LA TROBE UNIVERSITY — Assurance Group

Assessing Privacy Compliance, Risks and Impacts at La Trobe

To assist in ensuring compliance with Victorian and other privacy legislation applicable to La Trobe University, the key legislative requirements (set out in the 'Information Privacy Principles') should be emedded into the architecture/design of any project/ program of work (project) as early as possible (e.g. before decisions are made about the purchase of platforms) and then on an ongoing basis, including implementation and beyond. This is known as 'privacy by design.'

The following tools are a key part of helping to achieve and evidence privacy by design as they help to identify, assess and then mitigate privacy risks, applying a risk-based approach. These tools should be completed as early as practicable and treated as a live document so that they are updated where a project or its scope changes.

1. For these purposes these privacy tools, a project can include new or existing processes, technology, systems or any program of work that involves personal information.
2. The first step is to complete the Privacy Threshold Assessment (PTA) in Part A below which is a basic assessment consisting of a 4 screening questions. The PTA will determine if a more detailed Privacy Impact Checklist (PIC) is required.
3. The Privacy Impact Checklist (PIC) in Part B below is a mid-level assessment tool to help identify privacy risks so they can be managed. A PIC will also help determine whether a comprehensive Privacy Impact Assessment (PIA) is required.
4. The University's **Privacy Policy** outlines when a PIC must be completed, including where:
   - a PTA suggests one is required;
   - a new project or program of work involves personal or health information;
   - there are substantiative 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 are being renewed and they may not have had a privacy assessment previously undertaken.

PART A: LTU Privacy Threshold Assessment (PTA)

Personal information is defined in the Privacy and Data Protection Act 2014 (Vic) as follows:

"information or an opinion that is recorded in any form (including forming part of a database), whether true or not, about an individual, whose identity is apparent or could be reasonably ascertained from the information or opinion".

Reasonably ascertained is where various pieces of information can be compared, cross-referenced, compiled and matched to enable the identification of an individual.

Does the project you are working on involve any one or more of the following:

Collection of personal information?	◯ Yes	◯ No
Storage of personal information?	◯ Yes	◯ No
Use of personal information (within the University)?	◯ Yes	◯ No
Disclosure of personal information (outside the University)?	◯ Yes	◯ No

If you answered **"Yes"** to any of the questions above, proceed through to the Privacy Impact Checklist (PIC) below.

If you answered **"No"** to all of the questions above, you do not need to proceed with the Privacy Impact Checklist below.

PART B: LTU Privacy Impact Checklist (PIC)

OVERVIEW

This section is intended to provide a high-level snapshot of the project (or program of work) as it relates to privacy and the Information Privacy Principles.

1 Name of project (if any)

---

2 Brief description of project

Please provide a brief outline of the project, which may include:

- *the type of project or program of work, which could be a a new system/process or altering an existing one*
- *what the project is intended to achieve*
- *the stage of development i.e design/conceptual or more advanced*

3 Stakeholders

Please list the key internal and external stakeholders who have an interest in the project, or who will be affected by the project. For example:

Project Sponsor: *the person accountable for the Project*

Project Manager: *the person responsible for ensuring the Project is compliant from a privacy perspective and that all internal processes are followed*

Contract Signatory: *the person accountable for the decision to contract*

Contract Sponsor: *the person proposing the contractual arrangement and responsible for ensuring all pre-contractual steps are followed*

Data Owners/Custodians: *the individual/s responsible for the type of data set(s) involved [hyperlink data custodian list]*

System Owner: *the senior manager responsible for the IT platform/system on an ongoing basis*

System Administrator: *the person who manages access to an IT platform/system*

Any other key stakeholders:

---

4 What types of personal information will be involved in the project? (check all that may apply).

Please note, La Trobe should only collect personal information if it is absolutely necessary and only the mimium amount of personal information required should be collected. Personal information should not just be collected because it might be useful to have in the future.

