

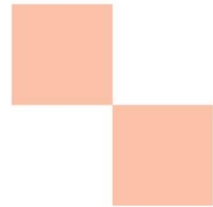


UTS
College

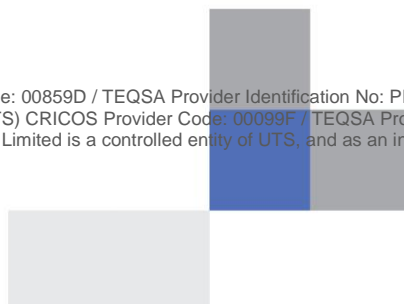
UNIVERSITY
OF TECHNOLOGY
SYDNEY

Privacy Management Plan

September 2023



UTS College Limited ABN 39 001 425 065 | CRICOS Provider Code: 00859D / TEQSA Provider Identification No: PRV12022, Provider Category: Institute of Higher Education. University of Technology Sydney (UTS) CRICOS Provider Code: 00099F / TEQSA Provider Identification No: PRV12060, Provider Category: Australian University. UTS College Limited is a controlled entity of UTS, and as an institute of higher education, UTS College Limited provides pathway courses to UTS.



CONTENTS

1	INTRODUCTION	3
2	SCOPE	3
3	DEFINITIONS.....	4
4	PRIVACY PRINCIPLES.....	5
5	PERSONAL INFORMATION	7
6	REQUIREMENTS OF THE PLAN	7
7	UTS COLLEGE USE OF PERSONAL INFORMATION.....	7
8	POLICIES, PRACTICES AND CONTROLS.....	10
9	DISSEMINATION OF POLICIES AND PRACTICES	13
10	INTERNAL REVIEW PROCEDURES	14
11	PRIVACY AND PROTECTION OF PERSONAL INFORMATION	16
12	RELATED LEGISLATION	16
	APPENDIX A: ABOUT THE PRIVACY LAWS	17



1 INTRODUCTION

Insearch Limited (**UTS College**) is a commercial provider of higher education. Its main operation is the provision of pathway programs for domestic and international students preparing to enter degree programs at UTS, and through its joint venture arrangements provides English language programs for overseas students.

UTS College must comply with its applicable obligations under the following legislative regimes:

- [Privacy Act 1988 \(Cth\)](#) (the **Privacy Act**) and its Australian Privacy Principles (**APPs**)
- [Privacy and Personal Information Protection Act 1998 \(NSW\)](#) (the **PPIP Act**) and its Information Privacy Principles (**IPPs**); and
- [Health Records and Information Privacy Act 2002 \(NSW\)](#) (the **HRIP Act**) and its Health Privacy Principles (**HPPs**).

Under section 33 of the PPIP Act, UTS College is required to have an established Privacy Management Plan and in accordance with section 33-5, a copy has been lodged with the NSW Privacy Commissioner.

The UTS College Privacy Management Plan (**Plan**) informs our stakeholders and staff how we manage personal information and explains who a person can contact questions about the personal or health information we hold, how they can access and amend their information and what to do if they think UTS College may have breached the PPIP Act or the HRIP Act. It is also used as a staff training tool.

All staff and students, and any person employed or engaged by UTS College, its representative offices, and its controlled entities, are required to comply with the legal obligations of privacy, and personnel working in areas most likely to have access to or be exposed to personal or sensitive information must ensure that such information is safeguarded. However, everyone is expected to respect each other's privacy, maintain confidentiality, and comply with the APPs.

The APPs and Privacy Act address the collection, storage, security, use and disclosure of personal and health information, and establish the standards for collecting and dealing with personal information to eliminate the risk of misuse of that information. The APPs also allow individuals to exercise control over what happens to their own personal information.

Please refer to Appendix A for more information about the APPs and Privacy Act, and other privacy-related legislation.

Section 41 of the PPIP Act (*Directions*): the NSW Privacy Commissioner provides public interest directions that can be obtained from the Information and Privacy Commission NSW [website](#).

This Plan has been developed in line with the Information and Privacy Commission New South Wales: [A Guide to Making Privacy Management Plans 2022](#). This Plan is reviewed every 5 years, or in the event of any legislative, administrative, or systemic changes.

2 SCOPE

This Plan applies to;

- UTS College board of Directors
- UTS College, its representative offices, and its controlled entities, employees and affiliates
- UTS College students and student bodies
- Education agents
- joint venture partners and education affiliates
- consultants and contractors of UTS College; and
- conjoint and visiting appointees.



Board of Directors

Under UTS College's corporate governance framework, which incorporates all relevant statutory requirements and legal obligations, the board of Directors, acting in their capacity as Directors for UTS College, will comply with the PPIP Act and APPs.

UTS College employees

UTS College's employees, when acting in their capacity as employees of UTS College, will comply with the PPIP Act and APPs.

Where UTS College regards information concerning its employees as personal information in respect of the PPIP Act and the Privacy Act, it will treat such personal information in accordance with applicable laws.

UTS College students and student bodies

UTS College regards all personal information (as defined under the applicable legislation) concerning its students as information protected by the PPIP Act and APPs.

