Privacy - Personal Information Policy

Section 1 - Background and Purpose

Preamble

(1) The Privacy and Data Protection Act 2014 applies to public bodies established for a public purpose under an Act. It provides that an act done or practice engaged in by an organisation is an interference with the privacy of an individual if the act or practice is contrary to, or inconsistent with, an Information Privacy Principle ('IPP'). The names of this and subsequent sections will vary and will be dependent on the actual processes to be followed.

(2) The Privacy Act 1988 does not generally apply to the University, however the University is electing to incorporate the standards of the Australian Privacy Principles (APPs) into its Privacy Procedures where appropriate.

(3) The University is bound by privacy legislation in accordance with the Information Privacy Principles in the Privacy and Data Protection Act 2014. The University also has obligations under some agreements, grants and other funding arrangements to adhere to the Australian Privacy Principles, contained within the Privacy Act 1988. Collectively, these Principles stipulate how the University should collect, store, disclose and give access to personal information.

(4) The University is a tax file number recipient and is required to comply with the Privacy (Tax File Number) Rule 2015.

(5) The University may also have obligations under the General Data protection Regulation (GDPR) where processing activities fall within the scope of GDPR.

Purpose

(6) This Policy and Procedure:

a. governs the management of personal information (including sensitive information) by the University;
b. informs staff and students about how the University manages personal information;
c. outlines how an individual can make a complaint if they believe there has been an interference with their privacy;
d. outlines the Data Breach Response Plan in circumstances where an actual or potential privacy data breach is identified.

Section 2 - Scope

(7) This Policy and Procedure applies to all:

a. Employees
b. Contractors, and
c. Volunteers

(8) This Policy and Procedure applies to all organisational areas of the University in relation to the collection, use, storage, disclosure and access to personal information of past and present University staff, students and other individuals associated with the University.

(9) This Policy and Procedure does not cover the management of health information. The management of health information is covered by the Health Records Act 2001 and the Health Privacy Principles and by the University's Privacy - Health Information Policy.

(10) Nor does this Policy and Procedure apply to personal information that is:

a. publicaly available;
b. kept in a library, art gallery or museum for reference, study or exhibition purposes;
c. a public record under the control of the Keeper of Public Records that is available for public inspection; or
d. an archive within the meaning of the Commonwealth Copyright Act 1968.

Section 3 - Policy Statement

(11) The University is committed to the protection of the privacy of personal information and will manage personal information in accordance with relevant privacy laws.

(12) The University aims to be proactive in its approach to privacy protection and will assess the privacy impacts of major initiatives and projects and embed privacy considerations into the design and architecture of information technology systems and business processes.

Section 4 - Procedures

Part A - Australian Privacy Principles

(13) The University will manage personal information in accordance with the Australian Privacy Principles (APPs), unless either:

a. the APPs are silent with regards to a matter under the IPPs; or
b. the IPPs require a behaviour or action by the University that the University considers to be a higher standard than the requirement of the APP. This standard is a matter for the University to decide at its discretion.

Tax File Numbers

(14) The University is a Tax File Number (TFN) recipient and must comply with the Privacy (Tax File Number) Rule 2015. The TFN Rule only applies to the TFN information of individuals and does not apply to TFN information about other legal persons including corporations, partnerships, superannuation funds and trusts. This Rule defines how the University handles TFN information including the collection, use, disclosure, storage and secure destruction of such information.

(15) The University must only request, collect and use TFN information from individuals and other TFN recipients for a purpose authorised by taxation law, personal assistance law or superannuation law.

(16) At the time of collection, the University must take reasonable steps to ensure individuals are informed:

a. which law authorises the University to collect the TFN;
b. the purpose for which the TFN is requested or collected;

c. that declining to provide a TFN is not an offence;
d. about the consequences of declining to quote a TFN.

(17) The University must also take reasonable steps to:

a. protect TFN information from misuse, loss, unauthorised access, use, modification or disclosure;
b. restrict access to TFN records to authorised individuals who need to handle that information for taxation law, personal assistance law or superannuation law;
c. securely destroy or permanently de-identify TFN information where it is no longer required to be retained by law or necessary for a purpose under taxation law, personal assistance law or superannuation law.