Contact information. Name, email, phone number

Staff information. Staff number, classification level

Educational. Student ID number, educational history, course and grade information

Identity. Date of birth, numbers or any documents connected to passports, drivers licence, Centrelink, Medicare, visa information

Financial. Bank account details, credit card details, tax file number

Health information. Physical, mental or psychological health of an individual and includes information about a disability and could include medical records, special consideration, Workcover, Counselling or LTU Clinic records.

Sensitive information. Racial or ethnic origin, political opinions, memberships of political associations, religious or philosophical beliefs, membership of professional or trade associations, sexual preferences or practices and criminal record.

Biometric information. Facial or voice recognition, fingerprints, iris scans.

Location information. GPS, wi-fi, geo-fencing features.

Children's information. Information about someone under the age of 18

Other (please state). Photos, videos, voice recordings, CCTV, use of drones, browser cookies etc

---

5 What is the purpose for collecting the personal information, or where personal information is already held by the University, for what purpose was it originally collected?

Please ensure the answer addresses the following:

- *why does/did the University need to collect this information?*
- *what is the project seeking to achieve?*
- *what is the benefit to the University?*
- *what is the benefit to the individuals whose information is being collected?*

Means of collection – *how is the personal information going to be collected/obtained? For example, via an online portal or form, survey, telephone, email, paper-based form, face to face collection, Middleware integration. Include all the ways that personal information may or will be collected.*

Proposed use (i.e. internal use) – *Please specify who will be able to use or access this personal information within the University.*

Proposed disclosure (i.e. external disclosure) (if applicable) – *Please specify whether anyone external to the University will be given access to the personal information and in what circumstances:*

Does the project involve the purchase or implementation of any of the Information Services (IS) related areas below:

IS consultancies;

software licences;

contracts for purchase of ICT hardware or related services;

contracts for software development or maintenance (including applications or website development);

cloud services agreements (including website subscriptions or hosting agreements);

internet service provider or internet usage agreements;

domain name registration or subscription agreements.

If yes, IS need to be involved early in the process as the Chief Information Officer (CIO) is the delegated authority for signing any ICT contracts as per the topics listed above. Please contact contracts@latrobe.edu.au

COLLECTION (IPP 1)

The University must not collect personal information unless the information is necessary for one or more of its functions or activities. It must collect information only by lawful and fair means, and not in an unreasonably intrusive way.

Wherever practicable, a Privacy Collection Notice should be provided to individuals each time their personal information is collected by the University. Collection Notices must contain specific information by law. The University has a number of key Collection Notices which cover a range of common collection scenarios at the University. Wherever possible, when collecting personal information, one of these Collection Notices should be linked to/or provided to the individual concerned at the time of collection. Where the proposed collection of personal information is not covered by one of the University's key Collection Notices, a specific/bespoke Collection Notice should be prepared. Guidance on drafting a Privacy Collection Notice is available via the Privacy Intranet Site

1 Is the collection of personal information necessary for one of the University's functions? ◯ Yes ◯ No ◯ N/A

If yes, please select which University function/s this project relates to:

Research – invention, innovation, education and consultancy

Teaching and learning – our students, graduates and prospective students

Industry - government, partners of choice

Our people – our workforce and alumni

Community – enriching cultural and community life, equity and social justice

The University's functions and objects are set out in part 5 of the La Trobe University Act 2009

2 Is each piece of personal information being collected absolutely necessary for this project to collect and have access to? ◯ Yes ◯ No ◯ N/A

3 **Is the proposed collection of personal information covered by an existing Collection Notice on the La Trobe Privacy Collection Notice webpage?** ◯ Yes ◯ No ◯ N/A

If yes, please specify which Collection Noticethis project is covered by:

4 **If the answer to to question 3 was 'no', has a specific/bespoke Collection Notice been developed?** ◯ Yes ◯ No ◯ N/A

If yes, please provide attach a copy of the Collection Notice to this document.
Guidance on preparing a Privacy Collection Notice is available via the Privacy Intranet Site.

If no, please explain why a Collection Notice has not been developed or is not required:

5 **Do any of the following apply:** ◯ Yes ◯ No ◯ N/A

a. personal information will be collected or processed in the European Union.
b. goods or services will be offered to individuals located in the European Union.
c. individuals in the EU will be monitored/profiled as part of the project.

