Data Breach Response Procedure

PROCEDURE PURPOSE

This Response Procedure is intended to enable UTS College to contain, assess and respond to data breaches in a timely fashion, to help mitigate potential harm to affected individuals. It sets out details of the appropriate staff to notify in the event of a data breach, clarifies the roles and responsibilities of staff, and sets out processes to assist UTS College to respond to a data breach. Under the *Privacy Act 1988* (Cth) (**Privacy Act**) and the *Privacy and Personal Information Protection Act 1998* (NSW) (**PPIP Act**), certain breaches of Personal Information must be notified to the individuals affected and reported to the Office of the Australian Information Commissioner ('**OAIC**') and the NSW Privacy Commissioner.

SCOPE

This Response Procedure applies to Personal Information that is collected by Insearch Limited and its subsidiaries (including offshore subsidiaries) (together '**UTS College**').

This Response Procedure is to be followed by Insearch staff (including casual and sessional staff), contractors, any other person appointed or engaged by Insearch to perform work or functions for UTS College, and volunteers) in the event that UTS College experiences a data breach, or suspects that a data breach has occurred.

UTS College is bound by both the Commonwealth Privacy Act and the NSW PPIP Act. Accordingly, if there has been an eligible data breach as defined in this procedure, UTS College will take necessary steps to notify OAIC under the Commonwealth NDB scheme, the NSW Privacy Commissioner under the MNDB scheme and Affected individuals.

DEFINITIONS are set out at the end of this procedure.

PROCEDURE STEPS

Activity
1. IDENTIFICATION AND ASSESSMENT OF DATA BREACH
1.1 Preparation UTS College takes active steps to prepare for a data breach. This includes the following controls, which UTS College has implemented to ensure it is capable of promptly identifying actual or suspected data breaches, and to ensure they are effectively managed in accordance with this policy. These controls include: ▪ technical controls (such as data loss prevention tools) monitoring services (such as dark web monitoring, or social media monitoring) ▪ audits and reviews ▪ staff training and awareness; and ▪ appropriate provisions in contracts.

1.2 Notify actual or suspected data breach

Where an UTS College staff member discovers and actual or suspected data breach, or UTS College is otherwise alerted to an actual or suspected data breach, staff must immediately:

- email a notification to their manager, Executive, and the CFO/Company Secretary (with a copy to privacy@utscollege.edu.au)
- provide details of the time and date the actual or suspected data breach was discovered, the type of Personal Information involved, the cause and extent of the data breach, and the context of the affected information and the data breach.

1.3 Data Breach Response Team

The CFO/Company Secretary or Privacy Officer will:

- determine whether a data breach has or may have occurred on the basis of the notification provided
- determine whether the data breach is serious enough to escalate to the Data Breach Response Team ('**Response Team**'); and
- if so, immediately convene a meeting of the Response Team.

1.4 Assessment of data breach

Some data breaches may be comparatively minor, and able to be dealt with easily without action from the Response Team. For example, a UTS College staff member may, as a result of human error, send an email containing Personal Information to the wrong recipient. Depending on the sensitivity of the contents of the email, if the staff member can contact the recipient and the recipient agrees to delete the email, it may be that there is no utility in escalating the issue to the Response Team.

The CFO/Company Secretary or Privacy Officer should use their discretion in determining whether a data breach or suspected data breach requires escalation to the Response Team. In making that determination, the CFO/Company Secretary or Privacy Officer should consider the following questions:

- Are multiple individuals affected by the data breach or suspected data breach?
- Is there (or may there be) a real risk of serious harm to the affected individual(s)?
- Does the data breach or suspected data breach indicate a systemic problem in UTS College processes or procedures?
- Could there be media or stakeholder attention as a result of the data breach or suspected data breach?

If the answer to any of these questions is 'yes', then it may be appropriate for the CFO/Company Secretary or the Privacy Officer to convene a meeting of the Response Team.

2. MINOR DATA BREACHES

2.1 Minor data breaches

If the CFO/Company Secretary or Privacy Officer decides not to escalate a minor data breach or suspected data breach to the Response Team for further action, they will:

- determine the action required to address the data breach or suspected data breach
- require managers of the relevant department(s) to ensure the action is communicate the action required to managers of the relevant department(s) promptly completed and such completion is reported to the Governance department and where relevant, to the Cyber Security Committee
- record a copy of the notification of the data breach or suspected data breach, correspondence about the assessment process and the reason for their view that no further action is required; and
- provide aggregate reporting on minor data breaches to the UTS College Audit & Risk Committee (**ARC**) in the Compliance Incident Log.

3. SERIOUS DATA BREACHES

3.1 Response Team Meeting

The following process applies if the CFO/Company Secretary or Privacy Officer convenes a meeting of the Response Team.

Data breaches must be dealt with on a case-by-case basis, by undertaking an assessment of the risks involved, and using that risk assessment to decide the appropriate course of action.

There are four key steps to consider when responding to a data breach or suspected data breach.

- STEP 1: Contain the data breach and do a preliminary assessment
- STEP 2: Evaluate the risks associated with the data breach
- STEP 3: Consider data breach notification
- STEP 4: Prevent future data breaches

The Response Team should ideally undertake steps 1, 2 and 3 either simultaneously or in quick succession. The Response Team should refer to the OAIC's Data breach notification: a guide to handling personal information.

3.2 STEP 1: Contain the data breach and do a preliminary assessment

- Determine whether the data breach should be escalated to the Crisis Management Team under the UTS College Business Management Plan (e.g. if there is an ongoing data breach and a decision needs to be made on decommissioning the affected ITDS service(s)). The Crisis Management Team will assess if a crisis is declared and the Business Continuity Plan is invoked
- Immediately contain data breach:

- Escalate data breach to ITDS team, for assessment as a Priority 1 incident
- Inform the CEO; provide ongoing updates on key developments

- Ensure evidence is preserved that may be valuable in determining the cause of the data breach, or allowing UTS College to take appropriate corrective action
- Consider developing a communications or media strategy to manage public expectations and media interest.

