Data Breach Procedure and Response Plan

Section 1 - Policy

(1) This Procedure is governed by the Privacy Policy.

Section 2 - Introduction

(2) ACU is committed to managing personal information in accordance with the Privacy Act 1988 (Cth) and the Privacy Policy.

(3) This document sets out the processes to be followed by ACU staff in the event that ACU experiences a data breach or suspects that a data breach has occurred. A data breach involves the loss of, unauthorised access to, or unauthorised disclosure of, personal information.

(4) The Privacy Amendment (Notifiable Data Breaches) Act 2017 (Cth) (the NDB Act) established a Notifiable Data Breaches scheme requiring organisations covered by the Privacy Act 1988 (Cth) to notify any individuals likely to be at risk of serious harm by a data breach. The Office of the Australian Information Commissioner (OAIC) must also be notified.

(5) Accordingly, ACU needs to be prepared to act quickly in the event of a data breach (or suspected breach), and determine whether it is likely to result in serious harm and whether it constitutes a Notifiable Data Breach.

(6) Adherence to this Procedure and Response Plan will ensure that ACU can contain, assess and respond to data breaches expeditiously and mitigate potential harm to the person(s) affected.

(7) This Procedure and Response Plan has been informed by:

a. the Office of the Australian Information Commissioner's "Guide to developing a data breach response plan";
b. the Office of the Australian Information Commissioner's "Data breach notification guide: a guide to handling personal information security breaches";
c. the Privacy Amendment (Notifiable Data Breaches) Act 2017 (Cth);
d. the Privacy Act 1988 (Cth) and Australian Privacy Principles (Schedule 1 of the Act).

(8) This document should be read in conjunction with the Privacy Policy.

Section 3 - Process Where a Breach Occurs or is Suspected

Alert

(9) Where a privacy data breach is known or suspected to have occurred any ACU staff member who becomes aware

of this must, within 24 hours, alert a member of the Executive in the first instance.

> Note: the term ‘member of the Executive’ is defined in the Delegations of Authority Policy and Register.

(10) The Information that should be provided (if known) at this point includes:

a. the date and time of the breach;
b. description of the breach (type of personal information involved);
c. cause of the breach and / or its means of discovery;
d. which system(s) are affected if any;
e. which Directorate / Faculty / Institute is involved; and
f. whether corrective action has occurred to remedy or ameliorate the breach (or suspected breach).

(11) The Data Breach Process Form can assist in documenting the required information.

Assess and Determine the Potential Impact

(12) Once notified of the information above, the member of the Executive must consider whether a privacy data breach has (or is likely to have) occurred and make a preliminary judgement as to its severity. The Privacy Coordinator should be contacted for advice.

Criteria for Determining Whether a Privacy Data Breach has Occurred

(13) The key criteria for determining whether a privacy data breach has occurred include:

a. the involvement of personal information;
b. the potentially sensitive nature of the personal information; and
c. the occurrence of unauthorised access to personal information, unauthorised disclosure of personal information, or loss of personal information in circumstances where access to the information is likely to occur.

(14) For the purposes of this assessment the following terms are defined in Section 9 of the Privacy Policy: personal information, sensitive information, unauthorised access, unauthorised disclosure and loss.

Criteria for Determining Severity

(15) The criteria for determining the severity of a data breach include:

a. the type and extent of personal 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 kind of person or people who now have access;
e. whether a real risk of serious harm is posed to the affected individuals; and
f. whether there could be media or stakeholder attention as a result of the breach or suspected breach.

(16) With respect to 15(e) above, serious harm could include physical, physiological, emotional, economic / financial or harm to reputation and is defined in Section 9 of the Privacy Policy and section 26WG of the Privacy Amendment (Notifiable Data Breaches) Act 2017 (Cth).

(17) Having considered the matters in clauses (13) to (16), the member of the Executive must notify the Privacy Officer within 24 hours of being alerted.

Privacy Officer to Issue Pre-emptive Instructions

(18) On receipt of the communication by the relevant member of the Executive under clauses (13) to (16), the Privacy Officer will take a preliminary view as to whether the breach (or suspected breach) may constitute a notifiable data breach. Accordingly, the Privacy Officer will issue pre-emptive instructions as to whether the data breach should be managed at the local level or escalated to the Data Breach Response Team (Response Team). This will depend on the nature and severity of the breach.