USE AND DISCLOSURE (IPP 2)

Personal information should only be used (internally) and/or disclosed (externally) for the purpose for which it was originally collected as set out in the original Collection Notice (the 'primary purpose') or for a secondary purpose connected to the primary purpose and where a person would reasonably expect their information to be used in that manner.

Does the project involve the use of existing personal information by the University for a new purpose (i.e. one that is different to the purpose for which it was originally collected)? ◯ Yes ◯ No ◯ N/A

Does the project create a new or changed way of transferring personal information between ◯ Yes ◯ No ◯ N/A

i) different areas of the University; or
ii) between different systems used by the University; or
iii) between the University and an external agency/entity?

Will personal information be used for research or statistics? ◯ Yes ◯ No ◯ N/A

Will personal information be used to make decisions or take action against individuals in ways which can have a significant impact on them (for example, whether to receive a service or benefit from the University or automated decision making)? ◯ Yes ◯ No ◯ N/A

Will personal information from multiple LTU sources/databases be combined, compared, or matched? ◯ Yes ◯ No ◯ N/A

Will personal information that was previously managed separately be aggregated and/or stored together? ◯ Yes ◯ No ◯ N/A

Will personal information be linked, matched or cross-referenced with other data sources (e.g. to create a profile)? ◯ Yes ◯ No ◯ N/A

DATA QUALITY (IPP 3)

LTU must take reasonable steps to ensure the personal information it collects, uses or discloses is accurate, complete and kept up to date.

What steps will be taken to ensure the personal information used in this project is accurate, complete and kept current/up to date?

DATA SECURITY (IPP 4)

LTU must take reasonable steps to protect the personal information it holds from misuse, loss, unauthorised access, modification or disclosure and destroy or permanently de-identify personal information when it is no longer needed (i.e. when no longer required to be retained pursuant to the Public Records Act).

Will a new or amended way of storing, securing or retaining personal information be created?	◯ Yes	◯ No	◯ N/A
Is the system accessible via Single Sign on?	◯ Yes	◯ No	◯ N/A
Is data encrypted in transit and at rest?	◯ Yes	◯ No	◯ N/A
Does this system have role-based permission access levels?	◯ Yes	◯ No	◯ N/A
Will the personal information be provided to 'new' users who do not currently have routine access to this type of information?	◯ Yes	◯ No	◯ N/A
Does this system produce audit logs and trails which can demonstrate which roles have accessed the personal information?	◯ Yes	◯ No	◯ N/A
Where a new third-party platform is involved, will the vendor be engaging any subcontractors that will have access to any University data or information?	◯ Yes	◯ No	◯ N/A
Can this system integrate and export records to the University's Electronic Document Management System (EDMS) which is Content Manager?	◯ Yes	◯ No	◯ N/A
Can this system export records from this system in a universal format such as excel, PDF?	◯ Yes	◯ No	◯ N/A
Can LTU users upload any type of files which may include attachments, emails, case notes, images, scanned documents to this system?	◯ Yes	◯ No	◯ N/A
Does this project connect, use, share, receive or disclose personal information with anexisting University system?	◯ Yes	◯ No	◯ N/A
Will this project use Middleware to transfer or ingest information to or from any other LTU related systems?	◯ Yes	◯ No	◯ N/A
Will this project have a test or training environment/sandbox for users and/or user acceptance testing?	◯ Yes	◯ No	◯ N/A
Where a new third-party platform is involved, does the vendor have official third-party certification i.e ISO27001, PCI DSS, Soc2?	◯ Yes	◯ No	◯ N/A

ACCESS AND CORRECTION (IPP 6)

Individuals have the right to seek access to their own personal information and to make corrections to it if necessary.

