Data Breach Response Plan

Section	Council
Council Approval Date	
Approval Date	TBA
New Review Date	TBA
Policy Owner (PO)	Otago Polytechnic Council
Pastoral Care Code (PCC)	Outcome 1.
Version History	Version 1

Contents

Audience and Scope

1.1. Otago Polytechnic policies and procedures are guided by and give effect to Te Tiriti ō Waitangi and honour our obligations as a Tiriti partner.

1.2. This plan is relevant to Otago Polytechnic employees, including contracted staff, and consultants providing services for Otago Polytechnic, and those on fixed term contracts (collectively referred to as kaimahi in this document).

1.3. Specific roles are instrumental to this plan:

- Chief Executive

- Deputy Executive Director: Operations
- Deputy Executive Director: People and Safety
- Deputy Executive Director: Academic Delivery
- Deputy Executive Director: Industry Training and Innovation
- Director: Digital
- Chief Financial Officer or equivalent
- Head of Finance or equivalent
- Privacy Officer
- ISS department.

Introduction

2.1. A data breach is a security incident in which sensitive, protected or confidential data is copied, transmitted, viewed, stolen or used by an individual or entity unauthorised to do so. In the context of the Privacy legislation, it extends to an action that prevents Otago Polytechnic from being able to access personal information on a temporary or permanent basis.

2.2. Otago Polytechnic is committed to managing personal information in accordance with the Privacy Act 2020 and the Otago Polytechnic Privacy Policy.

2.3. Otago Polytechnic needs to be prepared to act quickly in the event of a data breach or suspected data breach and determine whether it is likely to result in serious harm and, in conjunction with the Privacy Officer, whether the breach is a notifiable privacy breach. A notifiable privacy breach is a privacy breach that it is reasonable to believe has caused or is likely to cause serious harm to an affected individual or individuals.

2.4. ISS is to be proactive in managing this risk by completing annual risk analysis and regular security audits of Information systems and supporting infrastructure with timely remedial action.

2.5. The Data Breach Response Plan has been informed by the Privacy Act 2020 and the current guidelines available on the Privacy Commissioner webpage (with these reviewed for updates on an ongoing basis).

2.6. This document should be read in conjunction with the Privacy Policy and Procedures of Otago Polytechnic.

Purpose

3.1. The purpose of this Data Breach Response Plan is to set out the processes to be followed by Otago Polytechnic kaimahi in the event Otago Polytechnic experiences a data breach or suspects that a data breach has occurred.

Compliance

Privacy Act 2020

Data Breach Alert

4.1. Where a suspected data breach has been identified, the following information must be collated immediately and provided to the Deputy Executive Director: Operations and the Privacy Officer:

a) When the breach occurred (time and date)
b) Description of the breach
c) How many people likely to have been affected
d) Cause of the breach (if known) otherwise how it was discovered
e) Which system(s) if any are affected
f) What area of the organisation is affected
g) Whether any corrective action has already been taken to remedy or ameliorate the breach (or suspected breach) and if so, details of the action and any advice received today.

4.2. Once notified of the information above, the Deputy Executive Director: Operations and Privacy Officer will engage with the Information Systems and Support (ISS) team and determine the type of data breach that has occurred and:

a) Whether financial information is involved
b) Whether personal information is involved
c) Whether the information is otherwise of a sensitive nature
d) Whether there has been unauthorised access to the information, or unauthorised disclosure of the information or a loss of information.
e) Where the breach involves financial information or is in any way commercially sensitive, the Head of Finance or equivalent will be immediately informed.

4.3. In all instances, the Chief Executive will be informed where the breach is of a serious nature and could in any way impact upon the reputation of Otago Polytechnic (refer 3.5 below).

