and/or consent as relevant to the situation, and
- relevant and necessary for a lawful activity of UTS.

Security and access

4.5 Personal information held by UTS must be stored securely in approved information systems and in line with the requirements of the Records Management Policy and the Cybersecurity Policy (under development).

4.6 Personal information may only be accessed by staff, students or affiliates for legitimate reasons and for the business of the university. Access to personal information of others for any other reason is not permitted.

4.7 Personal information may only be retained for as long as it may legally be used in line with the purpose(s) for which it was collected and/or for which consent was received. Minimum legal retention requirements under the Records Management Policy also apply.

Individual rights to access and accuracy

4.8 An individual has a right to know what personal information is held about them and a right to request access to that information for review or correction where appropriate.

Use and disclosure

4.9 Personal information may only be used or disclosed in line with the plan.

4.10 The immediate use or disclosure of personal information is allowed in emergency situations in line with the conditions outlined in the plan.

4.11 Where the university discloses or transfers personal information outside NSW, or to a Commonwealth agency, it is the responsibility of the relevant data steward where applicable to ensure that all privacy impacts are assessed and addressed in line with the plan.

4.12 A unique identifier or number may only be applied to a person’s health information where necessary for UTS to carry out its activities, and in line with the plan.

4.13 Exemptions to privacy requirements may only be applied where appropriate in the circumstances and in line with the plan and the privacy acts.

Working with external parties and service providers

4.14 Where UTS engages in an activity with an external party that involves the collection, use and/or storage of personal information, the relevant data steward where applicable must ensure that:

- the activity in question is assessed to ensure that it satisfies the privacy obligations outlined in this policy and the plan
- relevant privacy obligations are imposed on the external party through an enforceable contract equivalent to the requirements outlined in this policy, and
- the external party's compliance with privacy obligations in the contract is monitored to ensure the obligations are being met.

Data breaches and complaints

4.15 An identified or suspected data breach involving personal information must be responded to immediately and reported to the UTS Privacy Officer and the relevant data steward in line with the plan and the university's Data breach response procedures (Staff Connect).

4.16 Suspected or actual data breaches identified as part of a public interest disclosure must be managed in line with the Fraud and Corruption Prevention and Public Interest Disclosures Policy and Guidelines.

4.17 Breaches of this policy or the plan will be managed under the Code of Conduct and relevant enterprise agreements. Breaches of this policy in relation to research data (that constitute a research integrity breach) will be managed in line with the Research Policy.

4.18 Data breaches by students involving personal information must be managed in line with the Student Rules and Student Rights and Responsibilities Policy as appropriate.

4.19 Privacy complaints will be managed in line with the Staff Complaints Policy or the Student Complaints Policy as appropriate.

4.20 A privacy complaint that meets the requirements of a privacy internal review, or a request for a privacy internal review, under NSW privacy legislation will be managed as a privacy internal review in line with the plan.

5. Policy ownership and support

5.1 Policy owners

The Deputy Vice-Chancellor (Corporate Services) is responsible for policy enforcement and compliance, general oversight of records, information and privacy management at UTS, including the Privacy Management Plan (available at Privacy regulations). The Deputy Vice-Chancellor (Corporate Services) will also decide on external reporting to relevant statutory boards in the event of a data breach.

The Director, Governance Support Unit (GSU) is responsible for:

- managing policy compliance
- overseeing the implementation and review of this policy and the plan
- delegating and resourcing the role of UTS Privacy Officer
- overseeing and deciding the outcome of a privacy internal review conducted under PPIPA, and
- statutory reporting on privacy related activities.

5.2 **Policy contact**: The UTS Privacy Officer (GSU) (refer Privacy contacts) is responsible for:

- approving and disseminating procedures and guidelines to implement, and support compliance with, this policy and the plan (at a university-wide level, or activity basis as appropriate)
- establishing the UTS privacy program in line with this policy and the plan
- providing privacy training (available via Neo HR System) and other relevant education programs
- publishing procedures and providing advice on privacy
- assisting and providing advice on privacy impact assessments
- investigating privacy internal reviews and related complaints and referring outcomes to the Director, GSU
- appointing a privacy contact officer to assist in these duties as required.

5.3 Others

Deans, directors and heads of areas are responsible for:

- advocating good privacy practices and ensuring they themselves, and their staff, are aware of privacy requirements
- ensuring privacy is addressed in business process procedures where relevant
- approving information collection activities and processes, including acceptable use of the information collected
- approving the disclosure of information other than disclosure in emergency situations, or otherwise delegating under procedures or in position descriptions this function to a staff position or role
- providing appropriate training and education programs for all staff regarding the privacy needs of their relevant faculty or unit and its activities
- completing privacy impact assessments on new or high-risk activities and addressing any privacy issues identified, including where external parties may be involved in an activity in line with this policy
- dealing appropriately with informal privacy complaints in consultation with the UTS Privacy Officer.

All staff, students and affiliates are responsible for the management of personal information in line with this policy. This applies whether working or studying on or off-campus or when using personal or UTS IT resources.

6. Definitions

These definitions apply for this policy, the plan and all associated procedures.

Affiliates is defined in the Code of Conduct.

Consent means the informed, specific and current permission received from an individual (who has the capacity to understand and provide it), allowing the university to undertake certain actions in relation to their personal information. Consent must be voluntary and provided freely with choice.

Data breach is defined in the Data Governance Policy.

Data steward is defined in the Data Governance Policy.

Disclosure means providing personal information to a third party external to the university in circumstances where the information would not normally be accessible, and where UTS loses effective control of the information. Sharing personal information between business units of UTS is not considered a disclosure where it is required to conduct the legitimate business activities of the university, for which the information has been collected.

Emergency situation as used in the context of this policy and the plan refers to 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.

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.

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 policy 'personal information' includes 'health information' unless otherwise specified.

Privacy acts, for the purposes of this policy, means the Privacy and Personal Information Protection Act 1998 (NSW) and the Health Records and Information Privacy Act 2002 (NSW) and other legislative privacy provisions, including the Privacy Act 1988 (Cwlth) or the European Union's General Data Protection Regulation (GDPR), as applicable.

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.

7. Approval information

Policy contact	UTS Privacy Officer
Approval authority	Vice-Chancellor
Review date	2024
Version	2.0
File number	UR17/4140
Superseded documents	Privacy Vice-Chancellor's Directive (UR14/558)

Version history

Version	Approved by	Approval date	Effective date	Sections modified
1.0	Vice-Chancellor	20/12/2017	03/04/2018	New policy.
2.0	Vice-Chancellor	17/05/2021	28/05/2021	Amendments as a result of a scheduled three-year review and to reflect updates resulting from the Policy Impact Project (2020) and references to European Union's General Data Protection Regulations and clarification of the role of data stewards.

Web version

Privacy Policy

References

Code of Conduct

Cybersecurity Policy (under development)

Data Governance Policy

Enterprise agreements

European Union's (EU) General Data Protection Regulation (GDPR)

Fraud and Corruption Prevention and Public Interest Disclosures Policy and Guidelines

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

Privacy Act 1988 (Cwlth)

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

Privacy at UTS (and privacy contacts)

Privacy (Staff Connect)

Privacy training for staff (staff only)

Privacy Management Plan (available at Privacy regulations)

Records Management Policy