Privacy Vice-Chancellor's Directive

Abstract

This Directive articulates the requirements for UTS to protect the privacy of all individuals, including staff, students and members of the public, by appropriately managing personal information and data in the conduct of the University's business.

Dates	Directive approved Directive takes effect Directive is due for review (up to five years)	29/05/2015 24/06/2015 05/2020
Approved by	Vice-Chancellor	
Implementation Officer	Director, Governance Support Unit	
Relevant to	All staff (including contractors) and students	
Related documents	Privacy Management Plan (PDF) Privacy Impact Assessment Tool (.docm) (staff only) Records Management Vice-Chancellor's Directive Handling Student Complaints Policy and Guidelines Handling Staff Grievances Vice-Chancellor's Directive Fraud and Corruption Prevention and Public Interest Disclosures Policy and Guidelines Code of Conduct Student Charter Student Rules Acceptable Use of Information Technology Facilities Policy Information Technology Security Vice-Chancellor's Directive	
Legislation	Privacy and Personal Information Protection Act 1998 (NSW) (PPIPA) Health Records and Information Privacy Act 2002 (NSW) (HRIPA) Privacy Act 1988 (Cwlth) Government Information (Public Access) Act 2009 (NSW) State Records Act 1998 (NSW) Workplace Surveillance Act 2005 (NSW)	

File number	UR14/558
Superseded documents	Privacy and Protection of Personal Information Vice-Chancellor's Directive

Contents

1. Purpose

The University of Technology, Sydney respects the privacy of each individual and has a legislated obligation to protect personal and health finformation. The Privacy Vice-Chancellor's Directive (the Directive) supports data governance and articulates effective implementation of legislative requirements in relation to the management of personal and health information. This Directive is supported and implemented by the UTS Privacy Management Plan (PDF).

2. Scope

This Directive applies to all staff and students, including contracted third parties working on behalf of the University.

This Directive specifies behaviours and actions required in dealing with personal or health information, including the provisions specified in Part 2, Division 1 of the Privacy and Personal Information Protection Act 1998 (NSW) (PPIPA), and the Health Privacy Principles contained in Schedule 1 of the Health Records and Information Privacy Act 2002 (NSW) (HRIPA).

This Directive does not replace or limit the requirements of relevant privacy legislation, the provisions of which must be adhered to by all University staff, students and contractors.

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

This Directive should be used in conjunction with the Privacy Management Plan (PDF).

3. Definitions

The following definitions apply for this Directive.

Business unit refers to a UTS department, faculty, unit, research centre and other centres, institute, school, office or branch.

Consent refers to authorisation received from an individual, preferably in writing, permitting the University to undertake a particular action in relation to their personal information, for example, a use or a disclosure.

Directly related purpose is a secondary purpose that is closely associated with the primary purpose of information collection.

Disclosure refers to the provision of personal information to a third party external to the University. Provision of information internally may also be considered a disclosure where the provision of information is not for the primary purpose, not for a directly related purpose or not otherwise permitted by this Directive, the Privacy Management Plan (PDF) or by law. This is particularly relevant to health information.

Emergency situation refers to an immediate threat to either persons or property and, for the purposes of this Directive, where it is believed that a use or disclosure of personal information is necessary to prevent or lessen a serious and imminent threat to the life or health of the individual or another person. In relation to health information, this includes where it is necessary to prevent or lessen a serious or imminent threat to public health and safety.

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

This is covered in more detail in the Privacy Management Plan (PDF). For the purposes of this Directive, the use of the term 'personal information' includes health information unless otherwise specified.

Information systems refers to any system that collects, creates or captures and stores information, including but not limited to electronic databases, data or business systems and paper recordkeeping systems.

Internal review is a review required under PPIPA into a complaint regarding an alleged breach of a privacy principle.

Official record (**or record**) as defined in the Records Management Vice-Chancellor's Directive.

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

The Privacy Management Plan (PDF) covers personal information in more detail. For the purposes of this Directive, the use of the term 'personal information' includes health information unless otherwise specified.

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

Privacy notice refers to a notice or statement which defines for a particular circumstance what personal information is being collected, the purpose of the collection, how the information will be used, whether it will be disclosed and to whom, and any other conditions relating to the provision or non-provision of information (see section 5.2.3 in this Directive).

