

Privacy Procedure - Compliance

Section 1 - Key Information

Policy Type and Approval Body	Administrative - Vice-Chancellor
Accountable Executive - Policy	Chief Operating Officer
Responsible Manager - Policy	General Counsel & Director of Assurance
Review Date	3 years

Section 2 - Purpose

(1) This Procedure documents how to comply with the Privacy Policy with regard to the compliance requirements for handling personal information.

Section 3 - Scope

(2) This Procedure applies to:

- a. staff
- b. students
- c. other members of the University (including Council members, contractors, volunteers and honorary appointees).

(3) This Procedure also applies to:

- a. all areas of the University in relation to the collection, access, use and disclosure and storage of personal and health information of any individual;
- b. personal and health information recorded in any format – for example hard copy written format, online content, digital records and data, photographic images, video or audio recordings, or any other means.

Section 4 - Key Decisions

Key Decisions	Role
Insert powers/decision making/responsibility if applicable	Insert position title
Insert powers/decision making/responsibility if applicable	Insert position title
Insert powers/decision making/responsibility if applicable	

Section 5 - Policy Statement

(4) This Procedure forms part of the Privacy Policy which governs its application.

Section 6 - Procedures

Part A - Collection of Personal and/or Health Information

(5) Personal, health and sensitive information must only:

- a. be collected where it is necessary for, or directly related to, one or more of the University's functions or activities;
- b. be collected directly from the individual concerned (unless unreasonable or impracticable to do so) and where collected from someone else, reasonable steps must be taken to make the individual concerned is made aware of the collection (unless it would pose a serious threat to the life or health of any other individual);
- c. be collected in a lawful and fair manner and not in an unreasonably intrusive way; and
- d. where the personal information is sensitive information, be collected with an individual's consent or as otherwise permitted by law.

Collection Notice - Information to be Provided at the Point of Collection

(6) When collecting personal, health or sensitive information from an individual, all reasonable steps must be taken to notify the individual at the time of collection of the following:

- a. the purpose(s) for which the information is being collected;
- b. to whom the University usually discloses information of that kind;
- c. any law that requires the information to be collected;
- d. the main consequences (if any) for the individual if the information is not provided;
- e. if the University is likely to disclose the personal information to an overseas recipient, the countries in which recipients are located (where practicable); and
- f. a link to the University's Privacy Policy which contains information about how the individual may:
 - i. access their personal information held by the University subject to the provisions of the [Freedom of Information Act 1982](#) (Vic)
 - ii. seek correction of their personal information
 - iii. complain about a breach of an individual's privacy and how the University will deal with such complaints; and
 - iv. how to contact the University's Privacy Officer.

(7) The above information should be set out in a document commonly referred to as a 'Collection Notice' or 'Collection Statement'. The University's key Collection Notices can be found on the University's website [hyperlink] and should, wherever practicable, be provided to an individual when their personal or health information is first collected.

(8) If the proposed collection of personal information is not covered by the one of the University's key Collection Notices, a bespoke one should be created. Further information and a template for creating Collection Notices can be found on the La Trobe [Privacy Intranet page](#) .

Anonymity

(9) Individuals generally have the option of not identifying themselves when dealing with La Trobe. Requests to remain

anonymous should be accommodated wherever lawful and practicable. However, individuals should also be advised that the University may not be able to deliver its functions, activities and services or interact with them if they engage with the University in an anonymous way.

Unique Identifiers

(10) A unique identifier is an identifier (often a number) that is unique to a particular individual. Unique identifiers are considered personal information and must be handled in accordance with this Policy.

(11) Staff and students will be assigned with a unique identifier in the form of a La Trobe staff or student ID number shortly prior to or upon employment/enrolment. These ID numbers are necessary for the University to efficiently carry out its functions.

(12) Government issued unique identifiers (for example copies of passports or passport numbers, Tax File Numbers, Medicare details, drivers' licence, federally issued Unique Student Identifiers etc) must be treated with considerable care. The University must not adopt another organisation's unique identifiers as its own, the collection and use of such identifiers must be limited to only occur when strictly necessary (e.g. where required by law) and they must be collected directly from an individual with their consent.

(13) All business areas that are lawfully required to handle unique identifiers must:

- a. inform staff and students when using and disclosing their unique identifier and for what purpose via an appropriate Collection Notice;
- b. implement business practices to sight the original document but not retain a copy of the document wherever possible and practicable;
- c. limit the number of staff who have access to the documents and ensure staff who are granted access, undertake regular privacy training;
- d. if required by law to retain a copy, obscure the ID number on the copy wherever possible and appropriate; and
- e. limit and exercise caution if staff receive or send emails that contain unique identifiers.