3.3 STEP 2: Evaluate the risks associated with the data breach

- Conduct an initial investigation, and collect information about the data breach promptly, including:
  - the date, time, duration, and location of the data breach
  - the type of Personal Information involved in the data breach
  - how the data breach was discovered and by whom
  - the cause and extent of the data breach
  - a list of the affected individuals, or possible affected individuals
  - the risk of serious harm to the affected individuals
  - the risk of other harms
- Determine whether the context of the information is important
- Establish the cause and extent of the data breach
- Assess priorities and risks based on what is known
- Keep appropriate records of the suspected data breach and actions of the Response Team, including the steps taken to rectify the situation and the decisions made. Include incident in the Compliance Incident Log maintained by the Governance department.

3.4 STEP 3: Consider data breach notifications

- Determine who needs to be made aware of the data breach (internally, and potentially externally) at this preliminary stage
- Determine whether the data breach is an Eligible data breach, having regard to the OAIC's Identifying eligible data breaches guide
- For Eligible data breaches, provide a statement to the OAIC
- For Eligible data breaches, determine how to notify affected individuals, having regard to the OAIC's Notifying individuals about an eligible data breach guide. In some cases, it may be appropriate to notify the affected individuals immediately e.g., where there is a high level of risk of serious harm to affected individuals
- The Response Team will need to consider three options for notifying individuals, having regard to what is practicable for UTS College:
  - notify all individuals
  - notify only those individuals at risk of serious harm; or
  - publish a copy of the statement to the Commissioner on the UTS College website and take reasonable steps to publicise it
- Where a single Eligible data breach involves UTS College and one or more other entities, only one entity needs to notify the Commissioner and individuals at risk of serious harm. This should be determined between UTS College and the other entity or entities involved, having regard to any relevant contractual provisions and which entity has the most direct relationship with the individuals at risk of serious harm

- Consider whether others should be notified, including police/law enforcement, or other organisations affected by the data breach, or where UTS College is legally and/or contractually required to notify specific parties.

3.5 STEP 4: Prevent future data breaches

- Review the incident and take action to prevent future data breaches.
- Where relevant, actions may be referred to the Cyber Security Committee for ongoing review
- Fully investigate the cause of the data breach
- Report to the ARC on outcomes and recommendations:
  - Update security and response plan if necessary
  - Make appropriate changes to policies and procedures if necessary
  - Revise staff training practices if necessary
  - Consider an internal audit to ensure agreed actions are completed.

In reconsidering OAIC processes and procedures to reduce the risk of future breaches (STEP 4), the Response Team should also refer to the OAIC's Guide to securing personal information. This guide presents a set of non-exhaustive steps and strategies that may be reasonable for UTS College to take in order to secure Personal Information, and considers actions that may be appropriate to help prevent further breaches following an investigation.

3.6 Records management and Reporting

The Governance department will:

- record a copy of the notification of the data breach or suspected data breach, correspondence about the assessment and investigation process and details of actions taken
- prepare the report on each Serious data breach to the ARC; and
- update the Compliance Incident Log with information about the data breach and the action plan implemented.

DEFINITIONS

Affected individual	This term has the meaning given to that term under the PPIP Act
Data breach	Occurs when Personal Information is lost or subjected to unauthorised access, modification, use or disclosure or other misuse. The Personal Information may be recorded electronically, in hard copy or verbal. Data breaches can be caused or exacerbated by a variety of factors, affect different types of Personal Information and may give rise to actual or potential harm to individuals and organisations
Data Breach Response Team	The management team that will assess Eligible data breaches, consisting of: ▪ CFO/Company Secretary ▪ Head of Finance and Governance

	▪ Privacy Officer ▪ Head of ITDS; and ▪ the relevant manager (if required)
Eligible data breach	A data breach that is likely to result in serious harm to any individual to whom the information relates, where UTS College has not been able to prevent the likely risk of serious harm with remedial action. The likely risk of serious harm will be assessed using the OAIC's Identifying eligible data breaches guide.
Executive	Executive of UTS College
NSW Privacy Commissioner	The NSW Privacy Commissioner is the NSW privacy regulator
OAIC	Office of the Australian Information Commissioner, the Federal privacy regulator
Personal Information	Personal Information is defined as information or an opinion about an identified individual, or an individual who is reasonably identifiable: ▪ whether the information or opinion is true or not; and ▪ whether the information or opinion is recorded in any format or not. This is consistent with the definition of 'personal information' under the Privacy Act and the PPIP Act
UTS College	UTS Colelge Limited, its representative offices and its controlled entities

SUPPORTING DOCUMENTS:

[Include the title of supporting documents such as legislation, associated policies, related procedures and other UTS College resources.]

- *Privacy Act 1988* (Cth)
- Privacy Policy
- Information Classification Policy
- Document and Data Classification Procedure
- Business Continuity Plan
- Cyber Security Committee Charter

ADMIN USE ONLY

APPROVAL		
Position title:	**CEO**	Date: 19 March 2024
Procedure Title	Data Breach Response Procedure	
Executive	CFO/Company Secretary	
Manager	Head of Finance and Governance	
Procedure ID	PROC/GOV/00/24	
Effective Date	19 March 2024	
Approved by	**Executive**	**Date 19 March 2024**

VERSION HISTORY

No.	Author	Description of change/purpose	Date
1.0		October 2022	
1.1	Legal	Legal and position titles update	March 2024