

## PRIVACY BREACH MANAGEMENT PROCEDURES

<b>Category</b>	Governance
<b>Procedures Owner</b>	General Counsel
<b>Last review</b>	November 2024
<b>Next review</b>	November 2029
<b>Approved by</b>	Vice Chancellor
<b>Effective date</b>	November 2024

### 1. PURPOSE

The purpose of these procedures is to ensure that Privacy Breaches that occur at AUT (**University**) are managed in accordance with the Privacy Policy, Privacy Procedures and in compliance with obligations under the Privacy Act 2020.

### 2. SCOPE

These procedures apply to all members of the University. In particular:

Staff 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

Students who collect, access, use or disclose Personal Information in the course of their studies, research or with authorised permission.

### 3. DEFINITIONS

**Individual Concerned:** in relation to Personal Information, means the individual to whom the information relates.

**Notifiable Privacy Breach:** a Privacy Breach that has caused, or is likely to cause, Serious Harm to an individual.

**Personal Information:** means any information about an identifiable individual. The information does not need to name someone specifically if they are identifiable in other ways. This can include (but is not limited to): name, contact details, date of birth, image, log in details, opinion, employment information, health information and financial information.

**Privacy Breach:** an event when an organisation or individual either intentionally or accidentally:

- (a) provides unauthorised or accidental access to someone's Personal Information;
- (b) discloses, alters, loses, or destroys someone's Personal Information; or
- (c) a Privacy Breach also occurs when someone is unable to access their Personal Information (for example, their account being hacked).

<b>Privacy Officer:</b>	means:
	(a) for matters related to staff, the Group Director – People & Culture; or
	(b) for matters related to students, the Group Director – Student Services & Administration.
<b>Serious Harm:</b>	means as assessed in accordance with section 113 of the Privacy Act 2020.
<b>University:</b>	means the Auckland University of Technology and includes all subsidiaries.

#### 4. ACTIONS

Wherever possible, the Privacy Breach must be contained. If the breach involves a computer system, contact the Chief Information Officer for containment recommendations.

An Individual Concerned, or any person made aware of a Privacy Breach, may download a Privacy Breach Notification Form, and send to a Privacy Officer. The University's Privacy Officers are:

- For matters related to staff, the **Group Director – People & Culture**
- For matters related to students, the **Group Director – Student Services & Administration**

Privacy Officers will discuss with General Counsel to determine if a Notifiable Privacy Breach has occurred and whether the University must notify the Privacy Commissioner.

Discuss with the University's General Counsel to determine whether notifying to the Privacy Commissioner is required. NotifyUs can also be used.

Notifiable Privacy Breaches must be notified to the Privacy Commissioner and Individual(s) Concerned as soon as practicable. The Privacy Commissioner should be notified no later than 72 hours after the University is aware of a Notifiable Privacy Breach.

An Individual Concerned may also make a complaint to the Office of the Privacy Commissioner at [www.privacy.org.nz](http://www.privacy.org.nz).

#### 5. RESPONSIBILITIES

##### **A Privacy Officer will:**

- Be familiar with the privacy principles in the Privacy Act 2020;
- Work to make sure the University complies with the Privacy Act 2020;
- Deal with any complaints about possible Privacy Breaches;
- Deal with requests for access to Personal Information, or correction of Personal Information; and
- Act as the University's liaison with the Office of the Privacy Commissioner.

##### **They may also:**

- Train other staff to deal with privacy matters;
- Advise the University on compliance with privacy requirements;
- Advise the University on the potential privacy impacts of changes to the University's business practices;
- Advise the University if improving privacy practices might improve the business; and
- Be familiar with any other legislation governing what the University can and cannot do with Personal Information.

#### 6. POLICY BASE

[Privacy Policy](#)

**7. ASSOCIATED DOCUMENTS**

[Privacy Breach Notification Form](#)

Personal Information Procedures

**8. FORMS RECORD KEEPING**

All records of this procedure will be retained by General Counsel.

**9. DOCUMENT MANAGEMENT AND CONTROL**

Procedures Owner:	General Counsel
Last review:	November 2024
Next review:	November 2029
Approved by:	Vice Chancellor
Effective date:	November 2024