Privacy Management Rule - Annexure 1 - Data Breach Policy

Section 1 - Overview and Scope

(1) This Policy supports the UNE Governance Framework's Information Governance functions and assist the University of New England in preparing for and responding to personal information data breaches in line with our obligations under the Privacy and Personal Information Protection Act 1998 (PPIP Act) and Part IIIC of the Privacy Act 1988.

(2) The objective of this Policy is to describe UNE's approach to reducing the risks associated with data breaches. The approach includes the immediate containment and mitigation of harm, evidentiary and reporting requirements, and future strategies to improve the management of personal information reducing the likelihood of breach reoccurrence.

(3) Within this Policy:

a. Part A defines data breaches and UNE's responsibilities;
b. Part B deals with a suspected data breach; and
c. Part C deals with identifying and responding to a data breach.

(4) The Data Breach Policy applies to:

a. All UNE Representatives, University's decision-making and advisory bodies.
b. All organisations or entities that manage personal information on UNE's behalf.

Part A - What is a Data Breach

(5) A data breach occurs when there is a failure that has caused or has the potential to cause, unauthorised access to, disclosure of, or loss of, UNE physical or digital data containing personal information.

(6) Data breaches are serious and can potentially harm individuals and organisations.

a. For individuals this includes risk to individuals' safety, mental and physical harm, financial loss to an individual, damage to personal reputation or position.
b. For organisations this can include loss of public trust, commercial risk through disclosure of commercially sensitive information to third parties, threat to systems, capacity to provide services, reputation, finances, interests or operation and financial or legal penalty.

> Example Data Breach: A criminal group access the university network using login credentials stolen in a phishing email. They download student data from the past 20 years, including names, addresses, dates of birth, phone numbers, personal email addresses, emergency contact details, tax file numbers, bank account details, passport details and student academic records. The students suffer from the financial and emotional impact of managing the ongoing threat of identity theft.

> Example Data Breach: A lecturer, using their class contact list, accidently emails all the students in a unit

with the Special Assessment application of one of the students, Stevie. This contains health information and contact details. Some of the student make comment on social media about Stevie and one emails it to Stevie's family. Because of Stevie's family cultural beliefs, they fear for both their physical harm and mental health. The information becoming public means there is a risk to Stevie's future employment and social wellbeing.

Example Data Breach: A researcher accidently leaves a folder of 50 consent forms for participants in a medical research project in café. She rushes back to the café; however, the file is gone. Each form contained the persons contact details, health status and signatures. Once informed many of the participants withdraw consent reducing the viability of any findings. The relationship between the researcher and their funding body is irreversibly damaged. The University's reputation is damaged because of exposing the individuals to potential identity theft and other harm.

UNE and University Representatives responsibilities

(7) Protect personal information against loss, unauthorised access or modification, disclosure or misuse.

(8) Provide access to personal information for University Representatives only where reasonably necessary for work purposes and incompliance with legal obligations.

(9) Report data breaches immediately.

(10) Respond to data breaches within the required legislative and UNE timeframes.

(11) Comply with voluntary and compulsory reporting schemes.

UNE Data Breach Response Plan

(12) UNE keeps an up-to-date Data Breach Response Plan that defines:

a. Definition of what constitutes a data breach
b. Strategy and actions for containing, assessing and managing data breaches
c. Documentation requirements
d. Reporting and notification
e. Response team roles and responsibilities

(13) The Data Breach Response Plan outlines the processes and roles and responsibilities for managing data breaches at UNE and should be read in conjunction with the Information Security Policy, Emergency Management Plan, Privacy Management Rule, and the IT Service Continuity and Disaster Recovery Plan.

Part B - Suspected data breach

(14) A suspected data breach is any event that may have involved unauthorised access to, unauthorised disclosure of, or loss of data involving personal information managed by UNE and third parties acting on UNE's behalf.

Reporting a suspected data breach

(15) All UNE Representative are responsible for reporting suspected data breaches to the UNE Privacy Officer immediately, providing accurate details in the data breach reporting form and assisting with triage an assessment.

Part C - UNE's approach to responding to a data breach

(16) Assessment of all reported suspected data breaches is completed by the UNE UNE Privacy Officer.

(17) Data breach are assessed for harm, impact and risk defined in the UNE Data Breach Response Plan.

Table 1 – Suspected data breach

1. Triage	2. Assess
Identify the suspected data breach Take necessary steps to immediately limit the impact of the data beach Notify the UNE UNE Privacy Officer within 24 hours	Gather information on the suspected data breach Evaluate the evidence and assess level of harm, impact, and risk Document assessment Decide reporting requirements

Table 2 – Responding to a data breach

1. Analyse	2. Notify	3. Remediate
Undertake steps to reduce potential harm Initiate detailed investigation engage specialist response team(s): o Security Incident Management Team (SIMT) o Data Breach Management Team (DBMT) Enact the Data Breach Response Plan	Prepare and submit voluntary and/or mandatory notifications Notify other relevant bodies Notify affected individuals if not already completed as part of mitigation steps	Identify changes to prevent future breaches Implement changes Evaluate effectiveness of implemented changes

(18) Roles and responsibilities for responding to data breaches and escalation points are defined in the Data Breach Response Plan.

