UNSW College

Data Breach Policy and Procedure

1. Purpose

This Policy and Procedure describes the principles and procedures for responding to a breach of UNSW College (College) held data, including managing a data breach and notification of persons whose privacy may be affected by the breach. It establishes responsibility and accountability for all steps in addressing information security incidents resulting in data breaches and describes clear roles and responsibilities. It also describes the principles and procedures relating to internal and external notification and communication of such data breaches.

2. Scope

This Policy and Procedure applies to all staff and students of the College, and contractors, third party vendors, agents and consultants of the College.

3. Policy statement

The following principles guide College staff in identifying, assessing, managing and responding to a breach of data held by the College:

(a) Data is an important business asset that must be protected.

(b) Personal information and health information held by the College is managed in accordance with the APPs, IPPs and HPPs, and other applicable privacy laws and contractual obligations.

(c) A robust data breach management program assists the College in complying with its legislative obligations to protect data; avoiding or reducing possible harm to affected individuals and the College; and may prevent future breaches.

(d) Data breaches are reported as soon as they are identified.

(e) Data breaches are assessed and managed systematically and effectively in accordance with the Data Breach Management Plan set out in clauses 0to 5.13.

(f) Affected individuals and entities are appropriately notified of a data breach in accordance with legislative obligations.

(g) Data breaches are accurately recorded to enable the College to comply with legislative obligations and monitor, analyse and review the type and severity of suspected data breaches and the effectiveness of its response.

(h) The College's training in data governance, recordkeeping, privacy and cyber security enables College staff to effectively and efficiently identify, respond to and manage a data breach.

For the purpose of the *Privacy and Personal Information Protection Act 1998* (NSW) (PPIP Act), and in accordance with s59ZJ, the functions of the CEO, acting as the head of the College for the purpose of the PPIP Act, are delegated to the Chief of Staff.

This document also serves as a data breach response plan for the purposes of the *Privacy Act 1988* (Cth).

4. Types of data breach

4.1. What is a Data Breach?

A Data Breach occurs when **any** information (whether in digital or hard copy) held by the College is subject to unauthorised access or disclosure, or is lost. A Data Breach may be caused by malicious action (by an external or insider party), human error, or a failure in information handling or security systems.

Examples of data breaches include:

(a) loss or theft of physical devices (such as laptops and storage devices) or paper records that contain College information;

(b) unauthorised access to College information by an employee;

(c) inadvertent disclosure of College information due to 'human error', for example an email sent to the wrong person;

(d) a compromised user account (e.g., accidental disclosure of user login details through phishing).

4.2. What is an Eligible Data Breach?

An Eligible Data Breach involves **personal information**.

It occurs when there is an unauthorised access to, or unauthorised disclosure of, **personal information** held by the College or there is a loss of personal information held by the College in circumstances that are likely to result in unauthorised access to, or unauthorised disclosure of, the information, and 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.

Examples of an Eligible Data Breach includes:

(a) loss or theft of a device containing personal information of the College, a College database or information repository containing personal information being hacked;

(b) a device containing personal information of the College, a College database or information repository containing personal information being accessed without authorisation;

(c) the College inadvertently providing personal information to an unauthorised person or entity that would likely result in serious harm to an individual to whom the information relates.

5. Procedure

5.1. Reporting a Data Breach

College staff and students, or contractors, may report a confirmed or suspected Data Breach to the IT Service Desk at databreach@unswcollege.edu.au or on +61 (2) 8936 2215.

In reporting the Data Breach, the following should be provided:

(a) the date of the Data Breach;

(b) the cause of the Data Breach;

(c) a brief description of the Data Breach, including individuals and systems affected, and extent of personal information that was involved in the Data Breach.

5.2. Data Breach Response Team

Upon receipt of a confirmed or suspected Data Breach, the IT Service Desk will immediately inform the Head of Legal, Risk & Compliance, the Privacy Officer and the Head of IT. On receipt, the Head of Legal, Risk & Compliance, as chair of the Data Breach Response Team, will immediately notify all members of the Data Breach Response Team.

The Data Breach Response Team consists of:

(a) the Head of Legal, Risk & Compliance (chair);

(b) the Privacy Officer;

(c) the Head of IT;

(d) Head of Marketing, Future Students;

(e) if applicable, the "Head of" the Business Unit where the Data Breach, or suspected Data Breach, has occurred;

(f) other staff as required, such as:

   i. the Executive Director, Future Students and Business Development, if the Data Breach involves a future student;

   ii. the Executive Director, Students, if the Data Breach involves a current student.

