People & Culture

Privacy & Data Breach Policy

Date approved:	January 2024	**Date Policy will take effect:**	January 2024	**Date of Next Review:**	January 2027
Approved by:	Cheif Operating Officer				
Custodian title:	Head of People & Culture				
Author:	Head of People & Culture				
Responsible Unit:	People & Culture				
Supporting documents, procedures & forms of this policy:	Not applicable				
References & Legislation:	*Privacy Act 1998 (Cth)* *Australian Privacy Principles (APP)* *Health Records and Information Privacy Act 2022 (NSW) (HRIPA)* *Privacy and Personal Information Protection Act 1998 (NSW)* *(PPIPA) Public Interest Disclosure Act 1994 (NSW)* *UOW Pulse Code of Conduct*				
Audience:	Internal				
Expiry Date of Policy (if applicable):	Not Applicable				

Contents

1 Introduction / Background

1.1. UOW Pulse Ltd carries out its functions and activities, collects personal and/or health information from employees, students, customers and third parties. It is the responsibility of UOW Pulse to ensure that the overall management of that information, which includes the collection, storage, access, use and disclosure, complies with relevant Australian privacy laws and regulations.

1.2. The purpose of this policy is to set out:

(a) UOW Pulse's commitment to compliance with the Privacy Act 1988 (Commonwealth), the Privacy and Personal Information Protection Act 1998 ("PPIPA"), the Health Records and Information Privacy Act 2002 ("HRIPA") and other relevant privacy laws.

(b) TThe strategies to effectively respond to a Data Breach at UOW Pulse to ensure best practice data breach management, reduce possible harm to individuals and organisations and prevent future breaches;

2 Scope

2.1 This policy outlines the responsibilities of all employees when handling information to ensure that UOW Pulse complies with the relevant privacy laws.

2.2 This policy applies to the collection, storage, access, use and disclosure of information.

2.3 This policy defines the process, management and notifications associated with identified breaches of this Privacy & Data Breach Policy.

2.4 All UOW Pulse employees are bound by and must comply with the Privacy & Data Breach Policy.

2.5 A breach of this Privacy & Data Breach Policy would be considered very seriously by UOW Pulse and would be subject to investigation and possible disciplinary action.

3 Definitions

Word/Term	Definition
Data Breach	Data (whether held in digital or hard copy) is subject to unauthorised access, unauthorised disclosure or is lost in circumstances where the loss is likely to result in unauthorised access or unauthorised disclosure. A data breach may occur as the result of malicious action, systems failure, or human error.
Customer	A member of the public who visits the campus and either purchases products or utilises the services or facilities under UOW Pulse management.
Eligible Data Breach	An 'eligible data breach' under the MNDB Scheme requires two conditions to be met: 1. 1. There is an unauthorised access to, or unauthorised disclosure of, Personal information or Health information held by UOW Pulse or there is a loss of Personal information or Health information held by UOW Pulse in circumstances that are likely to result in unauthorised access to, or unauthorised disclosure of, the information, and 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 i.
Health Information	The Privacy Act defines 'health information' as follows: (a) Information or an opinion about: i. The health, including an illness, disability or injury (at any time) of an individual; or ii. An individual's expressed wishes about the future provision of health services to the individual; or iii. A health service provided, or to be provided, to an individual, that is also personal information; or (b) Other personal information collected to provide, or in providing, a health service to an individual.