Education agents

All education agents must abide by the PPIP Act and APPs under the terms of their contracts with UTS College.

Consultants and private contractors of UTS College.

UTS College may employ consultants directly to perform a specific function; or contract services in whole or in part to private contractors including data service providers. Private contractors and consultants must abide by the PPIP Act and APPs under the terms of their contracts with UTS College.

Joint venture partners and educational affiliates

UTS College currently has agreements or partnerships with:

- University of Technology Sydney
- Shanghai University, Sydney Institute of Language and Commerce
- Education International Cooperating Limited (China)
- Guangha Education Group (China)
- IDP Education (Vietnam) Ltd – Australian Centre of Education & Training (Vietnam)
- UniSadhuGuna International College (Indonesia)
- International Education Network Inc (South Korea)
- Australian Education Centre (Myanmar)
- Gujarat Law Society University (India)
- Premier University (Bangladesh).

UTS College will ensure that these bodies comply with their respective obligations under the PPIP Act and APPs so far as it is practicable.

3 DEFINITIONS

Personal Information	Any information or opinions (including forming part of a database and whether or not recorded in a material form) about a person where that person's identity is apparent or can be reasonably ascertained, as defined in section 6(1) of the Privacy Act and section 4 of the PPID Act, including a person's name, address, student number, video recordings and photographs of an individual, and electronic records.
Personal Information held by UTS College	Personal information is held by UTS College when: <ul style="list-style-type: none">▪ it is in possession or control of the information.



	<ul style="list-style-type: none"> ▪ the information is in the possession or control of a person employed or engaged by UTS College in the course of such employment or engagement; or ▪ the information is contained in a State record for which UTS College is responsible under the <i>State Records Act 1998</i> (NSW).
Sensitive Information	<p>Sensitive Information has the definition given to that term under section 6(1) of the Privacy Act, and includes race or ethnicity, union membership, sexual preference, and medical conditions.</p> <p>The degree of sensitivity of the personal information may influence the way in which the information protection principles are applied. The more sensitive the nature of the information, the higher the level of care should be used by staff when dealing with the information, particularly where disclosure to a third party is being considered.</p>
Privacy and Confidentiality	<p>Privacy applies to personal information, irrespective of who provided it to UTS College. It relates to an individual's ability to control the extent to which their personal information, enabling identification, is available to others.</p> <p>Confidentiality restricts UTS College from using or disclosing some information in a way which is contrary to the interests of the person or organisation that provided it in the first place. Confidentiality is defined as a mode of managing private information, by the restriction of access to information to authorised persons, entities and processes at authorised times, in an authorised manner.</p>
Use and Disclosure of Personal Information	<p>Information protection refers to the treatment and handling of personal information within an organisation, particularly when this involves making decision on the basis of the information.</p> <p>Disclosure refers to making personal information available to people outside the organisation, other than to the individual concerned and includes the publication of personal information.</p>
Health Information	<p>Specific type of information as defined in section 6 of the HRIP Act. Health information can include, among other things, information about a personal's physical or mental health, or information about a person's medical appointment.</p>

4 PRIVACY PRINCIPLES

Information Protection Principles (IPP)

Part 2 Division 1 of the PPIP Act (NSW) includes 12 IPPs that all agencies must comply with. Sections 8-19 of the Act detail each one of the IPPs named as follows:

Section 8 - Collection of personal information for lawful purposes

Section 9 - Collection of personal information directly from individual

Section 10 - Requirements when collecting personal information.

Section 11 - Other requirements relating to collection of personal information.

Section 12 - Retention and security of personal information

Section 13 - Information about personal information held by agencies.

Section 14 - Access to personal information held by agencies.

Section 15 - Alteration of personal information

Section 16 - Agency must check accuracy of personal information before use.

Section 17 - Limits on use of personal information

Section 18 - Limits on disclosure of personal information



Section 19 - Special restrictions on disclosure of personal information

A detailed description of the IPPs is provided in [Appendix A](#).

Australian Privacy Principles (APPs)

UTS College is considered to be an “agency” pursuant to the *Privacy Act* (Cth), and therefore must comply with the private sector principles, namely the APPs from Schedule 1 of the Privacy Act.

There are 13 APPs that came into effect on 12 March 2014 and apply to UTS College.

APP 1 — Open and transparent management of personal information

Ensures that APP entities manage personal information in an open and transparent way. This includes having a clearly expressed and up to date privacy policy.

APP 2 — Anonymity and pseudonymity

Requires APP entities to give individuals the option of not identifying themselves, or of using a pseudonym. Limited exceptions apply.

APP 3 — Collection of solicited personal information.

Outlines when an APP entity can collect personal information that is solicited. It applies higher standards to the collection of ‘sensitive’ information.

APP 4 — Dealing with unsolicited personal information.

Outlines how APP entities must deal with unsolicited personal information.

APP 5 — Notification of the collection of personal information

Outlines when and in what circumstances an APP entity that collects personal information must notify an individual of certain matters.

