Data Breach Policy (Personal and Health Information)

Report a suspected breach here

Section 1 - Audience

(1) This Data Breach Policy (Policy) relates to all University of Newcastle ("we," "us" or "our") staff, students, contractors, conjoints, volunteers, affiliates, and any third party that manages and processes personal information for, or on behalf of the University. This Policy also applies to members of the public when they interact with us.

Section 2 - Executive Summary

(2) We want to ensure that any incident involving a breach of personal information or health information is responded to in an efficient and timely manner, and that we mitigate risk and protect the rights and interests of all individuals to whom the personal information or health information relates.

(3) Part 6A of the Privacy and Personal Information Protection Act 1998 (PPIP Act) establishes the NSW Mandatory Notification of Data Breach (MNDB) scheme.

(4) The MNDB Scheme requires every NSW public sector agency, like us, to notify the Information Privacy Commissioner and affected individuals of eligible data breaches.

(5) We are required to create a Data Breach Policy under section 59ZD of the PPIP Act (the Policy). Under the scheme, we make this Policy for managing eligible data breaches publicly accessible on our website and through our Policy Library. This enhances transparency and ensures that we remain accountable for the way we respond to data breaches. It also helps to enhance public trust and confidence in us.

(6) The Vice-Chancellor is responsible for our compliance with the MNDB scheme.

Section 3 - Purpose

(7) We are committed to the protection of the personal information and health information of our students, staff, community members, and alumni.

(8) This Policy will coordinate collaboration between stakeholders and will operate in parallel with any response by a Digital Technology Solutions (DTS) Incident Management team and the DTS Cyber Security Incident Management team if the breach is also a cyber breach as may be required; as well as the Business Continuity Management Policy and Business Continuity Management Framework.

(9) The Vice-Chancellor has sub-delegated the authority to perform certain duties in relation to data breaches to the General Counsel.

(10) This Policy establishes the roles and responsibilities of staff in relation to managing a breach, and the steps we

will follow when a breach occurs.

Section 4 - Scope

(11) This Policy applies to circumstances where personal information or health information held by us has been, or is potentially, compromised.

(12) This Policy applies to any actual or suspected data breach involving the following types of information, as defined by the Privacy Management Plan:

a. Personal information;
b. Health information;
c. Tax File Numbers (TFNs);
d. Individual Healthcare Identifier (IHI) information; and
e. Government-related Identifier (GRI) information,

defined as “Personal information”.

When does the MNDB scheme not apply?

(13) The MNDB scheme does not apply to data incidents or data breaches that do not involve personal information, or to breaches that are not likely to result in serious harm to an individual. Where the scheme does not apply, we are not required to notify individuals, but may still be required to notify to the Commissioner, and we will take action to respond to the breach. We may still provide voluntary notification to individuals where appropriate.

Section 5 - Terminology

(14) It is important to understand the terminology of the PPIP Act that applies to the MNDB scheme.

(15) An eligible data breach occurs where:

a. there is an unauthorised access to, or unauthorised disclosure of, personal information held by us or there is a loss of personal information held by us in circumstances that are likely to result in unauthorised access to, or unauthorised disclosure of, the information; and
b. a reasonable person would conclude that the access or disclosure of the information would be likely to result in serious harm to an individual to whom the information relates.

(16) Breaches can occur:

a. between agencies, for example if we inappropriately share information with another university, like an opinion about a student;
b. within the University, for example where we share personal information with a colleague who does not need to know that information to fulfill their role; and
c. external to the University, for example where cyber criminals gain access to personal information we hold.

(17) The MNDB scheme applies to breaches of ‘personal information’ as defined in section 4 of the PPIP Act.

Section 6 - The impact of a data breach

(18) The size, and nature of a breach, can have a significant impact on individuals affected by it. A breach can give rise to a range of actual or potential harm to individuals. These consequences can include financial fraud, identity theft, damage to reputation and even physical violence. For this reason, we will remain vigilant, when safeguarding the information, you provide to us.