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

Sensitive personal information is a subset of personal information, and is information about a person's ethnic or racial origin, sexual activities, religious or philosophical beliefs, political opinions or trade union membership. There are special restrictions in relation to the disclosure of sensitive personal information.

Third party means another individual, organisation or agency. Examples include another university, a government agency, an agent, a family member, friend, legal representative, a company engaged to undertake work on behalf of UTS.

Unsolicited information refers to personal information received by UTS:

- that was not actively collected (eg via a paper or online form)
- that was not collected as a by-product of an automated system (eg location data, login details), or
- where there was no system and/or procedure in place to facilitate its receipt (eg feedback processes).

Use in relation to the use of personal information refers to the application of information to undertake or facilitate a particular activity. Uses of personal information may be for primary purposes or a directly related purpose.

4. Directive principles

The following principles underpin the University's commitment to privacy and the protection of personal information it collects, holds and manages:

- appropriate collection of personal information
- protecting personal information from loss or misuse
- reasonable and authorised use or disclosure of personal information in all circumstances
- appropriate retention and destruction or deletion of personal information
- creating and promoting a culture of privacy across the University community and incorporating privacy requirements into processes, procedures and information systems which deal with personal information
- engendering a relationship of trust between the University and individuals in line with our values.

5. Directive statements

The Privacy Management Plan (PDF) provides further detail on the implementation of this Directive and should be used in combination with the following statements.

5.1 Privacy responsibilities

5.1.1 Staff and students

All staff and students, including contractors, are responsible for complying with privacy obligations outlined in this Directive, and are required to cooperate in full with the investigation of any complaint or other privacy related matter.

5.1.2 Senior Executive, deans, directors, and business unit heads

Members of the Senior Executive, deans, directors and business unit heads are accountable for the activities within their respective faculties and units, and are required to ensure that:

- they are aware of privacy requirements and advocate good privacy practices across the business units and staff under their direction
- business units, staff and contractors under their direction comply with privacy policies and procedures, noting specific requirements may be imbedded in other UTS governance instruments
- appropriate privacy impact assessments are undertaken on any new activities or projects that deal with personal information or may have the potential to impact on individual privacy
- informal privacy complaints received by their area are appropriately handled in consultation with the UTS Privacy Officer, and
- privacy training and education is supported to foster knowledge and development of expertise with respect to their particular functions and activities.

5.1.3 Governance Support Unit

The Governance Support Unit coordinates and maintains the privacy program at UTS. This includes:

- delegating the role of UTS Privacy Officer
- developing and delivery of the privacy training program
- developing and maintaining this Directive, the Privacy Management Plan (PDF), the Privacy at UTS website and University-wide privacy practices
- providing advice and assistance in the development of activity-specific governance instruments and privacy notices, in consultation with faculties and units, and
- investigating privacy complaints and internal review requests in line with legislative requirements.

5.1.4 Contracted third parties

Contracted third parties are responsible for adhering to the privacy obligations specified in their contracts with the University. They are also required to comply with directions provided by UTS in relation to the information they have access to or manage on behalf of the University.

5.2 Collecting personal information

5.2.1 Purpose of personal information collection

Personal information may only be collected for a lawful purpose where it is directly related to the University's functions and activities and necessary for that purpose.

5.2.2 Source of personal information collection

Personal information will be collected from the individual it relates to, unless consent has been provided to collect from another individual or party, or it is collected from a parent or legal guardian of a minor.

5.2.3 Openness and privacy notices

A relevant and up-to-date privacy notice is required as part of collection activities to facilitate openness and transparency. A privacy notice defines the obligations of the University and the individual's privacy rights by informing them about what information is being collected, why it is being collected, who will be storing and using it, whether it will be disclosed (to whom and why), and how individuals can access or correct their information. Where possible, notices should be accessible or provided to individuals before information is collected.

5.2.4 Collecting relevant personal information

Personal information collected must be relevant to and not excessive for the purpose it is being collected for. Reasonable steps are required to ensure that information collected is accurate and up-to-date at the time it is collected.

Where it is not necessary to identify who information relates to, such as with a survey, personal information should be collected in such a way so as to ensure an individual cannot be identified from the collected information.