Tax File Numbers

(14) In accordance with the Privacy Act 1988 (Cth), the University is considered a 'Tax File Number (TFN) recipient.' The University must therefore comply with the Privacy (Tax File Number) Rule 2015 (Cth) (also known as the 'TFN Rule'). In accordance with the TFN Rule, TFN information must only be requested, collected and used where the purpose is authorised by taxation law or superannuation law. Individuals should be informed of the specific law authorising its collection, that it is not an offence to decline to provide one, and of the consequences should they choose not to do so.

(15) If in doubt, advice should be sought from the University's Legal Services office.

Unique Student Identifier (USI)

(16) Students require a federally issued Unique Student Identifier (USI) and are assigned one by the Australian Government under the [Student Identifiers Act 2014 \(Cth\)](#). The USI is an individual's education number for life. A USI is required for graduating higher education, seeking a HELP loan or Commonwealth Supported Place, among other things.

(17) The [Student Identifiers Act 2014 \(Cth\)](#) requires the protection of privacy of individuals and their USI. Therefore, the University must not use USIs as its own identifier and must not print a USI on a Student ID card.

Part B - Use and Disclosure

(18) 'Use' of personal information refers to the use of personal or health information by the University and 'disclosure' refers to the disclosure of personal or health information to third parties.

(19) Staff, contractors and associates must also ensure that they do not use or disclose personal or health information unless:

- a. it is for the primary purpose for which the information was originally collected (and which should generally be set out in a 'collection notice' – see Part A above);
- b. the individual has provided consent; or
- c. the use or disclosure is otherwise permitted by law (e.g. where it is necessary to lessen or prevent a serious threat to an individual's life, health, safety or welfare etc).

Disclosing Personal or Health Information to Third Parties

(20) Personal or health information of any individual must not be released to a third party without the individual's written consent, except where required and/or authorised by law.

Parents of La Trobe students

(21) Student personal information should not be provided to parents unless the student concerned has provided their consent. Students should complete and submit a consent form to provide their consent and authorise the release of their personal information to a nominated third party.

(22) There may be exceptions to requiring express consent from a student before releasing their personal or health information to a parent or guardian — for example, if a student is under the age of 16, has an intellectual disability or is subject to a Guardianship Order. In addition, in an emergency, a student's next of kin should be notified and serious health and safety considerations should take priority.

(23) Any queries should be referred to the Privacy Officer on privacy@latrobe.edu.au or Legal Services on legal.services@latrobe.edu.au.

Law Enforcement Agencies

(24) Staff and business areas may occasionally receive requests for information directly from a law enforcement agency (e.g. the Federal or Victorian Police etc.). In accordance with the privacy legislation, the University is permitted (but not required) to disclose personal information to law enforcement agencies where it 'reasonably believes' that the disclosure is 'reasonably necessary' for a 'specified purpose' by a law enforcement agency.

(25) A specified purpose includes:

- a. the prevention, detection, investigation, prosecution or punishment of criminal offences or breaches of a law imposing a penalty or sanction;
- b. the enforcement of laws relating to the confiscation of the proceeds of crime;
- c. the protection of the public revenue;
- d. the prevention, detection, investigation or remedying of seriously improper conduct; or
- e. the preparation for, or conduct of, proceedings before any court or tribunal, or implementation of the orders of a court or tribunal.

(26) Staff should take the following steps to satisfy themselves that the request has been made appropriately and the disclosure is reasonably necessary:

- a. requests for information should be made in writing (an email is sufficient) by the law enforcement officer clearly stating what information is required and for what purpose;
- b. consider if the request relates to one of the five specified law enforcement purposes above; and
- c. verify the identity and authority of the person make the request i.e was the request from a police email account with the officer's name, position and badge number in the signature block. In some cases, confirmation may be required by a more senior officer in the law enforcement agency.

Keeping a record

(27) If a decision is made to release information to a law enforcement agency, only the relevant information that is requested should be provided to prevent making an excessive disclosure of information. Consideration should also be given as to whether any third-party information needs to be redacted.

(28) Privacy legislation requires that a written record of the release of information must be retained. Data Custodians will be responsible for ensuring that there is a process for recording the release of personal information to law enforcement agencies and ensuring the following details are recorded: to who it was released, when, how and the name and title of the staff member who approved the release.