Information	Any health information, sensitive information and/or personal information that is collected by UOW Pulse about a student, employee, customer, visitor or third party in the course of its operations.
Line Manager	An employee of UOW Pulse who acts in a supervisory or leadership capacity (whether acting or permanent) to other team members of UOW Pulse.
Personal Information	Is defined by PIPPA and the Privacy Act as: "information or an opinion about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion". Personal information does not include information: • About an individual who has been deceased for more than 30 years; • Which is publicly available; • About an individual contained in a public interest disclosure under the *Public Interests Disclosure Act;* or • An opinion about an individuals suitability for appointment or employment as a public sector official.
Primary purpose	Means the main purpose for which the information was collected.
Sensitive information	Defined by the *Privacy Act* as a subset of Personal Information, which includes: i. Information or an opinion about an individuals: a. Race, racial or ethnic origin; b. Political opinions; c. Membership of a political association; d. Religious beliefs or affiliations; e. Philosophical beliefs; f. Membership of a professional or trade association; g. Membership of a trade union; h. Sexual preference or practices; or i. Criminal record ii. Health information about an individual; or iii. Genetic information about an individual that is not otherwise Health Information
Serious harm	Defined in the context of a data breach, Serious Harm may include serious physical, psychological, emotional, financial or reputational harm. Assessing whether an eligible data breach is likely to result in serious harm, the following will be considered: i. The kinds of information; ii. The sensitivity of the information; iii. Whether the information is protected by one or more security measures or technology; iv. The persons, or the kinds of persons, who have obtained or who could obtain the information; v. The likelihood of the person who has obtained the information causing harm to any individuals to whom the information relates; vi. The nature of the potential harm; and vii. Any other relevant matters.
Employee	All persons employed by UOW Pulse of any seniority and including those in continuing, part-time, maximum term, casual, trainee or contract roles.
Students	A person registered for a course at the University of Wollongong.
Use (of information)	Means the communication or handling of information within UOW Pulse.
Visitor	An external person or business representative visiting the campus but not necessarily to purchase or utilise services, including but not limited to contractors, franchisees, members of the community and volunteers.

4 Information you give us

4.1. UOW Pulse will collect information in an open manner, including informing individual's why the information is being collected and how it will be used.

4.2. The information we collect is directly related to our functions and activities and may include:

4.2.1. Registration details when you establish a membership account with Pulse Perks;

4.2.2. Personal and health information when you set up a membership account with UniActive;

4.2.3. Information captured at application, selection, recruitment or on-boarding processes;

4.2.4. Information provided when you participate in promotions, competitions or surveys;

4.2.5. Marketing preferences;

4.2.6. Transactional information from online services;

4.2.7. CCTV images from equipment in place in and around our facilities for the purpose of prevention and detection of crime and public safety;

4.2.8. The Children's Services Group (Long Day Care Centres, After School Care and Vacation Care facilities) are a highly regulated industry and by laws are required to collect a comprehensive amount of information as part of the enrolment process. The information required is very specific and detailed covering personal and health information, developmental information and any court orders affecting custody of the child.

4.3. UOW Pulse will collect information directly from the individual to which it relates, unless:

4.3.1. The person has consented to information being collected on their behalf by a someone else;

4.3.2. The person is under 16 years of age and the information has been provided by a parent or guardian; or

4.3.3. It is unreasonable or impracticable to do so.

4.4. At the time of collection (or as soon as practicable thereafter) UOW Pulse will take reasonable steps to ensure that the individual is aware of:

4.4.1. The identity of UOW Pulse and how to contact the organisation;

4.4.2. The fact that individuals are able to obtain access to their information;

4.5. UOW Pulse will provide individuals with the option of not identifying themselves, or of using a pseudonym when it is practical and lawful to do so.

5 How we use the information we collect

5.1. UOW Pulse may use information for the following purposes:

5.1.1. Improving the customer experience and our quality of service;

5.1.2. Collecting payment, processing and fulfilling your order, provided order tracking facilities, or otherwise providing you with the information, products and services you may request from us;

5.1.3. Complying with our legal and regulatory obligations (including fraud prevention, anti-money laundering and sanction screening). This may include checking the information you provide us against information from other sources.

5.1.4. Contacting you (including by email or SMS) with marketing messages to inform you of special promotions, events and programs on offer, which may be opted out of at any time.

