Privacy Policy

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	31 August 2026

Section 2 - Purpose

(1) This Policy outlines how the University manages its privacy compliance obligations and its commitment to appropriately manage the personal information it collects and holds about its staff, students, and other individuals with whom it interacts.

Section 3 - Scope

(2) This Policy and Procedure applies to:

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

(3) This Policy and 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/Responsibilities	Role
Receives and investigates privacy complaints	Privacy Officer
Nominated Data Protection Officer (DPO) for the purposes of GDPR	Privacy Officer
Determines that a comprehensive Privacy Impact Assessment (PIA) is required	Privacy Officer
Approves a PIA being undertaken by an external consultant	General Counsel & Director of Assurance
Decision-maker in relation to significant privacy breaches	Chief Operating Officer

This policy document may be varied, withdrawn or replaced at any time. Printed copies, or part thereof, are regarded as uncontrolled and should not be relied upon as the current version. It is the responsibility of the individual reading this document to always refer to La Trobe's Policy Library for the latest version.

Section 5 - Policy Statement

La Trobe's Commitment to Protecting Individuals' Privacy

(4) The University is bound by Victorian privacy legislation (Privacy and Data Protection Act 2014 (Vic) and the Health Records Act 2001 (Vic) and the Information Privacy Principles and Health Information Principles respectively created under those pieces of legislation (privacy principles).

(5) Collectively, the privacy legislation and the privacy principles set out how the University must collect, store, use/disclose and grant access to personal information.

(6) In some instances, the University also has obligations under:

a. the Federal Privacy Act 1988 (Cth) – for certain regulated information, including Tax File Numbers, or when it contractually agrees to comply with this Act, for example under Federal funding and service arrangements;
b. the European Union General Data Protection Regulation (GDPR)- for example, if the University monitors or offers goods and services to individuals in the EU or when it contractually agrees with third parties to comply with the GDPR; and
c. applicable privacy laws of other jurisdictions, such as the UK General Data Protection Regulation, when dealing with personal information that is subject to, or by agreement with third parties to comply with, those privacy laws.

(7) The University is committed to complying with all relevant privacy laws and the protection of the privacy of individuals' personal and health information.

(8) The University will only collect information about individuals where it is necessary, by lawful and fair means and in a non-intrusive way. Personal and health information will also only be collected where required for one or more of the University's functions or activities (e.g. teaching, research and community engagement).

(9) The personal and health information collected will depend on the type of interaction an individual has with the University and will normally be accompanied by a 'collection statement' which sets out prescribed information including the purpose for which the information is being collected and to whom the information will generally be disclosed.

(10) Personal information will usually be collected directly from the individual concerned, for example from:

a. prospective and current students
b. participants or prospective participants in non-award programs of study
c. prospective and current staff
d. members of the University community
e. alumni and donors
f. research participants and collaborators
g. industry partners
h. licensees and tenants
i. sporting clubs and associations e.g. gym members
j. respondents to University goods and services, including enquiries, applicants and bookings
k. employees, contractors and volunteers from other organisations
l. other members of the public who interact with us

(11) Personal information may also be collected from publicly available sources where reasonable and practicable.

(12) Personal data may automatically be collected and processed by the University when an individual visits a campus or uses our websites, mobile applications, Wi-Fi and other online services, examples include:

a. the use of cookies on University controlled websites;
b. connecting to EduRoam, including IP address, location, date and time and online service that was accessed;
c. personal data and images collected via CCTV on campuses.

(13) Personal or health information collected about an individual will only be used and/or disclosed by the University for:

a. the original purpose (primary purpose) for which that the information was collected;
b. for a related secondary purpose (with the exception of sensitive or health information), and where a person would reasonably expect such a use/disclosure;
c. as required or permitted by law; or
d. with an individual's permission or consent.

(14) The University will sometimes use sub-processors (i.e. third party data processors) to store and otherwise assist in the University delivering its services and activities. The University will undertake appropriate due diligence of sub-processors to ensure they are appropriate from a data security and privacy perspective and include appropriate contractual protections.

