Privacy Policy

Responsible Officer	General Counsel
Approved by	Vice-Chancellor
Approved and commenced	October 2018
Review by	October 2021
Relevant Legislation, Ordinance, Rule and/or Governance Level Principle	*Personal Information Protection Act 2004 (Tas)* *Privacy Act 1988 (Cth)* *Archives Act 1983 (Tas)* *Right to Information Act 2009 (Tas)* *General Data Protection Regulation (EEA)*
Responsible Organisational Unit	Legal Services

CONTENTS

1. Objective

The objectives of this policy are to:

- identify the University's obligations for handling personal information of past and present University staff, students, prospective students and staff, and individuals associated with the University; and
- inform University staff of the privacy obligations they must comply with; and
- outline the University's process for responding to suspected data breaches and complaints from individuals that their personal information has not been dealt with in accordance with this policy.

2. Policy Statement

The University respects and values the privacy of all individuals and is committed to ensuring that it complies with its legislative obligations under the *Personal Information Protection Act 2004* (Tas) (***PIP Act***); the *Privacy Act 1988* (Cth) (***Privacy Act***) when the University has legislative obligations and/or contractual obligations to the Commonwealth Government; and the *General Data Protection Regulation* (European Economic Area) (EEA) (***GDPR***) when the University processes personal data of data subjects in the EEA.

The policy applies to the personal and health information (including sensitive information) of staff, students, alumni and other individuals associated with the University, as well as individuals about whom the University holds personal information.

This policy applies to all areas of the University. All employees, volunteers, consultants, contractors and agents of the University must comply with this Policy when collecting personal information on the University's behalf and when using or dealing with personal information in the University's possession, including the obligation to report a suspected data breach. Failure to comply may constitute misconduct or breach of contract and may result in disciplinary action being taken by the University or termination of contract.

The policy explains how the University collects, uses, discloses, stores, destroys and manages various types of personal information. It explains how an individual can access personal information. It also explains how to report a suspected data breach and how to complain about suspected interferences with privacy.

3. Definitions

Personal information is any information or opinion in any recorded format about an individual –

a) whose identity is apparent or is reasonably ascertainable from the information or opinion; and
b) who is alive or has not been dead for more than 25 years; but does not include personal information in a publicly available record or publication.

Personal information that is commonly collected includes:

- Name
- Address (residential, postal and email)
- Phone number
- Gender
- Ethnic origin
- Passport number
- Banking and credit card details
- Tax file number
- Health information
- Education and employment history details
- Emergency contact details
- Photographs or video recordings (including CCTV footage)
- Academic record
- IT access logs
- Identifiable data (eg IP address) collected via a website, mobile application, wifi or online service, including by cookies or related technology
- Observed information about the conduct or activities of a person
- Records of donations and transactions

Personal information may include sensitive information about an individual such as racial or ethnic origin, membership of a political association, political opinions, religious beliefs or affiliations, philosophical beliefs, membership of a professional or trade association, membership of a trade union; sexual preferences or practices; criminal record, as well as health information.

Personal data (defined under the GDPR) means any information relating to an identified or identifiable natural person residing in the EEA. An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, psychological, genetic, mental, economic, cultural or social identity of that natural person.

Health information means information or an opinion about the physical, mental or psychological health of an individual, a disability, an individual's future wishes relating to the provision of health services, other information collected to provide, or in providing, a health service and genetic information.

Consent means any freely given, specific, informed and unambiguous indication of an individual's wish by which the individual, by a statement or by a clear affirmative action, signifies agreement to the collection, use or disclosure of personal or health information or the processing of personal data relating to that individual.

Data subject means any individual within the borders of the European Union at the time of processing of their personal data.

Processing (in relation to personal data) means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

In this policy, a reference to "personal information" includes "personal data", unless "personal data" is expressly referred to in relation to obligations or requirements under the GDPR.

Privacy Impact Assessment (PIA) means a systematic assessment of a project that identifies the impact that the project might have on the privacy of individuals, and sets out recommendations for managing, minimising or eliminating that impact. PIAs are an important component in the protection of privacy and should be part of the overall management of privacy risk. Undertaking a PIA can assist the project manager and the University:

- describe how personal information flows in a project;
- analyse the possible impacts on individuals' privacy;
- identify and recommend options for avoiding, minimising or mitigating negative privacy impacts;
- build privacy considerations into the design of a project;
- achieve the project's goals while minimising the negative and enhancing the positive privacy impacts.

PIP Act means the Personal Information Protection Act 2004 (Tas)

Privacy Act means the Privacy Act 1988 (Cth)

GDPR means the *General Data Protection Regulation* (European Economic Area) (EEA)

Supervisory authority (for the EEA) means the public body established by the EEA country for the monitoring of compliance with the regulation of the privacy of personal data.