APP 6 — Use or disclosure of personal information

Outlines the circumstances in which an APP entity may use or disclose personal information that it holds.

APP 7 — Direct marketing

An organisation may only use or disclose personal information for direct marketing purposes if certain conditions are met.

APP 8 — Cross-border disclosure of personal information

Outlines the steps an APP entity must take to protect personal information before it is disclosed overseas.

APP 9 — Adoption, use or disclosure of government related identifiers

Outlines the limited circumstances when an organisation may adopt a government related identifier of an individual as its own identifier or use or disclose a government related identifier of an individual.

APP 10 — Quality of personal information

An APP entity must take reasonable steps to ensure the personal information it collects is accurate, up to date and complete. An entity must also take reasonable steps to ensure the personal information it uses or discloses is accurate, up to date, complete and relevant, having regard to the purpose of the use or disclosure.

APP 11 — Security of personal information

An APP entity must take reasonable steps to protect personal information it holds from misuse, interference and loss, and from unauthorised access, modification or disclosure. An entity has obligations to destroy or de-identify personal information in certain circumstances.

APP 12 — Access to personal information



Outlines an APP entity’s obligations when an individual requests to be given access to personal information held about them by the entity. This includes a requirement to provide access unless a specific exception applies.

APP 13 — Correction of personal information

Outlines an APP entity’s obligations in relation to correcting the personal information it holds about individuals.

5 PERSONAL INFORMATION

Under the PPIP Act and APPs, personal information means “information or an opinion (including forming part of a database and whether or not recorded in a material form) about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion”.

Section 4.3 of the PPIP Act specifies what is not considered personal information that includes, for example, information that is contained in a publicly available publication, information about an individual who has been dead for more than 30 years, information contained in a public interest disclosure.

6 REQUIREMENTS OF THE PLAN

In accordance with the PPIP Act, for a public sector agency, this Plan includes information relating to:

- (a) established policies and practices to ensure compliance with the requirements of the PPIP Act.
- (b) the systems and processes for dissemination of policies and practices to relevant stakeholders and persons within UTS College.
- (c) the established internal review procedures under Part 5 of the PPIP Act.
- (d) all other relevant matters in relation to privacy and the protection of personal information held by UTS College.

7 UTS COLLEGE USE OF PERSONAL INFORMATION

DEPARTMENT/ROLE	KEY FUNCTIONS	MAIN USE OF PERSONAL INFORMATION
Sales and marketing	<ul style="list-style-type: none"> ▪ Responsible for the recruitment of students into all of our courses, both directly and indirectly through our global network of education agents ▪ Activities include managing the UTS College brand, publications, surveys, promotional campaigns, PR activities, advertising campaigns, education agent management, provision of course information, and maintenance of prospect database 	<ul style="list-style-type: none"> ▪ Publishing ▪ Filming ▪ Photography ▪ Media ▪ Ambassador programs ▪ Direct marketing ▪ Prospect management and contact
Education agents	<ul style="list-style-type: none"> ▪ Management of applications from international students who wish to enrol at UTS College and UTS 	<ul style="list-style-type: none"> ▪ Prospect management and follow-up ▪ Application process ▪ Compliance with the Department of Home Affairs requirements
Student centre	<ul style="list-style-type: none"> ▪ Student’s face to face service/support ▪ Homestay service ▪ Changes/updates on students’ information 	<ul style="list-style-type: none"> ▪ Assisting with student visas, health cover and whole application process
Student admissions	<ul style="list-style-type: none"> ▪ Management of student admission 	<ul style="list-style-type: none"> ▪ Student applications

DEPARTMENT/ROLE	KEY FUNCTIONS	MAIN USE OF PERSONAL INFORMATION
	<ul style="list-style-type: none"> ▪ Maintenance of student records ▪ Maintenance of student files ▪ Management of student incidents ▪ Management of critical incidents 	<ul style="list-style-type: none"> ▪ Emergency contact information ▪ Tax file number management (for Fee-Help purposes)
Student administration	<ul style="list-style-type: none"> ▪ Timetabling and Enrolment ▪ Maintenance of student records ▪ Maintenance of student files ▪ Student activities and events ▪ Graduation events 	<ul style="list-style-type: none"> ▪ Dissemination of exam results, transcripts, testamurs. ▪ Financial information of students
Student advisers	<ul style="list-style-type: none"> ▪ Support to students in academic progress and personal challenges ▪ Assisting students to overcome adaptableness difficulties 	<ul style="list-style-type: none"> ▪ Monitoring student progression and support ▪ Assessment and review of students with sanctions
Teaching programs (ELT, Diploma and Foundation Studies)	Teaching, tutoring and assessment of students	<ul style="list-style-type: none"> ▪ Student assessment ▪ Course and subject lists ▪ Assessment and review of students ▪ Monitoring of student progression
Student Support Services	Student discipline and appeals	<ul style="list-style-type: none"> ▪ Handling complaints and student appeals ▪ Assessment of applications for special consideration ▪ Assistance for students with special needs ▪ Handling of grievance complaints
People	<ul style="list-style-type: none"> ▪ Recruitment ▪ Remuneration & benefits ▪ Talent management and development ▪ Employee relations ▪ Workplace health & safety for staff 	<ul style="list-style-type: none"> ▪ Employment screening to check and verify work history, qualifications and experience, immigration status, clearance to work with children and at times police records. ▪ Producing employment-related contracts ▪ Setting and administering individual salaries and benefits ▪ Managing performance and development ▪ Handling employment relations, staff complaints and grievances ▪ Staff health and wellbeing matters including workers compensation ▪ Reporting on people metrics
Payroll	<ul style="list-style-type: none"> ▪ The collation, processing, and administration of information in order to ensure staff are remunerated 	<ul style="list-style-type: none"> ▪ Creation of online personnel records. ▪ Arranging salary payments and lodgement into

