Privacy Breach Procedures

1. Purpose

The purpose of these Procedures is to ensure that Privacy Breaches are managed in accordance with the University's Privacy Policy and in compliance with the University's obligations under the Privacy Act 2020, including privacy breach notification requirements.

These procedures are intended to ensure transparency and accountability, not blame. All staff members and students should feel safe to speak up. Once alerted to a privacy breach, the University can take steps to manage it. The procedure requires speed, care and collaboration. It is important to include the right people at the right time.

2. Application

Privacy is everyone's responsibility. These Procedures apply 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; and

(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.

Procedures

Step 1: Report

3.1 Any person who causes or discovers a Privacy Breach must, as soon as practicable after becoming aware of it, report the breach to:

(a) their line manager or supervisor; and/or

(b) the Privacy Officer.

Note: Breaches can be reported to the Privacy Officer

3.2 Where the privacy breach is (or may be) also an IT security incident, the breach must also be reported to the Director, Digital Solutions.

Step 2: Evaluate and contain

3.3 The Privacy Officer must, on receipt of a report and in liaison with the relevant manager and other staff members as appropriate, determine the scope of the Privacy Breach, including:

(a) identifying the types of Individuals affected

(b) identifying the type and sensitivity of the Personal Information at risk

(c) evaluating the likelihood of harm to the Individuals affected

3.4 The relevant manager must, under the guidance of the Privacy Officer, determine what steps, if any, are required to contain the Privacy Breach, including steps that the affected Individuals might take.

Step 3: Notify

3.5 The Privacy Officer must determine whether the Privacy Breach is a Notifiable Privacy Breach

Note: Factors that may be relevant to this determination include the sensitivity of the personal information involved, the number of individuals affected, the distribution of the information and the nature of the recipient, and the ability to contain the breach or its consequences.

3.6 Where the Privacy Officer has determined that the Privacy Breach is a Notifiable Privacy Breach, the Privacy Officer must prepare notifications to the Privacy Commissioner, or any other relevant regulator, and the Individuals affected by the breach.

3.7 Privacy breach notifications must be made to the Privacy Commissioner and Individuals affected by the breach as soon as reasonably practicable after the University has become aware of the privacy breach.

3.8 Notification to the Privacy Commissioner may only be made by the Privacy Officer (or nominee). Notification to Individuals affected by the breach should usually be made by the relevant manager or as otherwise agreed with the Privacy Officer.

Step 4: Prevent

3.9 The Privacy Officer (or nominee) will investigate the reasons for the Privacy Breach. If the Privacy Breach is also an IT Security Incident, the investigation will be carried out by the Director, Digital Solutions (or nominee).

3.10 Investigation findings must be reported to the Chief Operating Officer who will consider them and determine what, if any, action is to be taken to prevent a similar breach in the future.

Definitions

In this Procedure, 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*
IT Security Incident	includes attempted or successful unauthorised access, use, disclosure, modification or destruction of information, interference with IT operations, impersonation of any member of the University community through electronic and/ or social media, spoofing, or setting up any web presence (including presence on social media) that purports to be, or might reasonably be perceived to be, an official Victoria University of Wellington website or social media group, page or account
Notifiable privacy breach	a privacy breach that has caused, or is likely to cause, Serious Harm to an Individual.
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; (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 purpose (f) an external attack on a University system (g) a lost or stolen University device or document
Serious Harm	serious harm as assessed in accordance with section 113 of the Privacy Act 2020
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

3. Related Documents

Education and Training Act 2020
Health Information Privacy Code 2020
Information Security Policy
Privacy Act 2020
Privacy Policy
Privacy Notice

4. Document Management and Control

Approver	Chief Operating Officer
Approval Date	8 December 2020
Effective Date	8 December 2020
Last Modified	N/A
Review Date	1 December 2023
Sponsor	Chief Operating Officer
Policy Owner	General Counsel & Privacy Officer