Privacy Policy

1. Purpose

The purposes of this Policy are to:

(a) ensure that Personal Information collected or held by the University is managed in accordance with good global privacy practice, the Privacy Act 2020, other relevant laws, the principle of manaakitanga, and the University's Privacy Notice; and

(b) ensure that individuals have trust and confidence in the University's ability to manage and secure their Personal Information.

2. Application of Policy

Privacy is everyone's responsibility. This Policy applies to:

(a) Staff Members who may be required to collect, access, use or disclose Personal Information, who may manage projects or systems that impact on Personal Information management, or who are responsible for making policy decisions about the way the University manages Personal Information;

(b) Students who collect, access, use or disclose Personal Information in the course of their studies or research or are otherwise permitted access to Personal Information held by the University.

This Policy should be read alongside the University's privacy notice and is supported by the Privacy Breach Procedures, Privacy Impact Assessment Guidelines and the Disclosure of Personal Information Procedures. All together, these documents form the University's Privacy Framework.

Policy Content

3. Collection of information

3.1 Personal Information must only be collected for a Lawful Purpose and to the minimum extent necessary for that purpose.

3.2 Personal Information must be collected from the Individual directly, unless an exception can be used to collect it from a third party.

Note: Exceptions are listed in principle 2 of the Privacy Act 2020

3.3 When Personal Information is being collected from an Individual, the Individual must be referred, or provided with a link, to the Privacy Notice or a specific privacy notice relating to the particular collection.

Note: The Privacy Officer can assist with the development of a specific privacy notice if the University's Privacy Notice is not appropriate for the particular collection of personal information.

4. Use and disclosure of information

4.1 Personal Information may only be used by the University or disclosed to another person where that use or disclosure is:

(a) necessary for the Lawful Purpose for which it was collected and made clear to the individual in the Privacy Notice (or a specific privacy notice relating to the particular use or disclosure); or

(b) otherwise permitted or required by law.

Note: A use or disclosure may be permitted if the University is able to rely on an exception to principle 10 (use) or principle 11 (disclosure) of the Privacy Act 2020. If this is not clear, consult the Privacy Officer. In certain circumstances (such as a request for access to Personal Information, a request under the Official Information Act 1982 or the serving on the University of a Production Order under the Search and Surveillance Act 2012), the University may be required by law to disclose information.

Note: See the Disclosure of Personal Information Procedures.

4.2 Before using or disclosing Personal Information, Staff Members and Students must take reasonable steps to ensure that the Personal Information is accurate and up to date particularly where the use or disclosure could impact on the rights and interests of an Individual.

4.3 Before Personal Information is disclosed to a contracted service provider or an overseas recipient, the person responsible for that disclosure must ensure:

(a) that the service provider or overseas recipient is required and able to provide an adequate level of protection for the Personal Information shared; or

(b) that the Individual has given their express consent to the disclosure.

Note: See the Disclosure of Personal Information Procedures. It will be sufficient compliance with this clause for there to be a cross-border information sharing agreement in place between the University and the overseas recipient. Digital Solutions, the Research Office and/or Legal Services can assist with this or provide further advice.

5. Access and correction

5.1 Every Individual (or their authorised representative) has the right to request access to the Personal Information the University holds about them, or to ask the University to update or correct their Personal Information if they consider changes need to be made.

5.2 Any request for access should be made or referred to the University's Privacy Officer.

6. Security and retention

6.1 All Staff Members are responsible for protecting the Personal Information they handle against loss, misuse, or unauthorised access, modification or disclosure.

6.2 Staff Members must:

(a) Ensure they have read and understood the University's information technology policies, including the Acceptable Use of Information Systems Statute and Information Security Policy;

(b) Only access or use Personal Information where this is necessary for a legitimate university purpose and in accordance with the Privacy Notice or any relevant specific privacy notice;

(c) Not retain Personal Information for longer than the University has a Lawful Purpose to use it;

(d) Delete or destroy Personal Information in accordance with the minimum retention period in the University's General Disposal Authority.

7. Privacy impact assessments

7.1 Wherever possible, the University endeavours to take a "privacy by design" approach to the development of new or changed processes or systems. This means that the University will proactively embed privacy into the design and operation of its processes or systems.

7.2 Any Staff Member responsible for creating or changing a process or system that involves a new or changed collection, use or disclosure of Personal Information or that may impact the security or integrity of Personal Information already held by the University, must undertake a Privacy Impact Assessment.