DEPARTMENT/ROLE	KEY FUNCTIONS	MAIN USE OF PERSONAL INFORMATION
	through salary, superannuation, incentive and benefit payments. <ul style="list-style-type: none"> ▪ Taxation management ▪ Coordination and security of personnel records and files 	financial and other institutions such as superannuation providers <ul style="list-style-type: none"> ▪ Business and management reporting ▪ The provision of personal and sensitive information where authorised
ITDS	<ul style="list-style-type: none"> ▪ Staff personal contact details and profiles ▪ Student profiles ▪ Management of BI data 	<ul style="list-style-type: none"> ▪ Allocation of laptops or other technical devices to staff ▪ Audits on student/staff use of systems ▪ Granting of access to systems (including Internet)
Executive and managers	<ul style="list-style-type: none"> ▪ Information of direct report staff used in managing the business. ▪ Remuneration and benefits 	<ul style="list-style-type: none"> ▪ Management of staff ▪ Performance management ▪ Professional development and review
Governance	<ul style="list-style-type: none"> ▪ Whistleblowing Policy ▪ Board and Audit & Risk Committee registers 	<ul style="list-style-type: none"> ▪ Maintain anonymity and confidentiality as required ▪ Personal and contact details ▪ Contract management
Finance department	<ul style="list-style-type: none"> ▪ Management of UTS College's financial resources, including accounting systems and payroll 	Payment of staff salaries and benefits
Facilities	<ul style="list-style-type: none"> ▪ Monitor the video surveillance ▪ Supplier details ▪ Engaging contractors ▪ Document storage and destruction 	<ul style="list-style-type: none"> ▪ Safety and security of building occupants ▪ Induction of Contractors
Joint venture partners educational affiliates	<ul style="list-style-type: none"> ▪ Monitoring potential students and offering information about courses ▪ Management of applications from overseas students who wish to enrol at UTS College and possibly UTS ▪ Staff personal information and salary information 	Partners/Affiliates must not disclose to any person, other than UTS College, any student's personal information unless that person has: <ul style="list-style-type: none"> ▪ given their written consent to such disclosure; ▪ been provided with the Privacy Notification Form prior to the collection of the personal information and the person is an intended recipient; or ▪ the disclosure is one which is otherwise authorised by the PPIP Act or other law. The obligation on the partners/affiliates under this clause must not be taken to have been breached where the information referred to is legally required to be

DEPARTMENT/ROLE	KEY FUNCTIONS	MAIN USE OF PERSONAL INFORMATION
		disclosed, provided the partners/affiliates notify UTS College immediately the request for disclosure is made. Should UTS College object to the making of the disclosure, the partners/affiliates must abide by that objection. A failure by UTS College to notify any objection must not operate to relieve the partners/affiliates of any obligation at law or create any obligation on the part of UTS College

Note: When a company or other agency contacts UTS College to verify if a prospective employee is an UTS College graduate, UTS College will confirm:

- a) if the person is or is not a graduate;
- b) the education level completed; and/or
- c) the program finalised.

This information is made publicly available at graduation ceremonies and is not considered personal information under the PPIP Act and Privacy Act.

8 POLICIES, PRACTICES AND CONTROLS

UTS College has implemented a [Privacy Policy](#) for students and staff in response to its commitment to the PPIP Act and APPs that addresses the collection, storage, security, access and accuracy, use and disclosure of personal information from individuals. The Privacy Policy is available on the Staff Intranet, Student Extranet and UTS College public website.

The [Privacy Statement](#) is also located in the Staff Intranet, Student Extranet and UTS College public website.

This Plan underpins the learning material which is included as part of the staff orientation process, privacy training sessions, and other staff training.

8.1 Code of Ethics

The UTS College board of directors strongly supports and promotes ethical and responsible decision making and operates within a [Code of Ethics](#) that sets out the core values UTS College applies in achieving its purpose. The Code provides the framework for individuals and groups of people to engage in ethical decision-making within the organisation.

UTS College is committed to being an established, international, commercial provider of higher education, operating with integrity, honesty, courage, compassion, respect and imagination, and expects its staff to perform with integrity, honesty and respect in professional, academic and personal matters, and to comply with the UTS College [Code of Ethics](#) and Code of Conduct.

