GRIFFITH UNIVERSITY

Policy

Data Breach

1.0 Purpose

This policy governs how the University manages data breaches, ensuring compliance with the Mandatory Notification of Data Breach (MNDB) Scheme of the *Information Privacy Act 2009* (Qld) (IP Act) and the University's privacy obligations. It aims to minimize harm to affected individuals, build public trust, and fulfill compliance obligations.

2.0 Scope

This policy applies to all employees, contractors, consultants, service providers, and other parties who handle personal information on behalf of Griffith University (collectively "staff"). It covers all data breaches, whether actual or suspected, regardless of format. This policy provides staff with guidance on handling such incidents and provides the public with transparency regarding Griffith's practices. An internal Data Breach Response Plan ("Response Plan") provides staff with more detailed guidance on fulfilling their obligations under this policy.

3.0 Data Breach Response

3.1 Preparation

The University employs a number of processes and controls for identifying, preventing and managing Data Breaches. These include but are not limited to:

- technical controls to assist in preventing, detecting, and managing breaches
- audits and reviews
- internal governance policies and procedures, such as the Response Plan, and Crisis and Incident Response Plan, and
- staff training and awareness communications and activities.

3.2 Immediate Reporting

Upon detection or suspicion of a data breach, staff must immediately report the incident by emailing privacyalert@griffith.edu.au. More detailed guidance for the immediate response to a suspected breach is available in the Privacy/Data Breach Checklist.

Student or members of the public who know or suspect there has been a data breach should contact privacyofficer@griffith.edu.au; those communications will be routed to the privacy breach alert or privacy complaint process as appropriate.

3.3 Rapid Assessment

When alerted through the alert inbox or other notification, an Incident Response Team (IRT) will conduct a rapid assessment to determine:

- whether a data breach has occurred
- the scope and nature of the breach
- the type of personal information, if any, involved
- the potential for serious harm.

3.4 Eligibility Assessment

3.4.1 Eligible Data Breach Determination.

The IRT will determine if the data breach is an Eligible Data Breach (EDB). It will consider multiple factors, including:

- the sensitivity of the personal information
- the likelihood of malicious use
- the nature of the information environment the information may have been exposed in
- the potential consequences for affected individuals.

3.4.2 Unable to Determine EDB status

Where the IRT is unable to determine whether a breach is an EDB, it will, in accordance with regulatory requirements, provide periodic updates to the regulator regarding the steps Griffith is taking to assess and contain the breach and to determine whether it is an EDB.

3.5 Containment and Remediation

3.5.1 The IRT will implement immediate measures to contain the breach, including:

- securing affected systems and data
- changing access credentials
- isolating compromised systems
- suspending the activity that led to the breach.

3.5.2 Develop and implement a remediation plan, including:

- data recovery
- system hardening, and
- enhanced security controls.

3.6 Breach Notifications

3.6.1 Notification to Individuals Affected by the Breach

The IRT will notify affected individuals as soon as practicable after forming a reasonable belief that the breach is an EDB and that notification is appropriate under the *Information Privacy Act 2009* (QLD). Notifications will provide clear and concise information about:

- a description of the breach and how it occurred

- the type of personal information involved
- potential risks arising from the breach and recommendations about steps the individuals can take to protect themselves
- steps the University has taken to secure the data and mitigate harm
- contact information for assistance regarding the breach.

3.6.2 How Individuals will be Notified

- **Direct Notification.** The University will directly notify (by telephone, letter, email, or in person) everyone whose information was included in an EDB, or, if that is not reasonable, directly notify those who are likely to suffer harm; or
- **Notification by Publication.** When direct notification is not reasonably practicable, Griffith will publish the notice on an accessible Griffith website for at least 12 months, in accordance with the requirements of the IP Act.

3.6.3 Notification to the Office of the Information Commissioner (OIC)

If the data breach is an Eligible Data Breach, the IRT will notify the OIC as soon as practicable, adhering to the notification requirements outlined in the *Information Privacy Act 2009* (QLD).

3.6.4 Other Regulator Notification

The IRT will provide notification to other authorities in accordance with applicable legal requirements. Notifications could include agencies such as the Queensland Police Services, Crime and Corruption Commission, Australian Federal Police, Australian Information Commissioner, Australian Taxation Office, Australian Cyber Security Centre, and Tertiary Education Quality and Standards Agency. It may also include notification of regulators in overseas jurisdictions depending on the breach.

3.6.5 Other Parties to Notify

Depending on the circumstances of the breach and the information involved, other notifications may be appropriate (e.g., Griffith may need to notify its financial institutions, professional or other regulatory bodies, insurance provider(s), other partners, or service providers).

3.7 Documentation

The IRT will maintain thorough records of all data breaches, including investigation findings, assessment of eligibility, containment and remediation actions, and notifications to regulators and individuals.

3.7.1 IP Act Obligations

Griffith will keep an internal breach register in accordance with IP Act requirements.

3.7.2 Other Obligations

When breached information is subject to other legal frameworks, Griffith will fulfill any additional recordkeeping obligations imposed by other state, federal, or overseas laws or regulations.