Note: See the Privacy Impact Assessment Guidelines and the Privacy Impact Assessment Template.

8. Privacy breaches

8.1 Any person who causes or discovers a Privacy Breach must report that breach to their line manager and/or the Privacy Officer as soon as practicable.

8.2 Where the Privacy Breach is or may also be an IT security incident, that breach must also be reported to the Director Digital Solutions.

8.3 Privacy Breaches must be managed in accordance with the University's Privacy Breach Procedures.

9. Roles and responsibilities

9.1 Managers are responsible for:

(a) implementing and operating this Policy within their faculties, schools, institutes and units;

(b) ensuring that Privacy Breaches and other privacy issues are identified and managed, and that privacy impact assessments are undertaken, in accordance with this Policy; and

(c) supporting Staff Members to understand and comply with this Policy and participate in any privacy training provided by the University.

9.2 Staff Members and Students are responsible for:

(a) complying with this Policy;

(b) actively participating in relevant privacy training provided by the University; and

(c) informing their manager and/or the Privacy Officer of any requests for access to Personal Information, Privacy Breaches or other privacy issues.

9.3 The Privacy Officer is responsible for:

(a) supporting Staff Members to understand and comply with this Policy, including by providing and maintaining relevant training, procedures, and guidelines;

(b) managing requests for access to Personal Information, Privacy Breaches, privacy complaints and other privacy issues;

(c) developing and maintaining processes for giving effect to this Policy (including responding to Privacy Breaches);

(d) reporting on Privacy Breaches and other privacy issues to the Vice-Chancellor and the Audit & Risk Committee; and

(e) Liaising with third parties in relation to privacy matters, including the Privacy Commissioner and other regulators.

Definitions

In this Policy, unless the context otherwise requires:

Individual:	any person about whom the University collects and holds personal information and includes students, Staff Members, contractors, alumni, donors, and visitors to the University's websites or campuses. *Note: The term "Individual" comes from the Privacy Act 2020 and is synonymous with the global term "Data Subject". This Policy uses "Individual" rather than "Data Subject" for plain language purposes*
Lawful Purpose	a purpose that is directly connected with any of the University's lawful functions or activities and includes the purposes stated in the Privacy Notice.
Personal Information	any information, whether electronic or hard copy, about an Individual whether or not the information directly identifies the Individual. Personal Information includes, but is not limited to, contact, demographic, health and academic information (including grades), CCTV footage, staff HR and performance information, emails and other correspondence, and opinions about the Individual.
Privacy Breach	an event (whether intentional or unintentional) in which: (a) Personal Information is lost or is accessed, altered, disclosed or destroyed without authorisation; (b) Personal Information is at increased risk due to poor security safeguards; or (c) The University is prevented (whether permanently or temporarily) from accessing the Personal Information that it holds. Privacy breaches include, but are not limited to: (d) accidental disclosure of Personal Information to the wrong recipient; (e) a Staff Member or Student accessing Personal Information without a legitimate University reason; (f) an external attack on a University system; and (g) a lost or stolen University device or document.
Privacy Framework	the Privacy Notice, any specific privacy notice, this Policy, the Privacy Breach Procedures, the Privacy Impact Assessment Guidelines, and the Disclosure of Personal Information Procedures.
Privacy Notice	the privacy notice published by the University that describes how the University collects, uses, and shares Personal Information.
Staff Member	an employee of the University.
Student	any person enrolled in a personal course of study at the University, or a person who is studying at the University under an exchange agreement with another institution, and includes a resident in a Hall of Residence.
University	Victoria University of Wellington.

Related Documents and Information

10. Related Documents

Acceptable Use of Information Systems Statute
Access and Use of Victoria University of Wellington's Relationship Management Database (RMD) Policy
Disclosure of Personal Information Procedures
Education and Training Act 2020
Health Information Privacy Code 2020
Human Ethics Policy
Human Ethics Policy Guidelines
Information Security Policy
Privacy Act 2020
Privacy Breach Procedures
Privacy Impact Assessment Guidelines
Privacy Impact Assessment Template
Privacy Notice
Public Records Act 2005
Records Management Policy
Staff Conduct Policy
Student Conduct Statute
Victoria University of Wellington Act 1961

11. Document Management and Control

Approver	Vice-Chancellor
Approval Date	1 December 2020
Effective Date	1 December 2020
Last Modified	8 December 2020
Review Date	1 December 2023
Sponsor	Chief Operating Officer
Policy Owner	General Counsel & Privacy Officer