Data Breach Managed at the Directorate / Faculty / Institute Level

(19) Where the Privacy Officer instructs that the data breach is to be managed at the local level, the relevant member of the Executive must:

a. ensure that immediate corrective action is or has been taken, including retrieval or recovery of the personal information, ceasing unauthorised access, shutting down or isolating the affected system); and
b. submit a report via the Privacy Coordinator within 48 hours of receiving instructions under Clause 18. The report must contain the following:
    i. description of breach or suspected breach;
    ii. action taken;
    iii. outcome of action;
    iv. processes that have been implemented to prevent a repeat of the situation;
    v. recommendation that no further action is necessary.

(20) The Privacy Officer will be provided with a copy of the report and will sign-off that no further action is required.

(21) The report will be logged by the Privacy Coordinator.

Data Breach Managed by the Response Team

(22) Where the Privacy Officer instructs that the data breach be escalated to the Response team, the Privacy Officer will convene the Response Team and notify the Vice-Chancellor and President.

(23) The Response team will consist of:

a. the Privacy Coordinator;
b. General Counsel (or nominee);
c. the Chief People Officer(or nominee);
d. the Academic Registrar (or nominee);
e. the Chief Information and Digital Officer (or nominee); and
f. the Chief Marketing Officer (or nominee).

Primary Role of the Response Team

(24) There is no single method of responding to a data breach and each incident must be dealt with on a case by case basis by assessing the circumstances and associated risks to inform the appropriate course of action.

(25) The following steps may be undertaken by the Response Team (as appropriate):

a. immediately contain the breach if not already contained. Corrective action may include: retrieval or recovery of the personal information, ceasing unauthorised access, shutting down or isolating the affected system;
b. evaluate the risks associated with the breach, including collecting and documenting all available evidence of

the breach having regard for the information outlined in clauses (13) to (16) above;

c. consult with relevant staff in the particular circumstances;
d. engage an independent cyber-security or forensic expert as appropriate;
e. assess the likelihood of serious harm (with reference to clauses (15) and (16) above and section 26WG of the Privacy Amendment (Notifiable Data Breaches) Act 2017 (Cth));
f. advise the Privacy Officer as to whether this breach constitutes a notifiable data breach for the purpose of mandatory reporting to the OAIC and the practicality of notifying affected individuals; and
g. consider the appropriateness of developing a communication or media strategy including the timing, content and method of any announcements to students, staff or the media with respect to the particular circumstances and nature of the breach.

(26) The Response Team must undertake its assessment within 48 hours of being convened.

(27) The Privacy Officer will provide periodic updates to the Vice-Chancellor and President as deemed appropriate.

Notification

(28) Having regard to the Response team's recommendation in clauses (29) to (31) above, the Privacy Officer will determine whether there are reasonable grounds to suspect that a notifiable data breach has occurred.

(29) If there are reasonable grounds, the Privacy Officer must prepare a prescribed statement and provide a copy to the OAIC as soon as practicable (and no later than 30 days after becoming aware of the breach or suspected breach).

(30) The Notifiable Data Breach Statement should be used as a template for the statement.

(31) If practicable, ACU must also notify each individual to whom the relevant personal information relates. Where impracticable, ACU must take reasonable steps to publicise the statement (including publishing on the website).

(32) The prescribed statement will be logged by the Privacy Coordinator.

Secondary Role of the Response Team

(33) Once the matters referred to in clauses (24) to (32) have been dealt with, the Response Team should turn attention to the following:

a. identify lessons learned and remedial action that can be taken to reduce the likelihood of recurrence – this may involve a review of policies and processes, and refresher training;
b. prepare a report for submission to Senate; and
c. Consider the option of an audit to ensure necessary outcomes are effected and effective.

Section 4 - Updates to this Procedure

(34) In line with the Policy Development and Review Policy, this Procedure is scheduled for review every five years or more frequently if appropriate.

Section 5 - Revisions Made to this Procedure

(35) Unless otherwise indicated, this policy will still apply beyond the review date.

Section 6 - Contact Details

(36) Contact for all matters related to privacy, including complaints about breaches of privacy, should be directed as follows:

> Privacy Coordinator
> E: privacy@acu.edu.au
> T: +617 3861 6415
> P: 1100 Nudgee Road, Banyo QLD 4014

Section 7 - Associated Information

(37) For related legislation, policies, procedures and guidelines and any supporting resources, please refer to the Associated Information tab.

Status and Details

Status	Current
Effective Date	15th March 2024
Review Date	30th April 2024
Approval Authority	Vice-Chancellor and President
Approval Date	15th March 2024
Expiry Date	Not Applicable
Responsible Executive	Diane Barker Director, Legal, Assurance and Governance
Responsible Manager	Matthew Charet National Manager, Governance
Enquiries Contact	Natalie Koppe Privacy Coordinator Legal, Assurance and Governance Directorate