(19) Data breaches can also have serious consequences for us as well. A breach may create risk through the disclosure of confidential information, or otherwise impact our reputation, finances, interests, or operations. Ultimately, data breaches can lead to a loss of trust and confidence in us.

(20) Responding quickly when a breach occurs is critical, and it can substantially reduce the effect on those people impacted, reduce the costs to us of dealing with a breach, and reduce the potential reputational damage which may result.

(21) We have a documented and operationalised Privacy Breach Response Plan for quickly and effectively responding to and managing data breaches.

What if we are also required to notify the Commonwealth regulator?

(22) In some cases, we will have notification obligations under both the MNDB scheme and under the Commonwealth Notifiable Data Breach (NDB) scheme and in some circumstances, notification obligations in other countries.

(23) For example, a data breach that involves TFNs and is likely to result in serious harm would be reportable to both the Office of the Australian Information Commissioner (OAIC) under the Commonwealth NDB scheme, and the NSW Privacy Commissioner under the MNDB scheme.

(24) The MNDB scheme has been designed to be consistent with and adopt, as far as possible, key features of the Commonwealth NDB scheme. For example, the MNDB scheme adopts the same thresholds for assessing and notifying data breaches so that we can meet both requirements with a single process.

What this policy includes

(25) This Policy outlines our overall strategy for managing data breaches from start to finish. Having a clear and well-defined Policy enables us to:

a. prepare for, evaluate, respond to, and report on data breaches at the appropriate level and in a timely fashion;
b. mitigate potential harm to affected individuals and us; and
c. meet compliance obligations under the PPIP Act and any other regulatory obligations.

How have we prepared for a data breach?

(26) This Policy provides a high-level outline of steps that the University has taken to prepare for a data breach, and how these fit within our broader systems, policies, and procedures (such as cyber response, broader incident and emergency management processes, communications strategies, and business continuity processes). The Policy covers key controls, systems, and processes that the University has in place to promptly identify actual or suspected data breaches, and to ensure that they are effectively managed.

(27) We have a dedicated Data Breach Response Team selected from staff across the University that can be convened rapidly to manage data breaches. The Team involves members that bring significant skills to enable rapid response to data breaches of many different kinds. Not all members will be needed for all incidents. The Team includes, but is not limited to, specialists in:

a. Cyber Security;
b. Digital Technology Solutions (DTS);
c. Legal;
d. Privacy;
e. Marketing;
f. Internal communications;
g. External communications;
h. AskUON;
i. Human Resources; and
j. Finance.

(28) The Team has rehearsed privacy breach scenarios and learned from prior breach management to improve its performance.

Section 7 - Training and Awareness

(29) Most data breaches, both in Australia and internationally, involve a human element (e.g., either through direct human error or cyber-attacks that rely on a human compromise). Building a well-trained and aware workforce is a strong front-line defence against breaches and other privacy risks.

(30) This Policy encourages all staff to undertake and attend staff training and awareness, (e.g. by enhancing staff awareness of privacy and cyber security principles and current threat trends), in addition to training and awareness around identifying, responding to, and managing data breaches. Privacy training is provided to all staff through Discover and refresher or tailored training can be requested at any time by emailing privacy@newcastle.edu.au.

Section 8 - Processes for identifying and reporting breaches

(31) The quicker we can detect a data breach, the better the chance that it may be contained, and potential harms mitigated through prompt action. Actual or suspected data breaches must be reported by staff, students, contractors within the University, but also by any member of the public outside the University. You can report here.

(32) This Policy outlines the kinds of processes we have in place for identifying data breaches, for example we employ technology solutions like detection software, firewalls, password and permission levels, and digital and physical access methods. Other measures for identifying and prevent data breaches include:

a. internal reporting as required by this Policy;
b. technical controls (such as Data Loss Prevention tools, access controls, and system monitoring);
c. information Security certification, audit, and testing;
d. internal audit strategies, in accordance with the Internal Audit Charter;
e. staff training and awareness at Discover or by emailing privacy@newcastle.edu.au.