(15) While privacy legislation focuses on the rights of individuals, the University acknowledges that community standards in relation to privacy can be conceived differently amongst different cultures. Some cultures may place an emphasis on collective rights in relation to information and that privacy interests may not only affect an individual. The University also acknowledges that there will be varying views around what is considered personal and sensitive information, which may not necessarily align with the definitions articulated under current privacy legislation. The University encourages staff to be mindful of community expectations regarding privacy in addition to complying with the law.

(16) The University is committed to being proactive in its approach to privacy protection. The University will assess the privacy impacts of and embed privacy considerations into business processes, including the design and architecture of information technology systems.

(17) The University will use a combination of people, processes and technology safeguards across information, ICT, personnel and physical security to protect information from misuse and loss, and unauthorised access, modification and disclosure.

(18) The University will also endeavour to only hold on to personal and health information for as long as it is required and to destroy or permanently de-identify personal and health information in accordance with the Public Records Act 1973 (Vic) and the relevant Retention and Disposal Authorities and the Records Management Policy.

Responsibilities

(19) All staff, students and other members of the University community have an obligation to comply with this Policy, along with any associated information security, information management or data governance policies.

(20) All individuals are strongly encouraged to raise any privacy concerns or issues with the University Privacy Officer as soon as practicable (privacy@latrobe.edu.au).

(21) Some roles at the University have additional specific responsibilities in relation to privacy compliance, and any one individual may have multiple roles. In particular:

Role	Responsibilities
Chief Data and Analytics Officer	Is responsible for: a. the University's data governance/management framework; b. the University data strategy and the implementation of the strategy; and c. the organisation and management of the University data storage layer and democratisation of data in accordance with this Policy.
Chief Information Officer	Is responsible for: a. technology-related privacy risk management; b. the data retention and destruction framework; c. the digital platforms and applications that create and store data; and d. security of the university digital platforms. e. third-party vendors or cloud service providers, overseeing the relationships, including contract management, and compliance with data security and privacy requirements.
Contract Signatory	In accordance with the University's Contracts Policy, staff who are authorised to execute contracts are accountable for the decision to contract. Contract Signatories are therefore responsible for ensuring that they are satisfied that a contractual arrangement complies or can comply with relevant legislation (including privacy legislation), this Policy and that appropriate contract management arrangements are in place for the life of the Contract, before executing any contract.
Data Owner/Custodians	In accordance with the University's Data Governance Policy and Research Data Management Policy, a Data Custodian (also known as a 'Data Owner') has administrative or operational responsibility for the relevant business domain's data and other information (e.g the Head of HR is responsible for employment information etc). Data Custodians are considered Responsible Officers for privacy legislation for the purposes of the University's Compliance Management Framework. Data Custodians are responsible for ensuring appropriate safeguards are implemented for the protection of personal and health information for which they are responsible. This includes: a. personal and health information collection control management; b. personal and health information use/disclosure control management (including approving any proposed use of personal or health information by other areas of the University internally); c. personal and health information data quality & destruction control management; d. approving the content of any Privacy Impact Check or Assessments where the data/information for which they are responsible is involved in any project or program of work; and e. privacy complaint management/remediation (on advice of University's Privacy Officer).
Data Stewards	Are responsible for supporting the Data Custodians in the day-to-day management of information in accordance with privacy legislation.
Privacy Officer	The University Privacy Officer is responsible for: a. the ongoing review of the University's privacy practices and providing advice to help ensure they comply with this Policy, current legislation and best practice; b. advising and educating individuals of their responsibilities under privacy legislation and this Policy; c. reviewing and providing advice and recommendations on privacy impact assessments d. the receipt and investigation of privacy complaints; e. managing the breach response plan in the event of a privacy data breach; and f. acting as the nominated Data Protection Officer for the purposes of GDPR.
Project Managers	Where a project is involved, Project Managers, are responsible for ensuring a Privacy Impact Check or Privacy Impact Assessment has been completed and approved by the relevant Data Custodian(s) before personal or health information is collected or used as part of any project or program of work and that they are kept up to date throughout the life of a project.
Project Sponsor	Has 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 (as well as meeting its objectives, within the approved budget and delivers the projected benefits). Privacy Impact Checks and Privacy Impact Assessments are intended to assist with evidencing legislative compliance.
Risk, Audit and Insurance Manager	Is responsible for the privacy risk management oversight program.