5.1.5. Providing you with any alerts, in app messages or other messages you have registered to receive;

5.1.6. Providing you with service messages, notifying you about changes to our services or changes to our terms and conditions;

5.1.7. Data analysis to allow us to derive insight and opportunities to improve our business processes, product offerings and quality of service;

5.1.8. Personal information will only be collected in so far as it relates to the service's activities and functions.

6 Information we share

6.1. We do not share the information with companies, organisations or individuals outside of UOW Pulse for marketing purposes or otherwise, nor do we sell your personal information. The only time your personal information may be shared with a third party is if:

6.1.1. We have your prior consent to do so;

6.1.2. We are processing information externally, through a trusted business partner, based on UOW Pulse's explicit instruction and in compliance with our Privacy Policy, confidentiality and levels of security;

6.1.3. We have aggregated, identifiable information, which is to be used for segmentation, statistical modelling, general research or trend analysis;

6.2. We are under a duty to disclose or share personal information in order to comply with our legal obligations. This includes exchanging information with organisations and law enforcement agencies for the purpose of:

6.2.1. Anti-money laundering obligations and sanction compliance, fraud and credit risk reduction;

6.2.2. Reporting to the relevant authorities information about the child and its family or others where we have grounds for suspecting that the child is at risk of significant harm;

6.2.3. CCTV images from equipment in place in and around our facilities for the purpose of prevention and detection of crime and public safety.

7 Retention and Security

7.1. We only retain your personal information for as long as is necessary for us to use your information as described above or to comply with our legal obligations.

7.2. We have a number of security measures in place to protect your personal information. We may store your information in printed or electronic format in our business units. The information is protected from unauthorised access, use modification or disclosure.

7.3. Disposal of personal information is conducted securely in accordance with approved methods, which in some circumstances that may de-identify the information priori to disposal.

7.1 Right to Erasure

7.1.1 To request the deletion of your personal data in connection with the UOW Pulse App, submit your request via email to pulse-corporate-support.uow.edu.au.

8 Access and Accuracy

8.1. We strive to ensure that the information we maintain is accurate, current and complete. We may periodically contact you to review and update the information that you have provided us to ensure our organisation can continue to provide the related products and services.

8.2. We respond to requests to access and correct inaccurate information in a timely manner. If you feel that your information that is held is incorrect, contact should be made with UOW Pulse via pulse-corporate-support@uow.edu.au

9 Reporting a Data Breach

9.1 An individual who becomes aware of a suspected or known Data Breach at UOW Pulse is to immediately notify:

(a) UOW Pulse CEO Office on +61 2 4221 8000 or at pulse-corporate-support@uow.edu.au

(b) For Staff, their appropriate Line Manager.

9.1 Examples of a Data Breach

9.1.1 A Data Breach includes:

- Unauthorised access by Staff or sharing of data between teams within UOW Pulse without relevant authority

Human error

- Letter or email sent to the wrong recipient.
- System access is incorrectly granted to someone without appropriate authorisation.
- Loss of a physical asset such as a paper record, laptop, USB stick or mobile phone containing data that is in the possession, control or the responsibility of UOW Pulse.
- Failure to implement appropriate security measures such as password protection or sharing password and log in information.

System failure

- A coding error allows access to a system without authentication, or results in automatically generated notices including incorrect information or being sent to incorrect recipients.
- Systems not maintained through the application of known and supported patches.

Malicious or criminal attack

- Cyber incidents such as ransomware, malware, hacking, phishing or brute force access attempts resulting access to or theft of data.
- Social engineering or impersonation leading into inappropriate disclosure of data.
- Insider threats from agency employees using their valid credentials to access or disclose data outside the scope of their duties or permission.
- Theft of physical asset such as a paper record, laptop, USB stick or mobile phone containing data that is in the possession, control or the responsibility of UOW Pulse.

9.2 Responding to a Data Breach

9.2.1 Where there are reasonable grounds to suspect that a Data Breach has occurred, UOW Pulse must:

(a) Take immediate steps to contain the breach or suspected breach to minimise the possible damage

(b) Report the breach to the CEO office who are authorised to receive and action a report of a suspected or known Data Breach;

(c) Carry out an assessment of the breach to determine what has occurred and whether an Eligible Data Breach has occurred, within 30 days;

(d) Make all reasonable attempts to mitigate any harm done by the suspected breach;

(e) Consider whether notification under legislation or other policies, procedures or agreements may be required. This may include notification to:

i. affected individuals;

ii. Privacy Commissioner;

iii. other regulatory bodies;

iv. third Parties with collaborative or contractual ties with the University; and

(f) Carry out post incident review and preventative efforts, based on the type and seriousness of the breach.