Appropriate provisions in contracts / other collaborations

(33) On occasions, we are required to outsource functions to external service providers (for example, for digital solutions). If this is the case, these relationships are usually covered by legally binding contracts, memorandums of understanding, or non-disclosure agreements. To ensure we meet our obligations under the PPIP Act, these agreements often include provisions in relation to the management and notification of data breaches and can extend

to third-party assurances made in relation to assisting us manage third-party data breaches (including in relation to notification and remediation).

(34) We adopt a privacy by design model and build privacy mitigation into our arrangements with third party service providers whenever we share personal information. Staff must complete a Privacy Impact Assessment (PIA) if high-risk information will be being transferred outside our control. Our Privacy and Right to Information Manager can provide guidance and assistance in the application of PIAs for new or existing projects, systems, and business operations to mitigate privacy risks and ensure best practice. Staff can request privacy advice by visiting the Legal and Compliance portal.

Section 9 - Schedule for testing and update this Policy

(35) As both the external threat environment, and University's internal makeup and functions are continuously developing and changing, our Policy will be annually reviewed to ensure it remains fit for purpose.

(36) Regular testing of the data breach response process is the best way to ensure that all relevant staff understand their roles and responsibilities, and to check that the details of the response process (contact information, reporting lines, approval processes, etc.) are up to date. Testing this Policy could involve the development of a hypothetical or test incident and a review of the way our personnel manage the event.

Section 10 - Alignment with other policies

(37) This Policy is aligned with existing policies, procedures, and capabilities. This Policy should be read in conjunction with:

a. Information Security Policy
b. Privacy Management Plan
c. Cyber Security Incident Management Procedure
d. Business Continuity Management Policy

(38) If a data breach includes a large volume of personal information the breach may be referred to the Critical Incident Team for the deployment of existing incident or crisis management processes. The General Counsel will make this referral, if deemed necessary.

Section 11 - What is a data breach is and how to identify one?

(39) Consistent with the definition of ‘eligible data breach’ in the PPIP Act, this Policy notes that a data breach may involve unauthorised access, unauthorised disclosure, or loss of personal information. Each data breach will be assessed on a case-by-case basis and no response can be applied in all cases.

(40) A data breach may be deliberate or accidental and may occur by a range of different means or channels, including but not limited to, loss or theft of physical devices, misconfiguration, or over-provisioning of access to sensitive systems, inadvertent disclosure, social engineering, or hacking.

(41) Data breaches can happen in all manner of ways, for example, an email may be sent to the wrong email address, a paper file or an unprotected flash drive could be left in a taxi, a phishing email may contain a link that tricks the

recipient into compromising their access credentials, or we may be the subject of a malicious cyber criminals.

Plan for managing data breaches

(42) This Policy outlines the steps we will take to respond to a reported, or suspected or confirmed data breach.

Response Plan to triage, contain, assess, notify and prevent

(43) To help ensure responses to data incidents are easily and quickly put into action, we need to take the following steps:

a. Initial assessment and triage of breach reports
    i. Does the incident involve the unauthorised loss or access of personal information?
b. Containing a breach or suspected breach to minimise the possible harm
    i. Staff must take all reasonable steps to contain any loss or unauthorised access to personal information and report the loss or access immediately. If an email has been misaddressed, immediately try to recall the message, or email the recipient's address and ask them to delete the misdirected email and confirm by return that they have done so. Another example of taking reasonable steps could include, If you left a file or your laptop in a taxi, or at the airport, call and advise them immediately, and ask them if it has been handed in, or could they try to recover it.
    ii. Provide as much information as possible to the Privacy team to help them investigate.
c. Legal and Compliance, with the assistance of other Data Breach Response Team stakeholders, must assess or evaluate the information involved in the breach and the risks associated to determine the next steps and to implement any additional actions identified to mitigate risks. This could involve consideration of:
    i. the kind or kinds of information involved;
    ii. the sensitivity of the information;
    iii. whether the information is protected by one or more security measures;
    iv. if the information is protected by one or more security measures – the likelihood that any of those security measures could be overcome;
    v. the persons, or the kinds of persons, who have obtained, or who could obtain, the information;
    vi. if a security technology or methodology:
        - was used in relation of the information; and
        - was designed to make the information unintelligible or meaningless to persons who are not authorised to obtain the information;
    vii. the likelihood that the persons, or the kinds of persons, who:
        - have obtained, or who could obtain, the information; and
        - have, or are likely to have, the intention of causing harm to any of the individuals to whom the information relates; and
        - have obtained, or could obtain, information or knowledge required to circumvent the security technology or methodology.
    viii. the nature of the harm;
    ix. any other relevant matters;
    x. the volume of information lost or accessed;
d. Notifying individuals / organisations affected by the breach, and the Privacy Commissioner and any other relevant data protection authorities; and
e. Post incident review and preventative efforts, based on the type and seriousness of the breach.

Section 12 - Strategies for managing supplier and / or partner agency breaches

(44) We have in place contractual provisions that outline strategies for managing data breaches that may occur at business-critical suppliers or partners and affect University data. This includes documenting key contacts and clarifying roles in relation to assessment, remediation, notification to affected individuals and reporting to the IPC.

Section 13 - Other obligations including external engagement or reporting

(45) We may be required by contract or by other laws or administrative arrangements to take specific steps in response to a data breach. These may include taking specific containment or remediation steps, or engaging with or notifying external stakeholders (in addition to the Privacy Commissioner), where a data breach occurs.

(46) Depending on the circumstances of the data breach and the categories of data involved, we may need to notify or engage with:

a. NSW Police Force;
b. Information Privacy Commission New South Wales;
c. Department of Customer Service'
d. The Office of the Australian Information Commissioner;
e. Australian Federal Police;
f. The Australian Taxation Office;
g. The Australian Cyber Security Centre;
h. Any third-party organisations or agencies whose data may be affected;
i. Financial service providers;
j. Professional associations, regulatory bodies, or insurers;
k. International data protection authorities.

(47) If, for example, we became aware of a criminal cyber-attack, that was an eligible data breach, we would report it to the NSW Police Force, as well the Information Privacy Commission New South Wales.

Section 14 - Clear communication strategy

(48) Our response plan includes a clear communication strategy that enables University staff to quickly communicate with affected individuals and other stakeholders.

(49) The response plan outlines:

a. responsibilities for implementing the communication strategy where there is a serious risk of harm to individuals that cannot be mitigated;
b. how to assess the risk of serious harm and determine when affected individuals or organisations must be notified;
c. key contacts for communications;
d. how affected individuals will be contacted and managed;
e. responsibilities for consulting with external stakeholders.

Section 15 - Capability, expertise, and resourcing

(50) To be effective, the response plan and strategies outlined above must be quickly and effectively implemented and actioned. However, this depends on having staff with the relevant skillsets available to deal with the breach. Where relevant, our strategy will ensure:

a. we have access to requisite expertise and resourcing to respond effectively. This may involve engaging (in advance) an outsourced cyber incident response service provider;
b. where our staff are called upon to assess a data breach or make an escalation decision, that those staff are trained and capable of adequately assessing the breach and its impact.

Section 16 - Roles and responsibilities

(51) All staff must comply with relevant policies and legislation and this Policy, and:

a. proactively monitor processes to identify potential data breaches;
b. contain and report data beaches; and
c. be aware of any issues, activities or behaviours that may indicate a potential breach has occurred.

(52) The Vice-Chancellor has the authority to issue notifications to the Privacy Commissioner, impacted individuals, and other data protection authorities.

(53) The Data Breach Response Team is responsible for:

a. containing any data breach;
b. providing information to assist Legal and Compliance to assess the risk of serious harm associated with the data breach;
c. mitigate any risk of serious harm;
d. where necessary, notify the Privacy Commissioner and impacted individuals of an eligible data breach; and
e. review an eligible data breach, develop, and action future preventative measures.