Part B - Information Collected by the University

(18) The University will:

a. only collect personal information that is necessary for, or directly related to, one or more of its functions or activities;
b. only collect sensitive information about an individual if the individual has consented, the collection is required or permitted under law (e.g. collection of statistics for a government agency) or the collection is otherwise in accordance with the relevant privacy principle/s; and
c. unless unreasonable or impracticable to do so, or the individual consents to the collection of information from someone other than the individual, the University will only collect personal information about an individual from that individual.

Information at Point of Collection

(19) Where the University collects personal information from an individual, it will take reasonable steps in the circumstances to notify the individual of:

a. the purposes for which the information about the individual is collected;
b. to whom the organisation usually discloses information of that kind;
c. any law that requires the particular 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, and if so, the countries in which such recipients are likely to be located (where practicable); and
f. the University's Privacy Policy and that the Policy 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;
    ii. seek correction of that information; or
    iii. complain about a breach of the individual's privacy and how the University will deal with such a complaint.
    iv. how to contact the University's Freedom of Information/Privacy Officer.

(Note: This clause will not apply to the extent that compliance with it would pose a serious threat to the life or health of any individual)

Use and Disclosure

(20) The University will:

a. not use or disclose personal information about an individual for a purpose other than the original purpose of collection except in accordance with the relevant privacy principle/s or as otherwise permitted by law;
b. as required by Section 6(1) of the Privacy and Data Protection Act 2014, interpret IPP 4.2 regarding destruction or permanent de-identification of personal information subject to the University's obligations under the Public Records Act 1973.
c. as required by Section 14 of the Privacy and Data Protection Act 2014, interpret IPP 6 regarding an individual's rights to access to, and correction of, personal information subject to the procedures contained in the Freedom of Information Act 1982.

Security of Personal Information

(21) The University holds personal information securely and such information may only be accessed by authorised users.

(22) The University will take reasonable steps and precautions to safeguard personal information we hold from loss, theft and unauthorised use, disclosure or modification. Personal information held by us is protected by a number of physical and electronic safeguards including:

a. Using measures such as firewalls, data encryption, virus detection methods, and password restricted access to prevent unauthorised access to our online and computerised systems;
b. Restricting access to storage areas via the use of staff ID cards;
c. Providing staff with training on how to handle personal information in accordance with this Policy and applicable privacy laws;
d. Ensuring that third parties who use or store any personal information adopt appropriate security measures;
e. The secure destruction of records is in accordance with the Records Management Policy.

Cross-border Disclosures

(23) In some circumstances, the University may disclose personal information to a third party which is outside Australia. In such circumstances, the University will take reasonable steps to ensure that the overseas third party does not breach the relevant privacy principle/s.

Access to Personal Information and Correction of Personal Information

(24) To find out further information, to access personal information held by the University or to seek the correction of personal information held by the University, the individual may contact the Freedom of Information/Privacy Officer via foi@latrobe.edu.au

(25) Where applicable, the Freedom of Information/Privacy Officer will respond to any 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.

(26) Fees may be charged by the University for access to personal information unless the University expressly decides to waive this fee. For current University fees, see the Freedom of Information Webpage.

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

Part C - University's Privacy Officer

(28) The responsibilities of the University's Freedom of Information/Privacy Officer will include:

a. ongoing review of the University's practices and procedures to ensure that they comply with this Procedure, current legislation and best practice;
b. reviewing this Procedure and advising and educating University management and staff of their responsibilities under this Procedure, the Privacy and Data Protection Act 2014 and the Health Records Act 2001;
c. the receipt and investigation of complaints; and
d. the responsibilities assigned to Responsible Officers as outlined in the Compliance Management Policy.

(29) To find out further information, to access personal information held by the University or to seek the correction of personal information held by the University, please contact:

> Freedom of Information /Privacy Officer
> La Trobe University
> Bundoora Victoria 3086
>
> T: +61 (03) 9479 1839
>
> F: +61 (03) 9479 1045
>
> E: privacy@latrobe.edu.au
>
> W: Privacy Webpage

Part D - Data Protection Officer – GDPR

(30) The University Privacy Officer is the nominated Data Protection Officer for the purposes of GDPR. EU data subjects should submit any requests or correspondence in relation to their rights as an EU data subject to the Data Protection Officer via dpo@latrobe.edu.au

Part E - Complaints

(31) Any individual in respect of whom personal information is or has been held by the University may complain to the University's Privacy Officer about an act or practice of the University that the individual believes is an interference with the privacy of that individual.