9.2.2 Where a Data Breach has been assessed as an Eligible Data Breach, UOW Pulse must:

(a) Notify the Privacy Commissioner immediately, using the form approved by the Privacy Commissioner; and

(b) Notify affected individuals as soon as practicable. UOW Pulse may elect to notify either:

i. all individuals regardless of their risk of harm; or

ii. only affected individuals (ie. those individuals who are likely to suffer Serious Harm as a result of the Data Breach that relates to them).

9.2.3 Each Data Breach should be assessed on a case by case basis and a response is to be determined, depending on the circumstances associated with the Data Breach.

9.2.4 UOW Pulse will comply with all relevant Statutory Guidelines issued by the NSW Information and Privacy Commission (IPC) under Part 6A of the PPIP Act.

9.3 Data Breach Response Team

9.3.1 The UOW Pulse CEO Office is responsible for receiving reports of a Data Breach, triaging, and leading the response as appropriate. Further responsibilities of the CEO Office are addressed at section 9.7 of this Policy.

9.3.2 Where required, the Data Breach Response Team (CEO Office) will be convened and will include key subject matter experts, depending on the nature and impact of the Data Breach. Key subject matter experts may include:

(a) Lead coordinator – UOW Pulse Senior Managers, UOW Pulse Senior Executives, the CEO Office or delegate, to lead the response. Where a suspected Eligible Data Breach has occurred, the Senior Manager or the CEO Office will carry out required actions as outlined at section 9.7 of this policy;

(b) General Counsel – responsible for reporting to UOW Pulse Senior Executives and the CEO Office, providing legal support and supporting team members. Where a suspected Eligible Data Breach has occurred, the General Counsel will carry out required actions as outlined at section 9.7 of this policy;

(c) Records and evidence support – maintain records of all actions taken by the Data Breach Response Team and providing administrative support;

(d) Technical support – a member of UOW Pulse IT to facilitate response and containment actions, assist with root cause analysis and provide forensic support, CEO office to involve UOW IMTS when and If relevant;

(e) Communication support – Senior Executives and the CEO Office to assist with communication to stakeholders and affected individuals, where relevant;

(f) Data Guardian – senior leadership with high-level knowledge, expertise and tactical decision making in data within their responsibility, where relevant;

(g) Data Specialist –business and technical subject matter experts who typically provide ongoing technical support as a part of their day-to-day role, where relevant;

(h) Other Staff, depending on the context of the breach.

9.3.3 The Data Breach Response Team will be convened in the event of a Data Breach, or suspected or potential Eligible Data Breach and will coordinate the response in accordance with the severity of the Data Breach.

9.4 Notification

9.4.1 UOW Pulse has 30 days from the date it becomes aware of a possible Data Breach to assess whether that Data Breach is an Eligible Data Breach. Whilst making this assessment, all reasonable attempts must be made to mitigate any harm already done.

9.4.2 In accordance with section 59M of the PPIP Act where an Eligible Data Breach has taken place (regardless of any applicable exemption) UOW Pulse must immediately notify the NSW Privacy Commissioner using the prescribed form IPC Mandatory Data Breach Reporting Form - Data breach notification to the Privacy Commissioner (nsw.gov.au).

9.4.3 Where a public notification is made on the UOW Pulse Public Notification Register, UOW Pulse will advise the Privacy Commissioner how to access the public notification on its website.

9.5 Public Notification

9.5.1 If UOW Pulse is unable to notify the individuals as described at 9.2.2 directly, it will publish a public data breach notification onto the UOW Pulse website and take all reasonable steps to publicise the notification through appropriate channels available to UOW Pulse.

The public data breach notification will provide details of:

a) the circumstances of the Data Breach, including a description of the breach and the type of Information impacted,

b) the actions UOW Pulse has taken or plans to take to control or mitigate the harm to individuals,

c) steps that an affected individual should consider taking in response to the Data Breach, and

d) how the individual may contact the University for any additional information.

