Privacy Breach Management procedure

Section 1 - Preamble

(1) This Procedure is effective from 14 December 2020.

(2) This Procedure includes the following schedule:

a. Schedule A: Privacy Breach Risk Matrix.

Section 2 - Purpose

(3) This Procedure governs the University's approach to the management of privacy incidents and suspected or actual privacy breaches.

Section 3 - Scope

(4) This Procedure applies to all staff and associates of the University.

Section 4 - Policy

(5) This Procedure is pursuant to the Privacy policy.

Section 5 - Procedure

Identification

(6) A Privacy Breach is the unauthorised use, access, disclosure, modification or loss of personal information, whether deliberate or inadvertent.

(7) Examples of Privacy Breaches include inadvertently sending personal information to the wrong email address, deliberate intrusion into University records or information and communication technology (ICT) systems by external parties, loss or theft of computers, portable devices or hard copy documents.

(8) A Privacy Incident is an event that did not result in a Privacy Breach but had the potential to do so. A Privacy Incident may be caused by process, system or technology weaknesses. Staff are encouraged to report a Privacy Incident to their manager. Recurrent Privacy Incidents should be reported to the Privacy Officer.

Management

(9) Management of a Privacy Breach consists of four steps:

a. containment and preservation.

b. notification and assessment.
c. investigation.
d. correction and prevention.

Containment and Preservation

(10) All staff and associates must promptly take all reasonable steps to contain a suspected or actual Privacy Breach to limit or prevent any further access to or distribution of the affected personal information.

(11) Depending on the nature of the Privacy Breach those steps may include:

a. retrieving emails or hard copy documents;
b. suspending an activity;
c. suspending a process or system;
d. suspending access to a physical location; and
e. changing authentication and permissions.

(12) All available evidence relating to the Privacy Breach must be preserved.

Notification and Assessment

(13) All staff and associates must notify their supervisor, line manager or contractor officer as soon as possible after becoming aware of a suspected or actual Privacy Breach.

(14) On receipt of notification, the supervisor, line manager, or contractor officer must immediately:

a. confirm that appropriate action was or will be taken to contain the Privacy Breach;
b. report the Privacy Breach to the Privacy Officer; and
c. provide all evidence relating to the Privacy Breach to the Privacy Officer.

(15) On notification of a Privacy Breach the Privacy Officer will make a preliminary assessment of the Privacy Breach with reference to Schedule A: Privacy Breach Risk Matrix, and other relevant factors, and will notify the Chief Operating Officer and Chief Digital Officer of the nature and scope of the Privacy Breach, including any mandatory breach notification obligations or contractual obligations to notify third parties.

(16) In consultation with the Chief Operating Officer and Chief Digital Officer, the General Counsel will notify the police if the Privacy Breach involves or may involve criminal activity.

(17) The Chief Operating Officer and Chief Digital Officer may direct that:

a. the Privacy Officer or nominee assist the organisational unit to investigate and remediate the Privacy Breach;
b. a working group be established to manage the Privacy Breach;
c. a Critical Incident Management Team be convened pursuant to the Critical Incident Management policy and procedure; or
d. an external party be engaged to investigate the breach and make recommendations for correction and prevention.

(18) If the Critical Incident Management Team is convened, its direction will take priority over the balance of this Procedure.

Investigation

(19) If an investigation is required, it will be undertaken by the head of the relevant organisational unit, with the assistance of other subject matter experts as required and with the advice of the Privacy Officer.

(20) If a head of organisational unit has or may be perceived to have a conflict of interest, they must not participate in the investigation other than to provide information at the request of the investigators.

(21) The investigation will:

a. identify the cause of the Privacy Breach;
b. identify whether the Privacy Breach was an isolated occurrence or a systemic issue;
c. identify actions that have been taken to remediate the Privacy Breach; and
d. recommend corrective and/or preventative actions to reduce the likelihood of the breach recurring.

(22) The head of the relevant organisational unit (or investigator if the head is conflicted) will document the investigation in a report to the Privacy Officer. The report will cover the matters specified in clause 21 of this Procedure and have regard to the assessment and advice provided by the Privacy Officer.

(23) The Privacy Officer may make additional recommendations to the head of the relevant organisational unit.

Correction and Prevention

(24) The head of the relevant organisational unit is responsible for implementing and monitoring corrective and/or preventative actions recommended in the report and by the Privacy Officer.

Reporting

(25) The Privacy Officer will:

a. report privacy breaches to the Risk and Compliance Unit on a quarterly basis or as otherwise required;
b. report to the relevant regulator under a mandatory data breach notification scheme where required.

Section 6 - Definitions

(26) For the purpose of this Procedure:

a. Associates: contractors, consultants, volunteers, visiting appointees and visitors to the University.
b. Contractor Officer: the staff member who is responsible for the administration of the engagement of contractors and consultants for an organisational area under the Contractors and Consultants procedure.
c. Privacy Officer: as defined in the Privacy policy.

Status and Details

Status	Current
Effective Date	14th December 2020
Review Date	14th December 2021
Approval Authority	Vice-Chancellor
Approval Date	14th December 2020
Expiry Date	To Be Advised
Responsible Executive	Kerrie Parker Chief Financial Officer cfo@deakin.edu.au
Implementation Officer	Shirley Rooney General Counsel +61 3 52278560
Enquiries Contact	Shirley Rooney General Counsel +61 3 52278560