5.3. Data Breach management

Each Data Breach should be assessed on a case by case basis and no template response can be applied all cases. However, there are five (5) key steps the Data Breach Response Team is to consider when responding to a data breach:

(a) contain the breach and conduct a preliminary assessment;

(a) evaluate the associated risks;

(b) recovery;

(c) consider notifying affected individuals, relevant privacy commissioners or other government bodies, or escalation to the College's Executive Team;

(d) prevent a repeat.

Sections 0 to 5.13 comprises the Data Breach Management Plan and sets out these steps in greater detail.

5.4. Data Breach Management Plan – Initial meeting of the Data Breach Response Team

On receipt of a notification of a Data Breach, the Head of Legal, Risk & Compliance will arrange for the Data Breach Response Team to meet. This meeting should take place no later than 24 hours after the notification. The Data Breach Response Team will discuss and take the necessary steps to cover the Data Breach management principles at clause 5.3, including:

(a) (if there are reasonable grounds to suspect the Data Breach is an Eligible Data Breach) reporting to the Chief of Staff of the potential Eligible Data Breach;

(b) assigning a member of the Data Breach Response Team (such as the Privacy Officer) as the Lead Investigator to assess and manage the Data Breach in accordance with the Data Breach Management Plan;

(c) assigning a member of the Data Breach Response Team (such as the Privacy Officer) to provide updates to the the Privacy Officer;

(d) taking steps to provide support and guidance to the person that identified the Data Breach.

The Data Breach Response Team shall not appoint a person as Lead Investigator if they reasonably suspect that person's action or omission led to the Data Breach.

5.5. Data Breach Management Plan – Investigating the Data Breach

Upon referral of a suspected or confirmed Data Breach or Eligible Data Breach, the Lead Investigator will contain the breach and conduct a preliminary assessment. The assessment requires an assessment of whether the Data Breach is likely to result in serious harm to any of the affected individuals. The Lead Investigator will complete the assessment of whether there is an Eligible Data Breach within 30 days.

5.6. Data Breach Management Plan – contain the breach and conduct preliminary assessment

The breach may be contained by:

(a) stopping the unauthorised activity; and/or

(b) recovering or limiting the dissemination of records disclosed without authorisation; and/or

(c) shutting down a compromised system.

The preliminary assessment will address the following:

(a) Who is affected by the breach?

(b) What information does the breach involve?

(c) If the information contains personal information, what types of personal information does the breach involve?

(d) Does the breach result in unauthorised access to, or unauthorised disclosure of, the information?

(e) Would a reasonable person conclude that the access or disclosure of the information will likely result in serious harm to an individual to whom the information relates?

In deciding whether the breach would be likely to result in **serious harm** to an individual to whom the information relates, the following should be considered:

(a) the types of personal information involved;

(b) the sensitivity of the personal information;

(c) whether the personal information is or was protected by security measures such as encryption and therefore unlikely to be accessed or misused;

(d) who has access to the personal information;

(a) whether the person/s who accessed the personal information may have malicious intent and whether they may be able to circumvent security measures; and

(b) the nature of the harm that has occurred or may occur.

The Lead Investigator will assess the risks associated with the breach by considering the following questions:

(a) What was the cause of the breach?

(b) What is the extent of the breach?

(c) Is there a risk of ongoing breaches or further exposure of the information?

(d) Is there evidence of theft?

(e) Is this a systemic problem within the College or an isolated incident?

(f) How many people are affected by the breach?

(g) What other harm could result from the breach?

(h) Have there been other breaches that could have a cumulative effect?

(i) How could the information be used?

(j) Has the information been recovered?

(k) What steps have already been taken to mitigate the harm?

(l) Is there a reputational risk to the College?

(m) Is there a commercial or intellectual property risk for the College?

If there are reasonable grounds to suspect, or there is evidence to conclude, that an Eligible Data Breach or a Data Breach has occurred, the Lead Investigator will immediately report their conclusion to the Chief of Staff and the Data Breach Response Team.

5.7. Data Breach Management Plan - notification to privacy commissioners

Where the Data Breach Response Team concludes or has reasonable grounds to suspect that the Data Breach amounts to an Eligible Data Breach and the Chief of Staff agrees with this assessment, the Chief of Staff will (with the Privacy Officer's and the Data Breach Response Team chair's assistance, if required):

(a) immediately notify the OAIC under the Commonwealth Notifiable Data Breaches scheme using OAIC's online form, unless an exception applies;

(b) immediately notify the IPC under the NSW mandatory notification of data breach scheme using the IPC's approved form, unless an exception applies.