Consequences for breach

(22) A breach of this Policy may result in disciplinary action, and in serious cases, referral to public agency bodies, such as the Federal or State Information Privacy Commissioners.

Section 6 - Procedures

Part A - Collection of Personal and/or Health Information

(23) 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

(24) 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.

(25) 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 Collection Notice website and should, wherever practicable, be provided to an individual when their personal or health information is first collected.

(26) 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

(27) Individuals generally have the option of not identifying themselves when dealing with the University. 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

(28) 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.

(29) 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 it functions.

(30) 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.

(31) All business areas that are lawfully required to handle government issued 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

(32) 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.

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

Unique Student Identifier (USI)

(34) 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.

(35) 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 (e.g it must not print a USI on a Student ID card).

Part B - Use and Disclosure

(36) '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.

(37) 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

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

Parents/Guardians of La Trobe Students

(39) Student personal or health information should not be provided to parents/guardians 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.

(40) There may be exceptions to requiring express consent from a student before releasing their personal or health information to a parent/guardian — for example, if a student is under the age of 16 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 risks/threats may take priority.

(41) 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

(42) 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 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.

(43) 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.

(44) 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

(45) 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.

(46) 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 that the following details are recorded:

a. to who it was released, when, how;
b. and the name and title of the staff member who approved the release.

Subpoenas and Warrants

(47) 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

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

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

(50) 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

(51) 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.

(52) 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.

(53) 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

(54) In accordance with the University's Contracts Policy, before a contract is entered, the Contract Sponsor is responsible for 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.

(55) 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.

(56) 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

(57) 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

(58) 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.

(59) 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).

(60) 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

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

(62) 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.

(63) 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

(64) 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)	The PIC is a short and mid-level assessment to help identify privacy risks and determine whether a detailed PIA is required. A PIC must be completed where: a. a PTA suggests one is required; b. a new project or program of work involves personal or health information; c. there are substantiative changes to an existing project or program of work that involves personal or health information; d. personal or health information is to be merged, combined or aggregated from other University technologies, processes or programs; e. existing processes which are being renewed that may not have had a privacy assessment previously undertaken.	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 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. PIC's must be kept up to date and revised if the nature/scope of the project or program of work changes. 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.
Privacy Impact Assessment (PIA)	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. A PIA must be undertaken where: a. a PIC result suggests a PIA is required; or b. the Privacy Officer determines one is required.	Project Sponsor/Contract Sponsor (or their nominee) must complete a PIA where one is required. Once a PIA will be completed, the Privacy Officer will make recommendations regarding risk mitigation strategies.

(65) 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.

(66) 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.

(67) 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.

(68) 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.

(69) 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

(70) 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.

(71) More information along with the tools and templates are available via the Privacy Intranet page.

Part G - General Data Protection Regulation (GDPR)

(72) 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.

(73) 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).

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

Part H - Privacy Breach Response

(75) A privacy breach may have occurred when an individual's personal information is subject to loss, unauthorised access, modification, disclosure or other misuse or interference. This can be caused from a cyber-security incident, accidental loss of IT equipment or hard copy documents, information handling practices or improper use of information.

(76) An eligible (reportable) data breach arises when all three of the following criteria occur and should be reported to the relevant Privacy Commissioner by the Privacy Officer:

a. there is unauthorised access or disclosure of personal information, or a loss of personal information that the University holds;
b. it is likely to result in serious harm to one or more individuals; and
c. the University has not been able to prevent the likely risk of serious harm with remedial action.

(77) If a staff member, student or other member of the University community discovers or is otherwise alerted to an actual, potential or suspected privacy breach, they must notify the Privacy Officer on (03) 9479 1839 or privacy@latrobe.edu.au as soon as practicable, and no later than 24 hours after detection. This is also consistent with the University's Compliance Breach Management Policy.