Criteria for determining severity

4.4. In determining whether a breach could potentially be of a serious nature, the Deputy Executive Director: Operations and Privacy Officer/ (in conjunction with the Head of Finance or equivalent and / or the Deputy Executive Director: People and Culture, as appropriate) will have regard to:

a) The type and extent of information involved
b) Whether multiple individuals have been affected
c) Whether the information is protected by any security measures (password protection or encryption)
d) The person or kinds of persons who now have access

e) Whether there is (or could there be) a real risk of serious harm to the affected individual(s) including any specific damage (financial loss through identity theft, loss of employment, physical injury or other forms of specific harm); loss of benefits (any adverse effect on the rights, benefits, privileges, obligations or interests of the individual(s)) or emotional harm.
f) Whether there could be media or stakeholder attention as a result of the breach or suspected breach.

4.5. If the breach is or could potentially be serious, the entire Data Breach Response Team will be convened and the Chief Executive informed of this decision.

Data Breach Response Team

4.6. The Data Breach Response Team will consist of the following:

- Deputy Executive Director: Operations
- Deputy Executive Director: Academic Delivery - where the breach relates to ākonga who is enrolled within their responsible College Otago Polytechnic
- Deputy Executive Director: Industry Training and Innovation - here the breach relates to ākonga who is enrolled within their responsible College
- Director: Academic Excellence - quality and delivery where the breach relates to an academic matter
- Deputy Executive Director: People and Culture - where the breach relates to any employer related information or breach impacts on kaimahi)
- Privacy Officer, Chief Financial Officer or equivalent and Head of Finance – where the breach relates to financial information
- Director Marketing, Communications and Engagement
- Director: Digital

Procedure

5.1. **Step one: Immediately contain the breach**

Immediately contain the breach (if this has not already occurred).

a) Corrective action may include retrieval or recovery of personal information, ceasing unauthorised access, shutting down or isolating the affected system. In the case of kaimahi, their machine will be quarantined and their network account locked until such time the response team are satisfied there is no further risk.
b) Deputy Executive Director: Operations will appoint a suitable person to lead the initial investigation.
c) Data breach response team to identify individuals from other areas - this might include kaimahi from within Otago Polytechnic or those from outside who have the expertise to deal with the situation.

d) Data breach response team to decide who needs to know within the organisation and build a list of those who need to be informed, such as internal auditors, risk managers, Council, and legal advisers.
e) Be careful not to destroy evidence that may be needed by Otago Polytechnic or the New Zealand Police in finding the cause of the problem, or which might allow the issue to be fixed.

5.2. **Step two: Evaluate the risks**

Responsibility: Data Breach Response Team

a) Evaluate the risks associated with the breach, including collecting and documenting all available evidence of the breach.
b) Further evaluate the risks using the Privacy breach self-assessment guidance provided by the Office of the Privacy Commissioner
c) Call upon the expertise of, or consult with, relevant kaimahi relating to the particular circumstances
d) Engage an independent cyber security or forensic expert, as appropriate
e) Assess whether serious harm is likely
f) Consider developing a communication or media strategy including the timing, content and method of any announcements to ākonga enrolled at Otago Polytechnic, kaimahi or the media.

5.3. **Step three: Consideration as to whether people affected should be notified**

Responsibility: The Data Breach Response Team

a) What is the risk of harm to people whose information has been breached?
b) Is it reasonable to believe that the breach caused (or could cause) serious harm to the affected individuals? This will involve a collective review of the matters considered in paragraph 4.4(e) above.
c) In assessing serious harm, regard should be had to:
    - the particular situation and, for example, whether there is a risk of identity theft, could it result in physical harm or damage to the individual's reputation or relationships, does it relate to health information?
    - who has obtained the information as a consequence of the breach?
    - how many individuals are affected?
    - how wide spread is the breach and how long has it been occurring?
    - if the breach relates to an entity or person Otago Polytechnic has a commercial relationship with, then even if this is not personal information, what are the legal and contractual obligations?