5.8. Data Breach Management Plan - notification to affected individuals

As soon as practicable, the Chief of Staff (with the Privacy Officer's and the Data Breach Response Team chair's assistance, if required) will send written notification to each affected individual or their authorised representative, unless exempt from doing so.

The notification to each individual will provide affected individuals with an accurate description of what happened, what risks may arise and what they can do to protect themselves. The notification will specifically contain the following information:

(a) the date the breach occurred;

(b) a description of the breach;

(c) how the breach occurred;

(d) the type of breach that occurred;

(e) the personal information that was the subject of the breach;

(f) the amount of time the information was disclosed for;

(g) actions the College has taken or plans to ensure the personal information is secured;

(h) actions the College has taken to control or mitigate the harm done to the individual;

(i) recommendations about the steps the individual should consider taking in response to the Eligible Data Breach; and

(j) information about:

  i. how to make a privacy-related complaint to the OAIC or IPC commissioners;

  ii. how to seek an internal review of the College's conduct; and

  iii. the contact details for the College, or a person nominated by the College, for the individual to contact about the breach.

If it is not reasonably practicable to directly notify any or all the individuals affected by the breach, the Chief of Staff will:

(a) arrange to have published a public notification on the College's website for at least 12 months detailing information about the breach, such as: the date the breach occurred, how the breach occurred, the type of breach that occurred, the amount of time the information was disclosed, actions taken or planned to ensure the personal information is secure, and where to contact for assistance or information;

(b) take reasonable steps to publicise that notification; and

(c) provide the IPC commissioner with information about how to access the public notification on the College's website.

5.9. Data Breach Management Plan – notification to third parties

The Data Breach Response Team, consulting with relevant senior staff of the College as required, will determine if it is appropriate and necessary to notify other third parties, such as:

(a) the Police;

(b) insurance providers;

(c) credit card companies and/or financial institutions;

(d) professional or other regulatory bodies;

(e) other internal or external parties who have not already been notified.

5.10. Data Breach Management Plan – notification to UNSW Privacy Officer

A representative from the Data Breach Response Team (such as the Privacy Officer) will provide an update to the UNSW Privacy Officer following the initial meeting of the Data Breach Response Team. They will provider further and regular updates to the UNSW Privacy Officer as necessary.

5.11. Data Breach Management Plan – notification to the staff or student that reported the breach

The chair of the Data Breach Response Team will notify the staff member or student who reported the breach of the outcome of the Data Breach and assist them in responding to any requests for information in relation to the breach from stakeholders or other third parties.

5.12. Data Breach Management Plan – GDPR notification

If a Data Breach relates to data being collected or processed under the GDPR, the Data Breach Response Team must take the following additional actions:

(a) If the College is the data Processor, inform the data Controller about the breach immediately and without undue delay.

(b) If the College is the data Controller, the Data Breach Response Team must:

i. Conduct an assessment to determine if the Data Breach can be classified as a Personal Data Breach that can result in a risk to the rights and freedoms of natural persons.

ii. Report Personal Data Breaches to their Supervisory Authority no later than 72 hours after becoming aware of it, except if the breach is unlikely to result in a risk to the rights and freedoms of natural persons. Notification to their Supervisory Authority should be provided in accordance with Article 33 of the GDPR. See here for a list of Supervisory Authorities in the European Union and the Supervisory Authority's contact details.

(c) Report Personal Data Breaches to affected Data Subjects, except if:

i. the breach is unlikely to result in a high risk for the rights and freedoms of data subjects; or

ii. appropriate technical and organisational protection were in place at the time of the incident (e.g. encrypted data); or

iii. this would trigger disproportionate efforts.

5.13. Data Breach Management Plan – prevention of future breaches

Once immediate steps have been taken to mitigate the risks associated with a breach, and relevant notifications have been made, the Lead Investigator will:

(a) investigate the cause of the breach;

(b) conduct a post-breach review and evaluation on the root cause of the breach;

(c) in consultation with the Head of Legal, Risk & Compliance, identify if there is a risk of legal proceedings against the College as a result of the breach (e.g. class action by affected individuals) and provide a report to the Data Breach Response Team.

The Chair of the Data Breach Response Team will:

(a) on behalf of the Data Breach Response Team, provide a brief to the College Audit and Risk Committee or the UNSW Board of Directors on the outcome of the post-breach review and relevant recommendations (such as further training for staff, or changes to data and information handling processes and physical and/or electronic security measures);

(b) publish information about the Data Breach, the steps the College took to mitigate the harm done by the breach and the actions to prevent future breaches in the College's internal Data Breach Incident Register.