Can an individual opt-out or request that their personal information not be used or stored (right to be forgotten)? ◯ Yes ◯ No ◯ N/A

Can an individual's personal information be accessed and easily extracted if a Freedom of Information (FOI) request, warrant or subpoena is received? ◯ Yes ◯ No ◯ N/A

UNIQUE IDENTIFIERS (IPP 7)

Use of unique identifiers is only allowed where an organisation can demonstrate that the assignment is necessary to carry out its functions efficiently. There are also restrictions on how organisations can adopt unique identifiers assigned to individuals by other organisations. An identifier can be a sequence of numbers, letters and/or characters used to identify or refer to a person.

Does this project create or use an existing unique identifier issued by the University e.g staff or student number? ◯ Yes ◯ No ◯ N/A

Does this project use or disclose a unique identifier assigned by another organisation e.g drivers licence, passport number, TFN? ◯ Yes ◯ No ◯ N/A

Will any unique identifiers be used to match or link pieces of personal information? ◯ Yes ◯ No ◯ N/A

ANONYMITY (IPP 8)

Where lawful and practicable, individuals should have the option of transacting with an organisation without identifying themselves.

Can an individual request to remain anonymous in this project? ◯ Yes ◯ No ◯ N/A

TRANSBORDER DATA FLOWS (IPP 9)

Organisations can only transfer personal information outside Victoria in certain circumstances, for example, if the individual consents, or if the recipient of the personal information is subject to a law or binding scheme that is substantially similar to the Victorian IPPs.

Will any of the information in this project/system be stored or hosted outside of Victoria (for example, by publishing information to a website or via the use of cloud services hosted interstate/overseas?) ◯ Yes ◯ No ◯ N/A

If, yes please list which State/Country:

RECORDS MANAGEMENT

Please contact Records Management via records@latrobe.edu.au for advice on the prescribed retention period under the Public Records Keeping Act 1973 (Vic) for the types of records this system will be handling prior to completing this section.

A record is defined as any and all information created, maintained, sent or received whilst carrying out your work. Public records can include emails, minutes, letters, memos, reports, information in a database and be created in a range of formats, including hardcopy and digital.

Will this system be used to store University records? ◯ Yes ◯ No ◯ N/A

The retention period for these records is:

Can this system integrate with the University's approved Electronic Document Management System (eDMS) which is Content Manager (previously called TRIM)? ◯ Yes ◯ No ◯ N/A

Can records be set for archiving or deletion directly in this system after a set period of time e.g after 3 years etc? ◯ Yes ◯ No ◯ N/A

Can records be directly deleted from this system if an individual makes a 'right to be forgotten' request? ◯ Yes ◯ No ◯ N/A

Are there measures in place to ensure that the information is de-identified or destroyed when no longer required? ◯ Yes ◯ No ◯ N/A

VENDOR, CONTRACTS AND DELEGATIONS

Does the vendor have a Privacy Policy? ◯ Yes ◯ No ◯ N/A

Please provide link:

Does the vendor have a Data Breach Response Plan? ◯ Yes ◯ No ◯ N/A

Please provide link:

Has Legal Services reviewed the contract (if applicable) as per the Contracts Policy? ◯ Yes ◯ No ◯ N/A

Will the University have the right to conduct audits if the data is being held/stored by a third party? ◯ Yes ◯ No ◯ N/A

If this system is part of an outsourcing arrangement, is it clear with the vendor that the ownership of the data and records resides with the University and that we have the right to have the data returned or destroyed when the contract ends? ◯ Yes ◯ No ◯ N/A

NOTE:

Please send through your completed checklist to the University Privacy Officer at privacy@latrobe.edu.au

The Privacy Officer will review your answers to the questions and will work with you in identifying the possible privacy impacts. Additional information may be required if a more comprehensive privacy impact assessment needs to be undertaken.

At any time you can contact the University Privacy Officer on (03) 9479 1839 or privacy@latrobe.edu.au for advice.

Declaration:

I declare that to the best of my knowledge the information provided in the preparation of this Privacy Threshold Assessment and Privacy Impact Checklist is true and accurate at the time provided.

Person completing this assessment:

_____

Project Owner/Sponsor:

_____

This Privacy Impact Checklist will be kept under review by:

_____

Date d d | m m | y y y y