5.2.5 Implementing new personal information collection activities

When undertaking or initiating a new personal information collection activity, the relevant dean, director or business unit head must authorise the collection and ensure it is undertaken in line with this Directive. This includes undertaking a privacy impact assessment (see section 5.11).

5.2.6 Changes to existing information collection activities

When changing an existing personal information collection activity, a privacy impact assessment should be undertaken to ascertain how proposed changes will affect the collection, security, storage, use or potential disclosure of personal information before the changes are approved or initiated. It should be noted that approved changes may impact the privacy notice (see section 5.2.3).

5.2.7 Unsolicited personal information

Unsolicited information received by UTS in the course of its activities is not deemed to have been collected by UTS. The requirements covering collection of information under section 5.2 do not apply, however the remainder of this Directive does apply.

5.3 Storing personal information

The University is required to ensure personal information is stored securely, is not kept longer than necessary and is protected from loss, unauthorised access, use or disclosure.

5.3.1 Secure storage of personal information

Information system owners are responsible for ensuring that suitable measures are in place to protect the personal information held within their systems.

For University-wide information systems which are accessible by different business units but not centrally managed, each business unit is responsible for the appropriate use and implementation of the system locally.

Personal information that is considered part of the official record of the University must be managed in line with the University's Records Management Vice-Chancellor's Directive.

In cases where personal information collected by the University will be stored externally to the University, a privacy impact assessment is required.

5.3.2 Storing personal information outside UTS

UTS may store data outside the University for the effective and efficient management of its resources and activities. A privacy impact assessment is required before engaging such services (see also section 5.7.3 for specific restrictions on transferring health information outside New South Wales). An IT security risk assessment may also be required.

5.3.3 Access to information systems

Information system owners are responsible for establishing appropriate system access controls to ensure that personal information can only be accessed and amended by staff who require such access as part of their role at UTS.

5.3.4 Retaining and destroying personal information

Business units must only retain personal information for as long as the information is required to support the purpose for which it was collected and as mandated by legal retention requirements.

The destruction or deletion of any personal information (whether in digital, paper or other media or formats) must be undertaken in a secure manner. For official records and recordkeeping metadata, destruction authorisation is required in accordance with the Records Management Vice-Chancellor's Directive.

5.4 Access and accuracy

UTS must explain to individuals what personal information is held about them, how it will be used and any rights they have to access it.

Individuals have a right to access their personal information without excessive delay or expense, as required by PPIPA.

UTS must allow individuals to update, correct or amend their personal information where necessary and appropriate.

5.5 Use of personal information

Personal information is to be relevant and accurate before it is used.

Personal information can only be used for the primary purpose for which it was collected or a directly related purpose, or where the individual provides consent.

Personal information may also be used where it is considered necessary in an emergency situation (see section 5.8).

5.6 Disclosing personal information

5.6.1 Limits on disclosing personal information

Personal information can only be disclosed for the primary purpose for which it was collected and as indicated to the individual at the time of collection, or for a directly related purpose where there is no reason to believe the individual concerned would object to the disclosure.

In relation to health information, a directly related purpose is one that an individual would reasonably expect.

Personal information may also be disclosed where it is considered necessary in an emergency situation (see section 5.8).

5.6.2 Disclosing sensitive personal information

Sensitive personal information may only be disclosed for the primary purpose for which it was collected, or where it is considered necessary in an emergency situation (see section 5.8).

5.7 Additional requirements for managing health information

In addition to the statements outlined above, the following statements apply to the management of health information.

5.7.1 Using numbers or codes to identify an individual's health information

Unique identifiers are sometimes used in the storage of health information to enhance privacy. UTS will only use unique identifiers where necessary to carry out the University's functions efficiently. Further information is provided in the Privacy Management Plan (PDF).

5.7.2 Anonymous health services

Where lawful and practical to do so, individuals may be given the option to receive health-related services anonymously.

5.7.3 Transferring health information outside New South Wales

Health information can only be transferred outside New South Wales where:

- the individual consents to the transfer
- the information is sent to a jurisdiction with a similar standard of privacy protection
- the transfer is for the benefit of the individual and, if not practicable to gain consent, it is believed the individual would have given consent
- the transfer is required to comply with contractual requirements between the individual and the organisation
- the transfer is required by law, or
- it is necessary in an emergency situation (see section 5.8).