Subpoenas and Warrants

(29) Court issued subpoenas and warrants from law enforcement agencies or must be immediately referred to Legal Services via legal.services@latrobe.edu.au.

Part C - Data Quality and Security of Personal Information

Data Quality

(30) Maintaining data quality is everyone's responsibility.

(31) All business units must take reasonable steps to ensure that the personal or health information they hold is accurate, complete, and up to date.

(32) Staff and students are expected to provide the University with accurate and up-to-date information and to inform the University of any changes to their personal information (for example by regularly checking and updating information held on staff and student portals). Individuals can self-manage updates to their personal information via the student and staff portals.

Data Security

(33) Having regard to the nature of the personal and health information being collected, reasonable steps and precautions must be taken to safeguard the information the University holds from loss, theft, unauthorised use, disclosure or modification.

(34) Access to personal and health information should be protected by physical and/or electronic safeguards to ensure only those with a legitimate need to access the information can do so. Safeguards may include:

- a. limiting access to personal and health information to authorised users who have a 'need to know' as part of their role;
- b. using measures such as single sign-on, multifactor authentication, firewalls, data encryption, virus detection methods, audit logs and passwords restricted to the University's online and computerised systems;
- c. restricting access to physical storage areas via the use of staff ID cards;
- d. providing staff with training on how to handle personal and health information in accordance with this Policy

and applicable privacy laws;

- e. ensuring that third parties who use or store any personal information adopt appropriate security measures and are bound by a legal contract; and
- f. de-identifying and/or securely destroying personal, health and sensitive information when it is no longer needed for any purpose and in accordance with the [Public Records Act 1973](#) and the University's [Records Management Policy](#).

(35) University staff, students and other members of the University community must only:

- a. access personal or health information to the extent necessary to perform their role/function;
- b. access personal or health information which they have authority to access; and
- c. use personal information or health information for a legitimate purpose and in accordance with this Policy.

Contracts

(36) In accordance with the University's [Contracts Policy](#), before a contract is entered, the Contract Sponsor is responsible for ensuring completing or ensuring all pre-contractual steps are followed and, once executed, implementing the contract and then actively managing it throughout its term. Pre-contractual steps include ensuring privacy compliance risks are considered and, where identified, ensuring they are satisfactorily addressed. Contract (or project) implementation also requires privacy compliance issues to be actively managed.

(37) The privacy tools set out in Part F 'Privacy Impact Assessments' are intended to assist with highlighting potential privacy risks and demonstrating that appropriate controls have or will be implemented.

(38) Staff authorised to execute contracts are ultimately accountable for the decision to contract. Therefore, delegated contract signatories must ensure that they are satisfied that:

- a. any contract they enter on behalf of the University complies with privacy legislation;
- b. appropriate privacy safeguards are in place for the protection of personal and health information; and
- c. there are contract management processes in place to ensure that any contractual obligations which relate to privacy (e.g. the requirement to notify specified persons/organisations in the event of a breach etc) can and will be met.

Part D - Access to and Correction of Personal Information

(39) Staff and students will be provided reasonable access to and the ability to correct their personal and health information held by the University. In most cases, individuals can request information held by the University about themselves directly to a business area. Routine requests for information can be submitted and generally will be directly handled by the relevant business area:

Students	ASK La Trobe or studentrecords@latrobe.edu.au
Staff	hr.enquiries@latrobe.edu.au
Graduate Researchers	grs@latrobe.edu.au
Alumni	alumni@latrobe.edu.au

(40) Individuals also have the right to make a Freedom of Information (FOI) request to access their personal or health information or to seek the correction of their information held by the University. Individuals can contact the Freedom of Information/Privacy Officer via foi@latrobe.edu.au, Information on how to submit a request and relevant charges that may be applicable is available via the University's FOI webpage [<https://www.latrobe.edu.au/statements/foi>]

(41) The Freedom of Information/Privacy Officer will respond to any valid request for access to information or request for the correction of information held by the University within 30 days or as otherwise prescribed under the [Freedom of Information Act 1982](#) (Vic).

(42) The University may take additional steps to verify the identity of any individual who is requesting access to or wanting a correction made to their information before processing any routine business area request or valid FOI request.

Part E - Trans-Border Disclosures

(43) In some circumstances, personal and/or health information may need to be disclosed to a third party outside Australia.