9.5.2 The public notification will remain on UOW Pulse's Website for a period of at least 12 months.

9.6 Other Notification Considerations

9.6.1 In some cases, UOW Pulse may have reporting obligations under both the NSW MNDB Scheme as well as the Notifiable Data Breaches Scheme under the Privacy Act 1988 (Cth). For example, a Data Breach involving TFN numbers, where it is likely to result in Serious Harm, would be reportable to

both the Office of the Australian Information Commissioner and the NSW Information and Privacy Commission (IPC).

9.6.2 Depending on the circumstances of the Data Breach UOW Pulse will ensure that its reporting obligations, either by other laws or administrative arrangements is included as part of its Data Breach response actions. Examples of organisations that these arrangements may assist with may include:

- Australian Cyber Security Centre (ACSC)
- NSW Police Force
- Australian Federal Police
- Department of Health
- Foreign regulatory agencies
- Professional associations, regulatory bodies or insurers
- Financial service providers
- Any third party organisations or agencies whose data may be affected.

9.7 Roles and Responsibilities

9.7.1 The MNDB Scheme assigns various responsibilities to the head of an agency (the person responsible for the agency's day to day management). In accordance with section 59ZJ of the PPIP Act, the head of an agency may delegate the exercise of those responsibilities to relevant Staff.

9.7.2 The CEO, as UOW Pulse's head of an agency, has delegated the exercise of those responsibilities to relevant Staff as outlined in this policy and as below;

The COO (Chief Operating Officer) is responsible for:

(a) deciding whether a Data Breach is an Eligible Data Breach, or there are reasonable grounds to believe the Data Breach is an Eligible Data Breach;

(b) escalating Data Breach response actions to the CEO, as appropriate;

(c) making determinations regarding the application of any exemptions and approval of any extension periods, as outlined in the MNDB Scheme;

(d) where UOW Pulse is unable to notify, or it is not practicable to notify, any or all of the affected individuals, making a determination to publish a public notification via the UOW Pulse website

General Counsel is responsible for:

(a) conducting an assessment of whether the Data Breach is, or there is reasonable grounds to believe the Data Breach is an Eligible Data Breach, within 30 days after being made aware that a Data Breach has occurred;

(b) where an assessment confirms an Eligible Data Breach, escalating the assessment to The CEO.

(c) notifying the Privacy Commissioner immediately in the approved form , if the Data Breach is an Eligible Data Breach;

(d) notifying each individual to whom the Information the subject of the breach relates, or each affected individual;

(e) providing written notice to the Privacy Commissioner regarding the application of any exemptions, any extension periods, or how to access any public notifications made by UOW Pulse, as outlined in the MNDB Scheme;

(f) identifying whether other external notification is required ie law enforcement or other third parties;

(g) identifying legal obligations and providing advice, as required.

Senior Executive Team is responsible for:

(a) receiving Data Breach notifications and confirming preliminary assessment reports;

(b) assessing the containment and/or remediation measures already undertaken (if any) and taking further actions as required to mitigate any further compromise of the data;

(c) where a preliminary assessment confirms a suspected or known Eligible Data Breach, escalating the preliminary assessment to General Counsel;

(d) making a determination to convene the Data Breach Response Team, in consultation with General Counsel. Where a determination has been made to convene the Data Breach Response Team, the following actions at 6e-6h will be conducted by the Senior Manager, Information Compliance in the capacity of lead coordinator of the team;

(e) ensuring Data Breach response actions are conducted in accordance with this policy and the Data Breach Response Plan;

(f) ensuring that all response actions are recorded in the Data Breach Report form and retained in accordance with the Records Management Policy;

(g) ensuring any relevant evidence of the Data Breach is preserved and securely stored, as appropriate;

(h) conducting and leading the post-response assessment of UOW Pulse's response to the Data Breach;

(i) establishing, maintaining and recording Data Breaches through the Audit, Risk Management and Compliance Committee.