The Code of Ethics is included in all key internal and external publications for students, staff, education agents and other stakeholders; it is part of the UTS College culture and is applied by staff in the conduct of UTS College business.

8.2 Code of Conduct

UTS College has a Code of Conduct that explains the principles of behaviour UTS College expects of its employees whilst at work and when representing UTS College in the course of work or at related



events. It specifically addresses privacy and confidentiality matters. The Board of Directors, Executive, managers and all employees are expected to abide by the Code of Conduct. Any suspected breach is treated seriously, fully investigated, and may result in disciplinary action.

The Code of Conduct is provided to all new staff with their Employment Offer, is a condition of employment, reinforced during regular Staff Orientation sessions and is accessible on both the website and staff intranet. All staff are required to verify their compliance with the Code of Conduct on an annual basis.

The Code of Conduct is reviewed periodically and was last updated in 2021.

8.3 Employees' responsibility

It is the responsibility of all employees to understand and comply with key principles and obligations in respect of privacy.

All employees are expected to act in a professional and ethical manner, comply with internal privacy control requirements, policies, and procedures, and follow legal requirements, with a view to maintaining and enhancing the reputation of UTS College.

It is expected that employees recognise signs of potential breaches of privacy, confidentiality issues and lack of discretion, and report these to their respective manager or a senior manager. Employees are also expected to assist with any enquiries and investigations pertaining to privacy breaches and associated misconduct.

Members of the Executive and managers must raise awareness of the privacy amongst staff through team meetings, and ensure training, induction or orientation programs are exercised.

8.4 Compliance Management Program

To comply with the IPPs, APPs and HPPs, applicable laws, regulations, codes and the organisation's standards, UTS College has implemented a risk-based compliance management program.

By implementing compliance management systems, UTS College aims to limit the risk of breaches of legislative requirements and adverse audit findings, including privacy issues or breaches that can have financial and non-financial implications for the organisation.

Related policy and procedure include Compliance Management Program, Compliance Reporting Register, Policy and Procedure Development Policy, Fraud and Corruption Control Plan, Risk Management Policy, Information Classification Policy, Records Retention and Destruction Policy and Procedure. To the extent such policies are public facing, these documents are available on the Policy and Procedures website.

Specific controls include: primary privacy contact, a dedicated privacy email address; the internal audit program; staff training; roles and responsibilities of board and committees, the Executive and all managers; the annual compliance reporting procedure, compliance management reports to the Audit & Risk Management Committee addressing changes in obligations, incidents and corrective action, training & communication activity, implemented compliance controls; managing non-compliance through operational level management processes and remedial action.

8.5 Other legal requirements affecting privacy

As part of the Recruitment Procedure, criminal record checks are required of holders of nominated positions at UTS College. These checks are conducted through the appropriate regulatory body.

8.6 Compliance with public register provisions

UTS College does not hold or maintain any public registers.

8.7 Privacy officer

Privacy is the responsibility of all staff and stakeholders at UTS College. Initial inquiries about information held is usually managed by the manager of the department that holds the information,



however, UTS College has a nominated Privacy Officer as the main contact for staff and students to deal with privacy matters.

The Privacy Officer will handle requests from staff or students for access to personal files held and will monitor compliance.

Contact details:

THE PRIVACY OFFICER
 UTS College Limited
 Level 13, UTS Building 10 (CB1) 235 Jones Street
 Broadway NSW 2007
 [E] privacy@insearch.edu.au

8.8 Responsibilities of the Privacy Officer

To ensure compliance with PPIP Act and APPs, the Privacy Officer will review internet contact forms, rates notices, application forms of whatsoever nature, or written requests by which personal information is collected.

The Privacy Officer will also provide advice as to:

- a) whether the personal information is collected for a lawful purpose
- b) if that lawful purpose is directly related to a function of UTS College; and
- c) whether or not the collection of that personal information is reasonably necessary for the specified purpose.

Any further concerns of a legal nature will be referred to UTS College’s legal advisers.

Concerning the general implementation of the Plan, the Privacy Officer will ensure that student enrolment forms:

- a) note the commencement of the new PPIP Act and APPs
- b) state that UTS College holds personal information.
- c) note that UTS College may use and disclose personal information in various circumstances; and
- d) state that for further information, the Privacy Officer should be contacted.

The Privacy Officer may recommend the assigning of designated officers as “Privacy Resource Officers” within the larger departments of the organisation. In this manner UTS College can ensure the information protection principles are more broadly understood and that individual departments have a greater focus on the information protection principles as they may be directly applied into day-to-day functions.