4. Authority

This policy is made under section 7(1)(g) of the *University of Tasmania Act 1992* (Tas) and the University's legislative obligations to comply with:

- The *PIP Act*;
- The *Privacy Act*; and
- The *Right to Information Act* 2009 (Tas); and
- The *General Data Protection Regulation* (EEA).

5. Policy Provisions

5.1 Collection of Personal information

The University will collect information only where it is necessary in order to carry out its functions and activities.

As part of its operations, the University collects information for various purposes, including for:

a the promotion and provision of education and related activities;
b the employment of staff;
c the provision of counselling and psychology services through its clinics;
d the conduct of research;
e the day to day operation of the University.

Before, during or as soon as practicable after collection of personal information, the University will provide to the individual a statement containing information about the purpose of collection and related information. These privacy statements are to be approved by Legal Services. Privacy statements for staff and students have been approved by Legal Services and can be accessed via the Privacy page on the Staff intranet.

When the University collects personal data from individuals in an EEA country, the University will provide the following additional information (at the time of or before the collection of the personal data):

- the period for which the personal data will be stored, or the criteria used to determine that period;
- the right to request access, rectification or erasure of an individual's personal data, restriction of processing, objection to processing and the right to data portability;
- where personal data is processed on the basis of consent, the existence of the right to withdraw consent at any time;
- the right to lodge a complaint with a supervisory authority (within the definition of the GDPR); and
- the existence of automated decision-making, including profiling.

If the University collects personal data of an individual residing in the EEA from third parties, the University will inform the individual to whom the data relates of the categories of personal data that have been collected, as well as all the matters referred to above. The University will inform the individual of these matters within a reasonable time after collecting the personal data, but at the latest within the following periods:

- within one month, having regard to the specific circumstances in which the personal data is processed;
- if the personal data is to be used for communication with the individual, at the latest at the time of the first communication; or
- if a disclosure to a third party is envisaged, at the latest when the personal data is first disclosed.

The University will not collect your sensitive information including health information unless the individual has explicitly consented, or the collection is required or permitted by law. This is unless the individual is an employee and the information collected is employee information.

5.2 How does the University use personal information?

The University will only use the personal information it collects for the purpose for which it was collected unless:

- the University obtains the consent of the individual to use the personal information for another purpose; or
- the University is permitted to use the personal information pursuant to the *PIP Act* or the *Privacy Act*.

5.3 Who does the University disclose personal information to?

The University will use or disclose personal information in accordance with:

- the purpose for which it was collected;
- a related purpose which you might reasonably expect;
- your permission to do so;
- as otherwise permitted or as required to do so by law.

This includes that personal information may be used to assist the University to effectively manage its premises, facilities and services.

The University may disclose personal information to:

- government departments and agencies and regulatory bodies to satisfy reporting requirements;
- the University's controlled entities to the extent such personal information is required by the controlled entity to provide services to the University or undertake activities for the University;
- another tertiary institution or tertiary admission centre if the individual applies to transfer studies or undertake an official student exchange, cross-institutional study, dual degree, industry experience or other approved collaborative study arrangement;
- scholarship providers or scholarship sponsors;
- external service providers;

- collaborating parties, to the extent such personal information is required for the collaborator to provide services to the University;
- law enforcement bodies, medical and emergency response providers;
- professional service providers and insurers of the University.

The University will not disclose personal information to third parties other than those listed in paragraphs 5.3 without the consent of the individual, unless:

- disclosure is permitted or required by law; or
- disclosure is necessary to prevent or reduce the likelihood of serious threat to the health, safety or welfare of an individual.

In relation to personal data of individuals residing in the EEA, the University will process such data only if processing is based on one of the following:

- the individual has consented to the processing for one or more specific purposes;
- processing is necessary for the performance of a contract;
- processing is necessary for compliance with a legal obligation under Australian law;
- processing is necessary to protect the vital interests of an individual;
- processing is necessary for the purposes of the legitimate interests of the University.

5.4 Does the University disclose personal information interstate or overseas?

The University may transfer personal information interstate or overseas where it is necessary for the purposes for which it was collected. Where the University transfers personal information outside Tasmania or overseas, it will comply with the requirements under the *PIP Act* (and *Privacy Act* where relevant) and will ensure that the recipient is within a jurisdiction that has comparable privacy protections or otherwise submits to binding obligations that are substantially similar.

Where the University transfers personal data to another country, it will do so in accordance with requirements under the GDPR.

5.5 Data Quality

The University will take reasonable steps to ensure that it keeps the personal information it holds up to date, accurate and complete. If the University holds personal information that is inaccurate, it will take reasonable steps to erase or rectify the information without delay, having regard to the purpose for which the information was collected and its obligations under law.

5.6 Data Security

The University will take reasonable steps to protect personal information from misuse, loss, disclosure and unauthorised access.