Section 2 - Authority and Compliance

(19) This Data Breach Policy is made by the Vice-Chancellor and Chief Executive Officer consistent with section 29 of the University of New England Act 1993 (NSW).

(20) The Custodian of this Policy and Rule, the Director Governance and University Secretary, is authorised to make minor administrative updates to this Policy, and to publish as associated documents any tool that will assist with compliance.

(21) The Data Breach Response Plan is the responsibility of the Director Governance and University Secretary and approved by Information Technology Governance Committee (VC Approved).

(22) UNE Representatives must observe this Policy in relation to University matters.

(23) This Policy is consistent with the:

a. Privacy and Personal Information Protection Act 1998 (PPIP Act)
b. Privacy and Personal Information Protection Regulation 2019
c. Health Records and Information Privacy Act 2002
d. Health Records and Information Privacy Code of Practice 2005

(24) This Policy operates as and from the Effective Date.

(25) Previous policies relating to Data Breach Policies are replaced and have no further operation from the Effective Date of this new Policy.

(26) This Policy should be read in conjunction with the Privacy Management Rule.

Section 3 - Quality Assurance

(27) Quality Assurance regarding the effective implementation of the Data Breach Policy will be supported by:

a. Assurance by the Director Governance and University Secretary to the Vice-Chancellor and Chief Executive Officer and through them to the Council, at least annually that that the Data Breach Response Plan is effectively and that issues or areas for continuous improvement are being followed up/actioned.

Section 4 - Definitions (specific to this Policy)

(28) Data breach - is the unauthorised access to, unauthorised disclosure of, or loss or personal information.

(29) Unauthorised access – is access of personal information occurs when personal information that UNE holds is accessed by someone who is not permitted to have access.

(30) Unauthorised disclosure – is making personal information accessible or visible to others outside UNE, or in specific circumstances to unauthorised parties within UNE in a way that is not permitted by the Privacy and Personal Information Protection Act 1998 and/or Health Records and Information Privacy Act 2002. This may be done intentionally or unintentionally.

(31) Data loss – is the accidental or inadvertent loss of personal information held by UNE and is likely to result in unauthorised access or unauthorised disclosure.

Status and Details

Status	Current
Effective Date	12th August 2021
Review Date	12th August 2023
Approval Authority	Director Governance and University Secretary
Approval Date	12th August 2021
Expiry Date	To Be Advised
Unit Head	Kate McNarn Director Governance and University Secretary
Enquiries Contact	Kate McNarn Director Governance and University Secretary Records, Policy and Governance Unit

Glossary Terms and Definitions

"UNE Representative" - Means a University employee (casual, fixed term and permanent), contractor, agent, appointee, UNE Council member, adjunct, visiting academic and any other person engaged by the University to undertake some activity for or on behalf of the University. It includes corporations and other bodies falling into one or more of these categories.

"Personal Information" - Refers to information or an opinion (including information or an opinion forming part of a database and whether or not recorded in a material form) about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion. In accordance with Section 4 of the Privacy and Personal Information Protection Act 1998 (NSW) (PPIPA). It includes such things as: a. a person's name, address, information about a person's family life, information about a person's sexual preferences, financial information, photos, contact details, opinions, health conditions or illnesses, housing or tenancy information, work history, education and criminal histories; b .an individual's fingerprints, retina prints, body samples or genetic characteristics; c. payroll details, information about next of kin, emergency contacts, superannuation fund and tax file numbers; d. health information, in accordance with Section 6 of the Health Records and Information Privacy Act 2002 (NSW), incorporating information or opinions about: the physical or mental health or a disability (at any time) of an individual, or an individual's express wishes about the future provision of health services to him or her, or a health service provided, or to be provided, to an individual, or other personal information collected to provide a health service, or in providing a health service, or in connection with the donation of human tissue or body parts; or genetic information that is or could be predictive of the health of a person or their relatives or descendants; and e. some things (such as information about an individual who has been dead for more than 30 years and information about an individual that is contained in a publicly available publication) are exempt from the definition of "personal information" and these are listed in full, under Section 4(3) of the PPIPA.

"Effective Date" - means the Rule/Policy takes effect on the day on which it is published, or such later day as may be specified in the policy document.

"University Representative" - University Representative means a University employee (casual, fixed term and permanent) contractor, agent, appointee, UNE Council member, adjunct, visiting academic and any other person engaged by the University to undertake some activity for or on behalf of the University. It includes corporations and other bodies falling into one or more of these categories.