8.9 Classes of personal information

Type of record	Personal information held in record
Student records – maintained in hardcopy files and on student database, includes past students	Personal details (name, address, phone), date of birth, previous education, Aboriginality, country of origin, subjects, marks/grades; may include special entry application details, special needs details, discipline reports, grievance reports, progress reports, special consideration applications, withdrawal details, tax file number, fees and debts, emergency contact information
Staff files – maintained in Affinity and on SharePoint	Personal details, date of birth, employment application, CV, previous employment details, referee reports, employment contract, medical details, salary and banking details, performance reviews, performance and conduct information, leave applications, medical certificates, EEO details, tax file number, emergency contact information, union membership



Student and staff surveys	Personal details, personal views and comments
Alumni Records	Personal details
Medical Records	Personal details, confidential health details
Subject folders	List of students; assignments identified by student name and ID, assignment mark and comments
Graduate lists	Names (mailing address in some instances), course
Grievance records	Personal details, statements, summary of grievance and outcome
Pay records – maintained in hardcopy and on database	Personal details, salary, banking and deduction details, tax file number
Supervisor files	Personal details, progress reports on students
Homestay Service files	Personal details, next of kin, smoker/non-smoker status, application may contain confidential personal information (e.g., health details, hardship) Homestay family personal details
Workers' compensation files	Personal and claim details, related medical information, medical reports, medical certificates, rehabilitation plans and progress reports
Company registers	Personal information of Directors and committee members

9 DISSEMINATION OF POLICIES AND PRACTICES

Internal training programs, and public awareness information comprise the following elements:

- legislative requirements under the PIPP Act, APPs and HRIP Act
- the fact that corrupt disclosure or use of personal information is a criminal offence
- the need to appoint members of staff as Privacy Resource Officers, where appropriate
- the need to attend to areas where breaches are more likely (such as inadequate security for staff and student files or failure to dispose of personal information that is no longer in use)
- all new staff are informed about Privacy in their employment contract, orientation and as part of a mandatory online course
- information about Privacy is on the UTS College Staff [intranet](#) and [website](#)
- regular updates and reminders about Privacy requirements are disseminated across the organisation and to specific units.

These activities are coordinated by the Privacy Officer and will be included in the compliance training program currently under development. In addition, some units conduct local privacy and confidentiality sessions to address specific work needs and matters.

9.1 Privacy training and education

Staff are required to attend training or awareness sessions to understand Privacy as it relates to their role, and to prevent any breaches due lack of information and/or knowledge. Supervisors and managers of staff who have high level involvement in work practices directly related to privacy matters, ensure these staff members receive the appropriate level of training. Training sessions are conducted every second year and attendance by UTS College personnel is compulsory. The compliance training program, incorporates formal training, and on-the-job learning and corporate communications and embeds privacy practices into daily operations through improved awareness and encouragement.

Notifications on updates/changes to legislation relating to privacy, copyright, records management and ESOS and the National Code of Practice are emailed to all staff as and when received.



A summary version of UTS College's Privacy Policy and this Plan is provided to all new staff via an e-learning course, and the full Plan is accessible on the Staff intranet.

10 INTERNAL REVIEW PROCEDURES

10.1 The internal review processes

An application for a review of a potential breach of privacy must:

- a) be in writing [[Application for Internal Review](#)]
- b) be addressed to:
The Privacy Officer
Level 13, UTS Building 10 (CB1) 235 Jones Street
Broadway NSW 2007
[E] privacy@insearch.edu.au
- c) specify an address in Australia to which a notice may be sent; and
- d) be lodged at an office of UTS College Limited within 6 months from the time the applicant first became aware of the conduct that is the subject of the application (or such later date as the agency may allow).

The review will be conducted by the Privacy Officer, where the Privacy Officer is not substantially involved in the matter relating to the application. Other suitably qualified members of staff may be called upon to conduct the review if the Privacy Officer where appropriate. At all times, the review will be held by an employee or officer of UTS College.

In reviewing the conduct that is the subject of the application, the individual dealing with the application must consider any relevant material submitted by the applicant and the Privacy Commissioner.

UTS College will endeavour to complete the review as soon as is reasonably practicable and will complete the review within 60 days from the day on which the application was received. If the review is not completed within this time the applicant may apply for a review of the conduct concerned to the NSW Civil and Administrative Decisions Tribunal under Section 55 of the PPIP Act.

On receiving an application for an internal review, UTS College must:

- a) inform the NSW Privacy Commissioner as soon as is practicably possible of the application.
- b) keep the NSW Privacy Commissioner informed of the progress of the internal review; and
- c) inform the NSW Privacy Commissioner of the findings of the review and of the action proposed to be taken by the agency in relation to the matter.

Once the internal review has been completed, UTS College may do one or more of the following:

- a) take no further action on the matter.
- b) make a formal apology to the applicant.
- c) take such remedial action considered appropriate.
- d) provide undertakings that the conduct will not occur again; and
- e) implement administrative measures to ensure that the conduct will not occur again.

Within 14 days of the completion of the review, UTS College will notify the applicant in writing of:

- a) the findings of the review (and the reasons for those findings)
- b) the action proposed to be taken by the agency (and the reasons for taking them); and
- c) the right of the person to have those findings, and the agency's proposed action, reviewed by the NSW Civil and Administrative Tribunal.

If an individual believes that UTS College has breached, or is likely to breach, one or more of the IPPs, they may submit a written request to UTS College to investigate the matter. The following procedures will be used to resolve an application for internal review.