(44) In such circumstances, reasonable steps must be taken to:

- a. seek an individual's consent to the transfer; and/or
- b. ensure that the overseas third party is subject to the same or similar privacy obligations at law;
- c. undertake appropriate levels of due diligence on the third party; and
- d. enter into legally binding contracts with the recipient (usually a contracted service provider, education or research partner) which requires the recipient to comply with the relevant or comparable privacy obligations.

(45) Whenever personal or health information is to be transferred outside of Australia, seek advice from the Privacy Officer or Legal Services.

Part F - Privacy Impact Assessments and Other Privacy Compliance Tools

(46) To assist in ensuring compliance with privacy legislation, any project or program of work at La Trobe must embed privacy principles as part of its design and implementation. The way the University expects this to be achieved and evidenced is by utilising the following privacy tools and applying a risk-based approach:

	Features and when to undertake	Roles and Responsibilities
Privacy Threshold Assessment (PTA)	The PTA is a basic assessment consisting of four (4) online screening questions to determine if a Privacy Impact Checklist (PIC) is required. Any staff member involved in a project or program of work which could involve personal or health information can check whether a PIC is required by completing the PTA. A PTA is not required when it is clear that personal or health information will not be involved.	Staff or relevant member of the University community can use the PTA

	Features and when to undertake	Roles and Responsibilities
Privacy Impact Checklist (PIC)	<p>The PIC is a short and mid-level assessment to help identify privacy risks and determine whether a detailed PIA is required.</p> <p>A PIC must be completed where:</p> <ul style="list-style-type: none"> - a PTA suggests one is required; - a new project or program of work involves personal or health information; - there are substantive changes to an existing project or program of work that involves personal or health information; - personal or health information is to be merged, combined or aggregated from other University technologies, processes or programs; - existing processes which are being renewed that may not have had a privacy assessment previously undertaken. 	<p>Any staff member responsible for a project or program of work involving personal or health information should ensure they complete a PIC and forward it to the Privacy Officer at privacy@latrobe.edu.au</p> <p>Project Managers/Contract Sponsors (or their nominee) must complete a PIC, ensure it is approved by the relevant Data Custodian and forward it to the Privacy Officer at privacy@latrobe.edu.au.</p> <p>PIC's must be kept up to date and revised if the nature/scope of the project or program of work changes.</p> <p>The Privacy Officer will review the PIC, make recommendations where appropriate and determine whether a more comprehensive Privacy Impact Assessment (PIA) will need to be undertaken</p>
Privacy Impact Assessment (PIA)	<p>A PIA is an in-depth and detailed assessment based on the Office of the Victorian Information Commissioner's template which considers compliance against each of the relevant privacy principles. The greater a project's size, complexity, or scope, the more likely a comprehensive PIA will need to be conducted.</p> <p>A PIA must be undertaken where:</p> <ul style="list-style-type: none"> - a PIC result suggests a PIA is required; or - the Privacy Officer determines one is required. 	<p>Project Sponsor/Contract Sponsor (or their nominee) must complete a PIA where one is required.</p> <p>Once a PIA will be completed, the Privacy Officer will make recommendations regarding risk mitigation strategies.</p>

(47) The above privacy compliance tools are intended to:

- a. identify potential privacy risks before a project/project of work commences and assist in the development of privacy risk mitigation strategies (also known as 'Privacy by Design'); and
- b. act as a record of the steps taken to consider and mitigate privacy risks and comply with relevant privacy legislation.

(48) The privacy compliance tools should:

- a. be completed before a project or initiative commences and early in the development stages so that it is still possible to influence the project design, or if there are significant privacy risks and impacts, reconsider the project;
- b. be completed prior to any contract relating to the collection, handling, storage, use or disclosure of personal or health information being entered';
- c. be updated if the scope of the project changes or if the personal or health information to be collected, used, disclosed or stored is to be done so in a different way; and
- d. be regularly reviewed by the Data Custodian and the Contract/Project Sponsor throughout the lifecycle of the project.

(49) Where a project or program of work is particularly significant, the General Counsel & Director of Assurance may authorise the undertaking a comprehensive PIA for a program by an external provider based on the recommendation of the Privacy Officer. The business area responsible for the project or program or work will be responsible for the cost of the PIA.

(50) The Privacy Officer may recommend to the General Counsel & Director of Assurance that a retrospective PTA and/or PIA be undertaken if one was not undertaken prior to the implementation of a project or program of work.

(51) A failure to undertake and/or accurately complete or submit a PIC or PIA will be reported and escalated to the Project/Contract Sponsor or relevant SEG member and may result in the inability to proceed with the project or withdrawal of executive support.