3.8 Post-Incident Review

The IRT will engage in post-incident review to identify root causes of Eligible Data Breaches, areas for improvement in security and operations, and effectiveness of the response. The review may result in updating or changing the Response Plan, trainings, and other University policies, procedures, and protocols. For breaches that are not eligible data breaches, the IRT will provide guidance on appropriate control measures or alternative solutions to the relevant staff.

3.9 Training & Awareness

The University will provide regular training to all personnel on information privacy obligations, data breach prevention and detection, and reporting procedures. Griffith will also conduct awareness campaigns to promote a culture of privacy.

4.0 Roles, responsibilities and delegations

ROLE	RESPONSIBILTY
All Staff	Immediately report any suspected or actual data breach to the designated Incident Response Team (IRT). Cooperate fully with investigations and remediation efforts. Participate in mandatory trainings.
Incident Response Team (IRT) (Includes representatives from Cybersecurity, General Counsel, the Information Owner/Custodian, Subject Matter Expert(s), and additional members as appropriate to the incident, up to and including executive leadership.)	Conduct prompt and thorough investigations. Assess whether a data breach has occurred and if it is an Eligible Data Breach (EDB). Implement containment, remediation, and recovery measures. Prepare and submit mandatory data breach notifications to the OIC. Notify affected individuals. Maintain comprehensive records of all breaches and responses. Any responsibilities allocated in the Data Breach Response Plan.
Privacy Officer	Approve notifications for Eligible Data Breaches (EDB). Any responsibilities allocated in the Data Breach Response Plan.
Senior Management	Provide resources and support for the IRT as needed. Any responsibilities allocated in the Data Breach Response Plan.
General Counsel	Maintain and update this policy. Provide resources and support for the IRT as needed.

	Approve notifications and maintain the Register of EDBs. Report suspected and known EDBs to the Privacy Officer, if not already reported. Any responsibilities allocated in the Data Breach Response Plan.
Director of Cybersecurity	Provide resources and support for the IRT. Report suspected and known EDBs to the Privacy Officer, if not already reported. Implement the Cybersecurity Management Plan and related procedures if the Data Breach is also a cybersecurity incident. Any responsibilities allocated in the Data Breach Response Plan.

5.0 Definitions

Data Breach: may occur as the result of deliberate or accidental acts or omissions of Griffith or of a third party. Refers to either of the following in relation to personal or non-personal information:

- Unauthorised access to, or unauthorised disclosure of, the information
- The loss of the information in circumstances where unauthorised access to, or unauthorised disclosure of the information is likely to occur.

Eligible Data Breach: A Data Breach involving personal information that triggers notification and other compliance requirements under the IP Act. To be an EDB, both of the following must apply:

- There is unauthorised access to or disclosure of personal information held by Griffith, or there is a loss of personal information held by Griffith in circumstances where unauthorised access to, or unauthorised disclosure of the information is likely to occur, and
- The unauthorised access to or disclosure of the information is likely to result in serious harm to an individual.

IP Act: Information Privacy Act 2009 (Qld).

Likely: means that something is more than merely possible, it must be more probable than not to occur. This is an objective determination.

Mandatory Notification of Data Breach (MNDB) Scheme: The IP Act obligation to notify the OIC and affected individuals of an Eligible Data Breach.

Personal Information: Information or an opinion about an identified individual, or an individual who is reasonably identifiable from the information or opinion, whether the information or opinion is true or not, and whether the information or opinion is recorded in a material form or not.

OIC: Office of the Information Commissioner Queensland.

Serious Harm: Includes physical, psychological, emotional, financial, or reputational harm. It occurs where the harm has resulted or may result in a real and substantial detrimental effect to the individual; the effect must be more than mere irritation, annoyance, or inconvenience to qualify as 'serious'.

Unauthorised access occurs when someone who is not authorised to access information does so.

Unauthorised disclosure occurs when Griffith intentionally or unintentionally discloses personal information to a third party where Griffith does not have permission nor is it entitled to make the disclosure.

6.0 Information

Title	Data Breach Policy
Document number	2025/0001118
Purpose	This policy provides staff and the public with information on how the University manages Data Breaches and ensures compliance with the MNDB scheme of the IP Act. It aims to minimize harm to affected individuals, build public trust, and fulfill compliance obligations.
Audience	Public
Category	Governance
Subcategory	Risk & Integrity
UN Sustainable Development Goals (SDGs)	This document aligns with Sustainable Development Goal: 16: Peace, Justice and Strong Institutions
Approval date	27 October 2025
Effective date	27 October 2025
Review date	2027
Policy advisor	General Counsel
Approving authority	Chief Operating Officer

7.0 Related Policy Documents and Supporting Documents

Legislation	*Information Privacy Act 2009* (Qld) *Privacy Act 1988* (Cth)
Policy	Privacy Statement Privacy Management Policy

	Information Security Policy
Procedures	Data Breach Response Plan Privacy Management Procedure Crisis and Incident Response Plan Crisis Communications Management Plan
Local Protocol	Contract Management Guidelines Privacy/Data Breach Checklist Risk Management Handbook
Forms	N/A