5.14. Testing and updating the Data Breach Management Plan

To ensure currency and effectiveness, the College will review, test and update (if necessary) the Data Breach Management Plan.

6. Roles, responsibilities and delegations

Role	Responsibility
UNSW College staff	Identifies and reports a suspected or confirmed Data Breach or Eligible Data Breach. Implements measures to ensure the College's data is protected.
IT Service Desk	Reports any regarding Data Breach or Eligible Data Breach to selected members of the Data Breach Response Team.
Lead Investigator	Investigates the suspected or confirmed Data Breach or Eligible Data Breach.
Data Breach Response Team	Implements the Data Breach Management Plan for suspected or confirmed Data Breach or Eligible Data Breach, appoints Lead Investigator, notifies Chief of Staff of suspected or confirmed Eligible Data Breach.
Head of Legal, Risk & Compliance	Chairs the Data Breach Response Team, and co-ordinates the formation of the Data Breach Response Team upon receipt of a confirmed Data Breach or suspected Data Breach.
Chief of Staff	Notifies the IPC or OAIC and affected individuals in the case of an Eligible Data Breach. In accordance with s59ZJ of the PPIP Act, is delegated with the functions of the CEO.

7. Definitions

Definitions and Acronyms	
APPs	The obligations prescribed by the *Privacy Act 1988* (Cth) by which the College must abide when it collects, stores, uses or discloses personal information.
Controller	Has the meaning given under the *GDPR*, being the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.
Data Breach	Has the meaning given in clause 4.1 of this document
Data Breach Management Plan	The plan of action that is determined by the Data Breach Response Team to contain and remediate the Data Breach.
Data Subject	has the meaning given under the *GDPR*, being an identified or identifiable natural person whose personal data is processed by a Controller or Processor.
Eligible Data Breach	Has the meaning given in clause 4.2 of this document.
GDPR	means the General Data Protection Regulation (Regulation (EU) 2016/679)
HPPs	The obligations prescribed by the *Health Records and Information Privacy Act 2002* (NSW) by which the College must abide when it collects, stores, uses or discloses health information.
IPC	Information and Privacy Commission NSW (who oversees the NSW privacy legislation).
IPPs	The obligations prescribed by the *Privacy and Personal Information Protection Act 1998* (NSW) by which the College must abide when it collects, stores, uses or discloses personal information.
OAIC	Office of the Australian Information Commissioner (who oversees the *Privacy Act 1988* (Cth)).
Personal Data Breach	has the meaning given under the GDPR, breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.
Personal information	Means information or an opinion about an identified individual, or an individual who is reasonably identifiable: (a) whether the information or opinion is true or not; and (b) whether the information or opinion is recorded in a material form or not.
Processor	has the meaning given under the *GDPR*, being a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.
Serious Harm	means serious physical, psychological, emotional, economic and financial harm, as well as serious harm to reputation and other forms of serious harm that a reasonable person in the entity's position would identify as a possible outcome of the data breach.

	Examples of serious harm include: (a) financial fraud including unauthorised credit card transactions or credit fraud; (b) identity theft causing financial loss or emotional and psychological harm; (c) family violence; (d) physical harm or intimidation.
Supervisory Authority	has the meaning given under the GDPR, being an independent public authority which is established by a Member State pursuant to Article 51.

Related Policy Documents and Supporting Documents	
Legislation	General Data Protection Regulation (Regulation (EU) 2016/679) Privacy Act 1988 (Cth) Privacy and Personal Information Protection Act 1998 (NSW)
Policy	Privacy Policy
Procedures	N/A
Forms	IPC's approved form for notification of Eligible Data Breaches. OAIC's online form for notification of Eligible Data Breaches.
Superseded documents	Data Breach Response Procedure v1.0.

8. Policy & Procedure Governance

Data Breach Policy & Procedure	
Category/Business Group	Legal and Compliance
Published Externally (Yes/No)	Yes
Approver	Chief of Staff (delegated by Chief Executive Officer)
Responsible Officer	Head of Legal and Compliance
Contact Officer	Privacy Officer
Effective Date	1/01/2024
Next Review Date	1/01/2027
Version	1.0

Revision History

Version	Approved by	Approval date	Effective date	Sections modified
1.0	Chief of Staff – Mai-Lynda Allen (delegated by	15 Dec 2023	01 Jan 2024	This is a new policy and procedure, to comply with the IPC's data breach policy checklist and to

	Chief Executive Officer)			align with UNSW's corresponding combined policy and procedure. This supersedes the Data Breach Response Procedure.

Please visit our website to ensure that you have the latest version of this Policy. Policies are available at: unswcollege.edu.au/about/policies