Research

(52) PICs and PIAs are generally not undertaken as part of research projects, as data collection, use, disclosure, security and data management form part of the ethics approval provided under the National Statement on Ethical Conduct in Research and Australian Code for the Responsible Conduct of Research. The La Trobe Human Research Ethics Committee (HREC) may, however, recommend or require that some research projects undertake a PIC or seek additional advice from the Privacy Officer as part of the ethics approval process or as required.

(53) More information along with the tools and templates are available via the [Privacy Intranet](#) page.

Part G - General Data Protection Regulation (GDPR)

(54) Additional rights under General Data Protection Regulation (GDPR) exist for processing an EU individual's personal, health or sensitive information while they are a resident in the European Union (EU) including the right to request access to a copy of their information, correction of their information, withdrawal of consent and restriction of use, erasure of information, ability to transfer their information to another data controller in an accessible format.

(55) For individuals outside the EU and for data that was not collected within the EU, the erasure of information will be subject to the retention periods specified by the Public Records Act 1973 (Vic).

(56) Access requests by a European Union (EU) data subject should be made in writing to the Data Protection Officer in the first instance via dpo@latrobe.edu.au

Section 7 - Definitions

(57) For the purpose of this Procedure:

- a. Contract Signatory: duly authorised contract signatory with ultimate accountability for the decision to contract – refer to [Contracts Policy](#).
- b. Contract Sponsor: University staff member or office responsible progressing the proposed arrangement, including ensuring there all pre-contractual steps are followed.
- c. Data Custodian (or Data Owner): has the administrative and/or operational responsibility for the Business area's data and other information, refer to [Data Governance Policy](#).
- d. Data Steward: is appointed by the Data Custodian and supports the Data Custodian in managing the day-to-day activities involved in data custodianship, refer to [Data Governance Policy](#).

GDPR means the European Union's General Data Protection Regulation, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data.

- f. Health information: health information has the meaning set out in the [Health Records Act 2001](#) (Vic). In summary, health information is personal information: about the physical, mental or psychological health or disability of an individual; about an individual's expressed wishes regarding the future provision of health services to them; about a health service provided, or to be provided, to an individual; collected to provide a health service; about an individual collected in connection with organ or body substance donation; or that is genetic information in a form which is or could be predictive of the health of the individual or of their descendants.
- g. Law enforcement agency: is defined in section 3 of the [Privacy and Data Protection Act 2014](#) (Vic) and

- specifically includes state and federal police, crime commissions and examiners, the Business Licensing Authority and the Special Investigations Monitor, agencies involved in the prevention and detection of crime, the release of persons from custody, the execution of warrants, the provision of correctional services, the management and seizure of property under confiscation laws and the protection of public revenue.
- h. Personal information: information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion.
 - i. Privacy (data) breach: a privacy breach occurs when an individual's personal information is subject to loss, unauthorised access, modification, disclosure or other misuse or interference. This may be a result of a malicious breach of the secure storage, information handling protocols or human error. Examples include: a cyber-security incident, accidental loss of IT equipment or hard copy documents, negligence, and improper disclosure of information.
 - j. Project Manager: individual responsible for delivering the project and ensuring it is implemented in line with this Policy.
 - k. Project Sponsor: individual with overall accountability for ensuring that a project or program of work complies with or can comply with relevant legislation (including privacy legislation) and this Policy, is within the approved budget and delivers the projected benefits.
 - l. Sensitive information: personal information about an individual's racial or ethnic origin, political opinions, membership of a political, professional or trade association or trade union, religious beliefs or affiliations, philosophical beliefs, sexual preferences or practices or criminal record.
 - m. Serious harm: may include physical, psychological, emotional, financial or reputational harm.

Section 8 - Authority and Associated Information

(58) This Procedure is made under the [La Trobe University Act 2009](#).

(59) Associated information includes:

- a. [Privacy Intranet](#)
- b. [OVIC webpage](#)
- c. [Contracts Policy](#)
- d. [Data Governance Policy](#)
- e. [Records Management Policy](#)

Status and Details

Status	Not Yet Approved
Effective Date	To Be Advised
Review Date	To Be Advised
Approval Authority	
Approval Date	To Be Advised
Expiry Date	Not Applicable
Responsible Policy Officer	Linda Robertson General Counsel & Director of Assurance
Author	Fiona Rowley +61 3 9479 1839
Enquiries Contact	Commercial, Legal and Risk