(32) 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.

(33) The Vice-Chancellor or nominee will make a decision on the complaint and advise the complainant in writing of the result of the investigation.

Part F - Privacy Breach Response Plan

(34) 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 as a result of a malicious breach of the secure storage, information handling protocols or human error amongst others. For example a cyber-security incident, accidental loss of IT equipment or hard copy documents, negligence, improper disclosure of information, or otherwise.

(35) Where a 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 reasonably practicable, or in any event within 24 hours of detection . This is also in accordance with the University's Compliance Management Policy.

(36) The Privacy Officer upon receipt of the notification will in consultation with relevant areas, including IS, Risk Management Office and Legal Services:

a. determine whether a privacy breach has or may have occurred;
b. assess the severity of the breach (actual or potential);
c. assess the risks and likelihood of serious harm;

(37) The Privacy Officer in conjunction with the responsible business area(s) will manage the breach response process which will include:

a. Liaising with relevant departmental stakeholder(s) to contain the breach as soon as practicable;
b. Informing the General Counsel & Director of Assurance of the issue as soon as practicable. Depending on the nature of the breach/potential breach, the General Counsel & Director of Assurance will inform the Chief Commercial Officer, Chief Operating Officer and/or Vice-Chancellor. Where deemed necessary the University's Critical Incident Management Policy will be instigated;
c. Undertaking any necessary investigations to assess the scale and materiality of the issue;
d. In consultation with Assurance and Risk, evaluating the risks and determining any additional and necessary actions to rectify and mitigate the breach;
e. Liaising with the relevant department(s) and stakeholders in compiling a rectification plan which will:
    i. Identify the root cause of the breach
    ii. Identify actions required to mitigate the breach
    iii. Identify actions required to prevent a reoccurrence
f. Presenting the written Responsible Officer - Breach Assessment Form which includes the remediation and prevention plan to the General Counsel & Director of Assurance for approval.
g. Reporting any confirmed breach and its remediation in the quarterly breach report to the Corporate Governance, Audit and Risk Committee (CGARC).

(38) The University is an entity that is covered by Victorian Privacy Legislation, however there are some instances where the University has obligations under the Privacy Act 1988 (Cth) and the General Data Protection Regulation (GDPR).

(39) In addition, if a breach is identified as a an eligible data breach under the Privacy Act 1988 and relates to an agreement, tax file number, grant, contract or other funding arrangement where the University has agreed or is obliged to adhere to the Australian Privacy Principles, the Privacy Officer will also be responsible for:

a. Informing the General Counsel & Director of Assurance and/or Chief Commercial Officer of the issue as soon as practicable and where deemed necessary the University's Critical Incident Management Policy will be instigated;
b. Notifying the effected organisation (as/where applicable) and working on an appropriate response which may include:
    i. Notifying the Office of the Australian Information Commissioner (OIAC) of the breach;
    ii. Taking reasonable steps to notify any affected individuals that are deemed to be 'at risk' in a timely manner, where it is practicable to do so.

(40) An eligible data breach arises when the following three criteria are satisfied:

a. There is unauthorised access or disclosure of personal information, or a loss of personal information that the University holds; and
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.

(41) Refer to the Data Breach Response Quick Reference Guide for guidance on the privacy incident response and reporting plan.

Section 5 - Definitions

(42) For the purpose of this Policy and Procedure:

a. Health information: Health information has the meaning set out in section 3 (1) of the Health Records Act 2001. 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 him or her;
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 his or her descendants.
b. Personal information: means 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.
c. Sensitive information: means 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.
d. Serious harm: may include physical, psychological, emotional, financial or reputational harm.

Status and Details

Status	Current
Effective Date	7th September 2018
Review Date	7th September 2021
Approval Authority	Vice-Chancellor
Approval Date	30th August 2018
Expiry Date	Not Applicable
Responsible Policy Officer	Taryn Rulton Chief Commercial Officer
Author	Fiona Rowley +61 3 9479 1839
Enquiries Contact	Fiona Rowley Policy Advisor +61 3 9479 1839 Commercial, Legal and Risk