5.4**. Step four: Notification process**

Responsibility: Data Breach Response Team.

a) The above information will be communicated to the Privacy Officer as soon as reasonably practicable.
b) The Privacy Officer will then apply the Privacy Policy and Procedures for notifying a Notifiable Privacy Breach to the Privacy Commissioner and

advise on the circumstances in which notification should be made to the affected individual(s) or public notification given (having regard to sections 114 to 116 of the Privacy Act 2020). Where a decision is made to provide public notification of a breach, this should be escalated to the Council Chairperson and the Chief Executive before the notification is submitted to the Privacy Commissioner.

5.5. **Step five: Notify third parties, if necessary**

Responsibility: The Data Breach Response Team should consider whether the following groups or organisations should also be informed, bearing in mind any obligations of confidentiality:

a) Third party contractors or other parties who may be affected
b) Internal business units not previously advised of the privacy breach, for example, members of the Kaunihera Whakahaere
c) Otago Polytechnic Council
d) Union or other kaimahi representatives
e) New Zealand Police
f) Insurers
g) Professional or other regulatory bodies
h) Credit card companies, financial institution/s or credit reporting agencies.

5.6. **Step six: Prevent a repeat**

Responsibility: The Data Breach Response Team once the breach matters have been dealt with should turn attention to the following:

a) Identify lessons learnt and remedial action that can be taken to reduce the likelihood of recurrence – this may involve a review of policies, processes, refresher training
b) Prepare a report for submission to Te Kāhui Manukura, Otago Polytechnic Council and notifiable parties
c) Consider the option of an audit to ensure necessary outcomes are affected and effective
d) The amount of effort should reflect the significance of the breach, and whether it happened as a result of a systemic problem or an isolated event. It could include:
    - A security audit of both physical and technical security
    - A review of policies and procedures
    - A review of kaimahi training practices
    - A review of any service delivery partners caught up in the breach.

5.7. **Step seven: Consider whether a disciplinary process is required**

a) If the breach was caused by kaimahi, consult with Deputy Executive Director: People and Safety to assess whether a disciplinary process is warranted.
b) If a contractor caused the breach, consult with the relevant relationship, Formal Leader and Deputy Executive Director: Operations as to whether the relevant contract should be terminated.

Roles and Responsibilities

6. The following roles and responsibilities apply to the:

Data Breach Response Team:

- Assess and determine the potential impact of data breach
- Ascertain whether the breach is a notifiable privacy breach
- Undertake steps outlined in this plan including containment of data breach and prevent reoccurrence.

Director: Digital and ISS Kaimahi:

- Ensure all relevant information is provided.

Deputy Executive Director: Operations:

- Appoint data breach Investigation lead
- Identify relevant personnel
- Convene the response team if assessed as serious in nature.

Deputy Executive Director People and Safety:

- Determine if kaimahi disciplinary processes are required and oversee any action required with the appropriate leaders.
- Work with the Data Breach response team on implementing and people related initiatives required to prevent recurrence.

Director of Marketing, Communications and Engagement:

- Work with Privacy Officer and Data Breach Response Team in on appropriate means of notifying a serious breach to the affected individuals or whether notification to other parties is deemed appropriate
- Develop and disseminate internal and external communications, in coordination with the Data Breach Response Team, where appropriate.

Privacy Officer:

- Comply with the Privacy Policy and Procedures when the breach is identified as a notifiable privacy breach
- Ensure timely notification to the Privacy Commissioner, where appropriate
- Liaise with Marketing, Communications and Engagement in relation to the manner in which notification to the affected individuals is to take place.

References

- Privacy Policy and Procedure
- Privacy Act 2020 Privacy Act 2020 No 31 (as at 01 April 2021), Public Act Contents – New Zealand Legislation

- Office of the Privacy Commissioner Responding to privacy breaches https://www.privacy.org.nz/privacy-for-agencies/privacy-breaches/responding-to-privacy- breaches

Approved

John Gallaher (Chairperson)
Otago Polytechnic Council
Date