- The application is assessed by UTS College's Privacy Officer to determine whether the complaint involves a breach of privacy.
- The Privacy Officer will notify the NSW Privacy Commissioner in writing that an application for internal review has been received.
- The Privacy Officer (or another person appointed by the Managing Director if the matter involves the Privacy Officer) will investigate the matter by considering all relevant material supplied by the applicant and the Privacy Commissioner.
- Every four weeks the Privacy Officer will inform the NSW Privacy Commissioner in writing about progress of the review.
- The review will be completed as soon as possible, and in all cases within 60 days of receiving the application.
- The Privacy Officer will notify the applicant of the following (as appropriate):
 - findings of the review;
 - reasons for those findings;
 - a formal apology from UTS College;
 - remedial action to be undertaken by UTS College (which may include compensation);
 - UTS College's undertaking that the breach of privacy will not recur;
 - administrative measures that will be implemented to ensure no further breach of privacy;
 - reasons for the proposed remedial action and administrative measures;
 - the applicant's right to have the findings and UTS College's proposed remedial action and administrative measures reviewed by the NSW Civil and Administrative Tribunal.

The Privacy Officer will notify the NSW Privacy Commissioner in writing of the findings and of any remedial action and administrative measures that UTS College proposes to undertake.

The Privacy Officer will initiate administrative measures to ensure that the breach does not recur. Where appropriate, new, or revised procedures may be incorporated into the Plan.

The Privacy Officer will provide an annual report on all requests and related outcomes of privacy internal reviews to the Executive, and the Audit and Risk Management Committee.

10.2 Incident reporting

Employees seeking to report privacy issues should, in the first instance, report the matter to their immediate manager. If, for any reason, the employee feels that reporting the incident through this channel would be inappropriate, the employee may report the matter directly to the Privacy Officer, a member of People or a member of the Executive. Such reports may be made confidentially if desired.

Any person making allegations or providing information in relation to an alleged fraud or other matter involving misconduct must be made aware that the information provided will be relied upon and eventually the person concerned may be asked to give evidence relative to their knowledge of the circumstances. A person who has made a confidential report will not be required to give evidence about their report.

10.3 Disciplinary procedures

The Performance Management Policy sets out UTS College's internal performance management processes designed to enable the achievement of individual, departmental and organisational goals and objectives and is supported by the Managing Unsatisfactory Performance Procedure.

The Complaints and Grievance Resolution Policy sets out how UTS College handles any employment-related or staff grievances, including the investigation and resolution process and is supported by the Complaints and Grievance Resolution Procedure.

The Whistleblowing Policy provides disciplinary processes related to fraud and corruption matters.



11 PRIVACY AND PROTECTION OF PERSONAL INFORMATION

11.1 Applications for access to personal information

Applications should be made to People (for staff records) or to the Privacy Officer (for student records). If, having inspected their file, the applicant lawfully alters personal information on that file, the Privacy Officer will send a copy of that alteration to the People Partner or Student Administration Unit (as appropriate) for attachment to the applicant's personal file and updating in other systems (e.g. Payroll) as required.

Applications that entail searches for extensive documentation located in various units should be referred to the Privacy Officer. These applications will be handled in a manner consistent with reasonable use of resources and without impeding the core business. Applications of a frivolous nature, or that would involve a substantial and unreasonable diversion of resources, will not be accepted.

12 RELATED LEGISLATION

With reference to its holdings of personal information, UTS College has made provision to comply with its obligations under the following legislation:

- State Records Act (1998) (NSW)
- Freedom of Information Act (1989) (NSW)
- Public Interests Disclosures Act (1994) (NSW).

ADMIN USE ONLY

APPROVAL		
Name:	Interim CEO	Date: 13 September 2023
Policy Title	Privacy Management Plan	
Policy Owner:	Company Secretary	
Policy ID	PO/GOV/20/23	
Effective Date:	13 September 2023	



APPENDIX A: ABOUT THE PRIVACY LAWS

This is a general summary of how UTS College staff and students must manage personal and health information under the PPIP Act, the HRIP Act and other relevant laws. For more information, please refer directly to the Information and Privacy Commission [website](#) or the [legislation](#).

The PPIP Act and personal information

The PPIP Act sets out how we must manage **personal** information.

About personal information

Personal information is defined in section 4 of the PPIP Act and is essentially any information or opinions about a person where that person's identity is apparent or can be reasonably ascertained. Personal information can include a person's name, address, family life, sexual preferences, financial information, fingerprints and photos.

There are some kinds of information that are not personal information, e.g. information about someone who has been dead for more than 30 years, information about someone that is contained in a publicly available publication, or information or an opinion about a person's suitability for employment as a public sector official. Health information is generally excluded here as it is covered by the HRIP Act.

Information protection principles (IPP)

Part 2, Division 1 of the PPIP Act contains 12 IPPs with which we must comply. Here is an overview of them as they apply to UTS College.