(j) managing any complaints received as a result of the Data Breach;

(k) reviewing, testing and updating this policy at least annually.

Senior Management Team is responsible for:

(a) receiving notifications of a suspected or known Data Breach and taking local immediate containment steps to prevent any further compromise of the data;
(b) conducting an initial assessment of the Data Breach, notifying the relevant Data Guardian and consulting with the Information Compliance Unit to determine appropriate response actions;
(c) completing the relevant sections in the Data Breach Report form at Appendix C;
(d) where a Data Breach can be/is being managed appropriately locally, ensuring that the completed Data Breach Report form is submitted to the Information Compliance Unit and retained in accordance with the Records Management Policy;
(e) participating in response actions, in accordance with this policy and associated incident management processes.

Line Managers are responsible for:

(a) receiving notifications of a suspected or known Data Breach and taking local immediate containment steps to prevent any further compromise of the data;
(b) conducting an initial assessment of the Data Breach, notifying the relevant Data Guardian and consulting with the Information Compliance Unit to determine appropriate response actions;
(c) completing the relevant sections in the Data Breach Report form at Appendix C;
(d) where a Data Breach can be/is being managed appropriately locally, ensuring that the completed Data Breach Report form is submitted to the Information Compliance Unit and retained in accordance with the Records Management Policy;
(e) participating in response actions, in accordance with this policy and associated incident management processes.

All Staff are responsible for:

(a) reporting any suspected or known Data Breaches immediately, as per section 9.2 of this policy;

(b) assisting in response actions in accordance with this policy and the Data Breach Response Plan.

9.8 Data Breach Response Team

CEO Office	
General	Email: pulse-corporate-support@uow.edu.au Phone: +61 2 4221 8000
CEO	Chief Executive Officer Email: Alfonso Maccioni (alf@uow.edu.au) Phone: +61 2 4221 8002
COO	Chief Operation Officer Email: wtony@uow.edu.au Phone: +61 2 4221 5662

10 Complaints and Enquiries

10.1. All privacy enquiries, comments or requests or complaints regarding the Privacy Policy and our management of your personal information are welcomed and should be addressed to the UOW Pulse email: uow-pulse@uow.edu.au.

11 Employee Confidentiality

11.1. All employees of UOW Pulse are required to follow this Policy and understand that during their employment that may obtain information that is of a confidential nature and that it must be kept confidential and that any breach of confidentiality may result in disciplinary action. All employees are required to acknowledge their responsibilities by signing a confidentiality declaration.

12 Roles and Responsibilities

12.1. UOW Pulse Management group is responsible for the overall compliance with our privacy and confidentiality obligations.

12.2. All line managers and members of the Management group are required to:

12.2.1. Implement this policy in their work area and ensure all team members are aware of their responsibilities in regards to the *Privacy Policy* and confidentiality;

12.2.2. Ensure that any potential/actual breach to the *Privacy Policy* is dealt with promptly;

12.2.3. Ensure all new starters read the *Privacy Policy* and sign the confidentiality declaration.

12.3. All employees have a responsibility to:

12.3.1. Comply with this policy;

12.3.2. Maintain confidentiality when managing information provided to, or collected by UOW Pulse and its business units;

12.3.3. Report any potential or actual breach of this policy to the line manager or the People & Culture team.

13 Version Control Table

Version Control	Date Released	Approved By	Amendment
1	2004	HR Manager	New policy created.
2	July 2011	Assistant General Manager	Migrated into new QA format.
3	December 2011	General Manager	Renamed Privacy/Confidentiality Policy. Increased references to privacy legislation.
4	March 2015	General Manager	Aligned with UOW Policy review.
5	February 2018	Head of People & Culture	Updated to reflect legislation.
6	June 2022	CEO	Updated to reflect further changes to the legislation.
7	December 2023	CEO	Significant additions to section 9 Data Breach to reflect the addition of Part 6A of the *NSW Privacy and Personal Information Protection Act 1988 (PPIP Act)* 7.1 added due to the implementation of the UOW Pulse App.