The University will dispose of personal information in accordance with the disposal schedules maintained under the *Archives Act 1983* (Tas).

5.7 Direct Marketing

From time to time, and where appropriate, the University may use or disclose information (excluding sensitive or health information) about an individual for marketing purposes. Where the University engages in marketing, it will ensure that there is a simple means by which an individual may easily request not to be identified in marketing materials.

5.8 Staff and Student Identification Numbers

The University assigns staff and students an identification number which is a unique identifier. The University treats this identification number as personal information. It is the responsibility of staff and students to protect this identification number as personal information.

5.9 How can an individual access and correct their personal information?

An individual may at any time request access to their personal information. The University may charge a reasonable fee to access that information, for example to recover the costs of photocopying or a time costed charge if it is necessary for University staff to spend a significant amount of time to provide access to the information. The University may require verification of an individual's identity before providing access to personal information.

If an individual believes the personal information the University holds about them is not up to date, accurate, or complete, the individual may contact the University in writing via the contact details provided in this policy.

On receiving a written request for an amendment to an individual's personal information, the University will provide the individual with a decision about their request as soon as possible (but within 20 working days of the request). If the University decides not to amend the personal information as requested, it will provide an explanation for that refusal.

The University is not required to provide access to personal information where it reasonably believes doing so would, for example (but not be limited to):

- prejudice law enforcement or crime prevention activities;
- pose a serious threat to health or safety;
- contain personal information of someone other than the person who has requested it; or
- be contrary to law.

Under the GDPR data subjects can make a request to access the following information:

- confirmation from the University that it is processing the individual's personal data;
- a copy of the individual's personal data; and
- other supplementary information such as:
    - the purposes of the University's collection, use or disclosure or processing (in the case of personal data);
    - the categories of personal data concerned;
    - the recipients or categories of recipient to whom the personal data will be disclosed;
    - the retention period for storing the personal data or the criteria for determining how long it will be stored;

- the existence of the individual's right to request rectification, erasure or restriction or to object to such processing;
- the right to lodge a complaint with a supervisory authority (within the meaning of the GDPR);
- information about the source of the data (if it was obtained from a third party);
- the existence of automated decision-making (including profiling); and
- the safeguards provided if the personal data is transferred to another country or international organisation.

For individuals who are not data subjects in the EEA, the University may provide the above information, upon request, at its discretion.

5.10 Other rights of residents in the EEA

In certain cases, data subjects in the EEA may have the following rights, subject to obligations under Tasmanian and Australian law:

- the right to access (as outlined above);
- the right to rectify incomplete or inaccurate personal data (as outlined above);
- the right to have personal data erased;
- the right to object to certain processing of personal data;
- the right to request the transfer of personal data to another party; and
- the right to restrict certain processing of personal data.

For individuals who are not data subjects in the EEA, some of the above rights are similar to the rights under the PIP Act or the Privacy Act. To the extent that this is not the case, the University may, at its discretion, provide the same or similar rights on request.

5.11 Data Breaches

University personnel who become aware of any actual or suspected loss or unauthorised access, use, modification, disclosure or other misuse of personal information ("data breach") must notify the data breach to the ICT Security Manager and General Counsel **immediately.**

There are strict legislative timelines that apply to notification to affected individuals in some countries (for example data breaches involving data subjects of an EEA country, the notification to a supervisory authority is required within 72 hours of discovering the data breach).

5.12 Data Breach Response Team

A data breach response team will be established for the purposes of responding to data breaches consisting of Chief Information Officer, ICT Security Manager, a nominee of Chief Operating Officer, General Counsel and Associate Director, Compliance.

Management of the breach will then follow the University's Data Breach Response plan detailed in paragraph 5.13.

5.13 Data Breach Response plan

The University will comply with any applicable mandatory data breach notification requirements.

The Data Breach Response plan is available at: https://universitytasmania.sharepoint.com/sites/legal-services/SitePages/Data-Breach.aspx?web=1.

5.14 Privacy Officer and EEA Data Controller

The Privacy Officer and Data Protection Officer of the University is the General Counsel (or nominee within Legal Services) and is contactable via legal.office@utas.edu.au

5.15 Complaints

If an individual believes their personal information has not been handled by the University in accordance with this Policy, the individual may make a complaint in writing or by email to the General Counsel.

The full complaints procedure, inclusive of contact details, can be found at: https://secure.utas.edu.au/legal-services-secure/privacy/complaints.

6. Versioning

Former Version (1)	*Version 1 - Privacy Policy*, approved Vice-Chancellor, December 2014; reviewed December 2017.
Former Version (2)	*Version 2 - Privacy Policy* (current document), approved by Vice-Chancellor, December 2014. Amended in December 2016 to incorporate Colleges.
Current Version (3)	*Version 3 – Privacy Policy* (current document), approved Vice-Chancellor, October 2018