(78) When a breach is notified to the Privacy Officer, the following actions will be undertaken based on the 4 keys steps prescribed by the Office of the Victorian Information Commissioner (OVIC):

a. Contain: the breach immediately to prevent compromise of personal information
b. Assess: the risks of harm to affected individuals by investigating circumstances of the breach

c. Notify: affected individuals if deemed appropriate in the circumstances
d. Review: the breach and the University's response to consider action to prevent future incidents of a similar nature and improve the handling of future breaches

(79) When a notification is made to the Privacy Officer, the individual or business area reporting the incident should take reasonable steps to contain the breach and preserve any information and records that may be required in the investigation, notification and reporting processes.

(80) The Privacy Officer will liaise and assist the relevant and responsible business areas to:

a. determine if a privacy breach has or may have occurred;
b. take all reasonable steps to contain the actual or potential breach as soon as practicable;
c. assess the severity of the actual or potential breach, the likelihood of serious harm and whether the breach is an eligible data breach that needs to be reported to a privacy regulator;
d. investigate the scale, materiality and root cause of the incident;
e. evaluate the risks and determine actions to rectify and mitigate the breach;
f. develop a rectification plan; and
g. report any confirmed breach and actions undertaken to the Corporate Governance, Risk, Internal Audit and Safety Committee (CGRIASC).

(81) The senior manager or head of the relevant business area is responsible for making decisions and undertaking remediation activities in relation to non-eligible data breaches based on advice from the Privacy Officer.

(82) The Privacy Officer will inform the General Counsel & Director of Assurance of any serious or eligible data breaches as soon as practicable. The General Counsel & Director of Assurance will brief the Chief Operating Officer and/or the Vice-Chancellor as appropriate.

(83) The Privacy Officer and/or the General Counsel & Director of Assurance will provide advice and recommendations to the Chief Operating Officer who will act as the decision-maker in relation to any serious, high risk, actual or potential privacy incidents.

(84) Any significant data breaches or cyber incidents will likely trigger a Code Green Incident under the University's Critical Incident and Business Continuity Management Policy.

(85) The Privacy Officer is responsible for notifying relevant privacy regulators as required, and will work with the relevant and responsible areas to determine and assist with:

a. notifying any external affected organisations;
b. taking reasonable steps to notify any affected individuals that are deemed to be 'at risk' in a timely manner; and
c. providing advice on whether other entities such as the police, law enforcement or other regulatory bodies need to be notified.

Part I - Complaints

(86) Individuals may complain to the Privacy Officer about a University act or practice that they believe is an interference with their privacy via privacy@latrobe.edu.au

(87) The Privacy Officer will promptly investigate the complaint and advise the Vice-Chancellor or nominee of their findings and recommendations about the complaint within 30 days of receipt.

(88) Individuals can also make a complaint directly to the Office of the Victorian Information Commissioner (OVIC) and the Health Complaints Commissioner if they have complained to the University and are concerned about or not received a satisfactory response:

a. Office of the Victorian Information Commissioner (OVIC) https://ovic.vic.gov.au/privacy/for-the-public/privacy-complaints/
b. Health Complaints Commissioner https://hcc.vic.gov.au/make-complain

Section 7 - Definitions

(89) 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 domain'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: has the meaning set out in 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: has the meaning set out in the Privacy and Data Protection Act 2014 (Vic) and includes 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

(90) This Procedure is made under the La Trobe University Act 2009.

(91) Associated information includes:

a. Privacy Intranet
b. Privacy Impact Checklist
c. OVIC webpage
d. Contracts Policy
e. Data Governance Policy
f. Records Management Policy

Status and Details

Status	Current
Effective Date	30th August 2023
Review Date	30th August 2026
Approval Authority	Vice-Chancellor
Approval Date	17th August 2023
Expiry Date	Not Applicable
Responsible Manager - Policy	Linda Robertson General Counsel & Director of Assurance
Enquiries Contact	Fiona Rowley Policy Advisor +61 3 9479 1839 Commercial, Legal and Risk

Glossary Terms and Definitions

"student" - Student is defined in the La Trobe University Act 2009 as: (a) a person enrolled at the University in a course leading to a degree or other award; or (b) a person who is designated as a student or is of a class of persons designated as students by the Council.

"staff" - Staff means any person employed by the University as per the definition in the La Trobe University Act 2009 (Vic).