5.7.4 Participating in health records linkages systems

An individual must provide written consent before their information is included in a computerised system that is designed to link their health records with those of other organisations for the purpose of facilitating access to those health records.

5.8 Using or disclosing personal information in an emergency situation

Approval for the immediate use or disclosure of information in emergency situations must be obtained from the Vice-Chancellor, Provost or Deputy Vice-Chancellor (Corporate Services), or from one of the following staff members in relation to the information they have responsibility over:

- Director, Student Administration Unit; Director, Student Services Unit; or Deputy Vice-Chancellor (Education and Students) in relation to current, past or prospective students
- Director, Human Resources, in relation to current, past or prospective staff or volunteers, or
- any other member of the Senior Executive in relation to information that falls under their portfolio.

5.9 Exemptions to privacy principles

There are exemptions to the privacy principles defined under sections 5.2–5.8 of this Directive. UTS may also be exempt from these requirements if required or permitted by law. Exemptions are only to be applied where assessed as appropriate in the circumstances and in line with the Privacy Management Plan (PDF).

5.10 Outsourcing and contracting services

Where a third party is contracted to undertake a function or activity on behalf of UTS (such as IT support, companies hosting information systems or storing data, mailing houses or agents), the work undertaken is, in effect, work of the University. The University's privacy obligations apply to the contracted third party and need to be incorporated into the contractual obligations.

5.11 Privacy impact assessments

A privacy impact assessment is required when a proposed new activity or change to an existing activity or process is likely to affect an individuals' privacy or involves personal information. The Privacy Management Plan (PDF) covers privacy impact assessments in more detail.

5.12 Complaints and breaches

5.12.1 Informal complaints

Informal complaints relating to the management of personal information should be referred to the relevant director or dean in the first instance. The director or dean must advise the complainant of their rights to request an internal review of any alleged breach of their privacy. It is recommended that the business unit consult with the UTS Privacy Officer in dealing with such complaints. Further information about the complaints process is available in the Privacy Management Plan (PDF).

Official records need to be filed on complaints handling activities at a faculty/unit level.

5.12.2 Internal reviews

Where an informal complaint does not provide a satisfactory outcome or a complaint is made under privacy legislation, this will be viewed as a request for an internal review. Such complaints must be forwarded to the UTS Privacy Officer.

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.

Refer to the Privacy Management Plan (PDF) for further information about the internal review process at UTS.

5.12.3 Disclosure of personal information in error

Unauthorised access to personal information must be reported to the UTS Privacy Officer and, where relevant, to the responsible owner of the information system concerned.

The Privacy Management Plan (PDF) specifies how erroneous disclosures and data breaches will be managed.

5.12.4 Corrupt conduct and Directive breaches

Breaches of this Directive (identified through an informal complaint, internal review or through other means) are considered a failure to comply with the University's Code of

Conduct and will be dealt with under section 4.11 (Failure to comply with the Code). This includes the right of UTS to notify a relevant statutory authority and/or agency where breaches of relevant legislation may be evident.

Where a breach falls under the provisions of the Fraud and Corruption Prevention and Public Interest Disclosures Policy, the issue should be reported directly to a nominated disclosure officer designated in Schedule 1 of the Fraud and Corruption Prevention and Public Interest Disclosures Guidelines.

6. Roles and responsibilities

Accountable Officer: The Deputy Vice-Chancellor (Corporate Services) is the officer responsible for managing Directive compliance and initiating the Directive review process (at least every five years).

Implementation Officer: The Director, Governance Support Unit is the primary point of contact for advice on implementing and administrating the Directive, and managing the consultation and review process.

Other positions: The Implementation Officer will appoint and delegate responsibility for some or all of these activities to the UTS Privacy Officer. The Implementation Officer may also appoint a Privacy Contact Officer to assist the UTS Privacy Officer in undertaking these duties.

7. Acknowledgements

Information and Privacy Commission NSW

8. Version control and change history

Effective date	Version	Approved by (date)	Amendment
24/06/2015	1	Vice-Chancellor (29/05/2015)	New Privacy Vice-Chancellor's Directive drafted to replace the 2010 Privacy and Protection of Personal Information Vice-Chancellor's Directive.