Collection

1. We collect personal information only for a lawful purpose that is directly related to our functions and activities.
2. We collect personal information directly from the person concerned or an authorised agency.
3. We inform people why their personal information is being collected, what it will be used for, and to whom it will be disclosed. We tell people how they can access and amend their personal information and any possible consequences if they decide not to give their personal information to us.
4. We ensure that personal information is relevant, accurate, is not excessive and does not unreasonably intrude into the personal affairs of people.
5. By only collecting information that is relevant to UTS College's functions as a Higher Education Provider, and making individuals aware, at the time of collection, that we are collecting personal information, UTS College ensures the information is relevant to that purpose, is not excessive, up to date and complete.

Storage

6. We store personal information securely, keep it no longer than necessary and destroy it appropriately. We protect personal information from unauthorised access, use or disclosure.
7. UTS College ensures that personal information is protected by storing it on secure data servers that are regularly maintained.

Access and accuracy

8. We are transparent about the personal information we store about people, why we use the information and about the right to access and amend it.
9. We allow people to access their own personal information without unreasonable delay or expense.
10. We allow people to update, correct or amend their personal information where necessary.
11. We make sure that personal information is relevant and accurate before using it.



Use

12. We only use personal information for the purpose we collected it for, unless the person consents to us using it for an unrelated purpose.

Disclosure

13. We only disclose personal information with people's consent unless they have already informed of the disclosure when we collected the personal information.
14. We do not disclose sensitive personal information without consent, e.g. ethnicity or racial origin, political opinions, religious or philosophical beliefs, health or sexual activities or trade union membership.

Exemptions to the IPPs

Part 2, Division 3 of the PPIP Act contains exemptions that may allow us not to comply with IPPs in certain situations. Here are some examples.

- We are not required to comply with IPPs 2-3, 6-8, or 10-12 if we are lawfully authorised or required not to do so.
- We are not required to comply with IPP 2 if the information concerned is collected in relation to a court or tribunal proceedings.

We do not use the other exemptions on a regular basis as they are not usually relevant to the work we do, however if required we will aim to be clear about the exemption used and our reasons for using it.

Privacy codes of practice and public interest directions can modify the IPPs for any NSW public sector agency. These are available on the Information and Privacy Commission [website](#).

There are currently no codes of practice that are likely to affect how we manage personal information.

There are public interest directions that may allow us:

- not to comply with IPPs 2-3, 6-8, 10-12 if necessary in order to properly conduct investigations
- to be exempt from the IPPs when transferring enquiries to a NSW public sector agency.

The other public interest directions are unlikely to affect how we manage personal information.

Offences

Offences can be found in sections 62-68 of the PPIP Act.

It is an offence for us to:

- intentionally disclose or use personal information accessed in doing our jobs for an unauthorised purpose
- offer to supply personal information that has been disclosed unlawfully
- hinder the Privacy Commissioner or a member of staff from doing their job.

The HRIP Act and health information

The HRIP Act sets out how we must manage **health** information.

Health information is a more specific type of personal information and is defined in section 6 of the HRIP Act. Health information can include information about a person's physical or mental health such as a psychological report, or even information about a person's medical appointment.

In the event UTS College receives health information from an individual, all the information will be handled in accordance with the HRIP Act and HPPs.

Privacy Act 1988 (Commonwealth)

The *Privacy Act 1988* (Privacy Act) is an Australian law that regulates the handling of personal information about individuals. This includes the collection, use, storage and disclosure of personal information, and access to and correction of that information.



Other laws that affect how we comply with the IPPs and HPPs

This section contains information about the main laws that affect how we comply with the IPPs and HPPs.

Crimes Act 1900

Under this law UTS College staff and students must not access or interfere with data in computers or other electronic devices unless authorised to do so.

Government Information (Public Access) Act 2009 (GIPA Act) and Government Information (Public Access) Regulation 2018

Under this law people can apply for access to government information we hold. Sometimes this information may include personal or health information. If a person has applied for access to someone else's personal or health information we must consult with affected third parties. If we decide to release a third party's personal information, we must not disclose the information until the third party has had the opportunity to seek a review of our decision.

When accessing government information of another NSW public sector agency in connection with a review, the Information Commissioner must not disclose this information if the agency claims that there is an overriding public interest against disclosure.

Government Information (Information Commissioner) Act 2009 (GIIC Act)

Under this law the Information Commissioner has the power to access government information held by NSW public sector agencies for the purpose of conducting a review, investigation or dealing with a complaint under the GIPA Act and GIIC Act. The Information Commissioner also has the right to enter and inspect any premises of a NSW public sector agency and inspect any record.

This Act also allows the Information Commissioner to provide information to the NSW Ombudsman, the Director of Public Prosecutions, the Independent Commission Against Corruption or the Police Integrity Commission.

Independent Commission Against Corruption Act 1988

Under this law we must not misuse information we have obtained in the course of doing our jobs.

Public Interest Disclosures Act 1994 (PID Act)

UTS College has Public Interest Disclosure Policy relating to our compliance with the PID Act.

State Records Act 1998 and State Records Regulation 2015

This law sets out when we can destroy our records. It also authorises the State Records Authority to establish policies, standards and codes to ensure that NSW public sector agencies manage their records appropriately.