(54) The Privacy and Right to Information Manager is responsible for:

a. establishing the seriousness of a data breach and convening the data breach response team;
b. provide privacy expertise and support to the data breach response team;
c. liaising with regulators;
d. record keeping of forensic evidence, and how we conducted our investigation;
e. maintaining and publishing (on our website) a public notification register for any notifications given; and
f. establishing and maintaining an internal register for eligible data breaches.

(55) The Director, Communications & Engagement is responsible for assisting to communicate with affected individuals and dealing with the media and external stakeholders.

(56) The Chief Digital & Information Officer is responsible for assisting with establishing the cause, impact and containing any data breach that involves DTS systems, and assisting to review security and monitoring controls related to the breach (for example, access, authentication, encryption, audit logs).

(57) System Owners / Information Owners are responsible for ensuring the systems that they are responsible for are regularly risk assessed, actively monitored for potential data breaches, and have system security patches installed to

reduce the likelihood of system vulnerabilities.

(58) Service Providers are responsible for ensuring DTS systems and processes meet the relevant privacy requirements and that systems are regularly monitored for system failures and/or potential system vulnerabilities. Provision for future audits should be included in contractual terms where necessary when the transfer of personal information is proposed.

Section 17 - Record keeping

(59) All staff must maintain appropriate records in accordance with the Records Governance Policy to provide evidence of how suspected breaches occurred, are managed, including those not escalated to the response team or notified to the Privacy Commissioner. Tracking data incidents and breaches allows the University to monitor, analyse, and review the type and severity of suspected breaches along with the effectiveness of the response methods.

(60) Preserving evidence for the management of data breaches can assist authorities investigate criminal activity. This may also help us to identify any weaknesses in security or processes that are prone to error. Monitoring of, and evidence from a number of small 'near misses' may identify a bigger systemic issue, which requires correcting.

Section 18 - Post-breach review and evaluation

(61) Understanding what went wrong, how issues were addressed and whether changes were needed to processes and procedures following a breach will mitigate future risks and are key to ensuring we continue to proactively manage data breaches in line with regulator and community expectations.

(62) We will include in our post-breach review:

a. a strategy to identify and remediate any processes or weaknesses in data handling that may have contributed to the breach;
b. a post response assessment of how we responded to the breach and the effectiveness of the response;
c. preventative steps required for improvement of our processes and prevent repetition.

Status and Details

Status	Current
Effective Date	29th November 2023
Review Date	29th November 2026
Approval Authority	Vice-Chancellor
Approval Date	23rd October 2023
Expiry Date	Not Applicable
Responsible Executive	David Toll Chief Operating Officer
Enquiries Contact	Daniel Bell General Counsel Legal and Compliance

Glossary Terms and Definitions

"University" - The University of Newcastle, a body corporate established under sections 4 and 5 of the University of Newcastle Act 1989.

"Risk" - Effect of uncertainty on objectives. Note: An effect is a deviation from the expected, whether it is positive and/or negative.

"Personal information" - Has the same meaning as in the Privacy and Personal Information Protection Act 1998 (NSW).

"Student" - A person formally enrolled in a course or active in a program offered by the University or affiliated entity.

"Health information" - As defined in the Health Records and Information Privacy Act 2002, or any replacing legislation.

"Information Owner" - A senior business, college or unit manager whom the University has authorised to collect, create, retain and maintain information within their assigned area of control.

"Staff" - Means a person who was at the relevant time employed by the University and includes professional and academic staff of the University, by contract or ongoing, as well as conjoint staff but does not include visitors to the University.

"System Owner" - An authorised individual who has been allocated responsibility by the University and is held accountable for an ICT resource.

"Affiliate" - A person or organisation legally obligated to, or informally associated with the University. Categories of affiliates are outlined on the University website.