



## People & Culture Privacy Policy

---

<b>Date approved:</b>	March 2022	<b>Date Policy will take effect:</b>	March 2022	<b>Date of Next Review:</b>	March 2025
<b>Approved by:</b>	Chief Executive Officer				
<b>Custodian title:</b>	Head of People & Culture				
<b>Author:</b>	Head of People & Culture				
<b>Responsible Unit:</b>	People & Culture				
<b>Supporting documents, procedures &amp; forms of this policy:</b>	Not applicable				
<b>References &amp; Legislation:</b>	<a href="#"><i>Privacy Act 1998 (Cth)</i></a> <a href="#"><i>Australian Privacy Principles (APP)</i></a> <a href="#"><i>Health Records and Information Privacy Act 2022 (NSW) (HRIPA)</i></a> <a href="#"><i>Privacy and Personal Information Protection Act 1998 (NSW) (PPIPA) Public Interest Disclosure Act 1994 (NSW)</i></a> <i>UOW Pulse Code of Conduct</i>				
<b>Audience:</b>	Internal				
<b>Expiry Date of Policy (if applicable):</b>	Not Applicable				

## Contents

1	Introduction / Background .....	3
2	Scope .....	3
3	Definitions .....	3
4	Information you give us .....	4
5	How we use the information we collect .....	5
6	Information we share .....	5
7	Retention and Security .....	6
8	Access and Accuracy .....	6
9	Notifiable Data Breach .....	6
10	Complaints and Enquiries .....	6
11	Employee Confidentiality .....	6
12	Roles and Responsibilities .....	7
13	Version Control Table .....	7

## 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 facilitate UOW Pulse's 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.

## 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 Policy.
- 2.4. All UOW Pulse employees are bound by and must comply with the Privacy Policy.
- 2.5. A breach of this Privacy Policy would be considered very seriously by UOW Pulse and would be subject to investigation and possible disciplinary action.

## 3 Definitions

Word/Term	Definition
<b>Data Breach</b>	When personal information held by UOW Pulse is lost or subjected to unauthorised access, modification, disclosure, or other misuse or interference.
<b>Customer</b>	A member of the public who visits the campus and either purchases products or utilises the services or facilities of UOW Pulse.
<b>Eligible Data Breach</b>	An eligible data breach in which the following conditions are satisfied: <ol style="list-style-type: none"><li>i. The unauthorised access to, or unauthorised disclosure of personal information held, or a loss of personal information held by UOW Pulse; and</li><li>ii. This is likely to result in serious harm to one or more individuals; and</li><li>iii. UOW Pulse has not been able to prevent the likely risk of serious harm with remedial action.</li></ol>
<b>Health Information</b>	The Privacy Act defines 'health information' as follows: <ol style="list-style-type: none"><li>(a) Information or an opinion about:<ol style="list-style-type: none"><li>i. The health, including an illness, disability or injury (at any time) of an individual; or</li><li>ii. An individual's expressed wishes about the future provision of health services to the individual; or</li><li>iii. A health service provided, or to be provided, to an individual, that is also personal information; or</li></ol></li><li>(b) Other personal information collected to provide, or in providing, a health service to an individual.</li></ol>
<b>Information</b>	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.
<b>Line Manager</b>	An employee of UOW Pulse who acts in a supervisory or leadership capacity (whether acting or permanent) to other team members of UOW Pulse.
<b>Personal Information</b>	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:

	<ul style="list-style-type: none"> <li>• About an individual who has been deceased for more than 30 years;</li> <li>• Which is publicly available;</li> <li>• About an individual contained in a public interest disclosure under the <i>Public Interests Disclosure Act</i>; or</li> <li>• An opinion about an individuals sustainability for appointment or employment as a public sector official.</li> </ul>
<b>Primary purpose</b>	Means the main purpose for which the information was collected.
<b>Sensitive information</b>	Defined by the <i>Privacy Act</i> as a subset of Personal Information, which includes: <ul style="list-style-type: none"> <li>i. Information or an opinion about an individuals: <ul style="list-style-type: none"> <li>a. Race, racial or ethnic origin;</li> <li>b. Political opinions;</li> <li>c. Membership of a political association;</li> <li>d. Religious beliefs or affiliations;</li> <li>e. Philosophical beliefs;</li> <li>f. Membership of a professional or trade association;</li> <li>g. Membership of a trade union;</li> <li>h. Sexual preference or practices; or</li> <li>i. Criminal record</li> </ul> </li> <li>ii. Health information about an individual; or</li> <li>iii. Genetic information about an individual that is not otherwise Health Information</li> </ul>
<b>Serious harm</b>	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: <ul style="list-style-type: none"> <li>i. The kinds of information;</li> <li>ii. The sensitivity of the information;</li> <li>iii. Whether the information is protected by one or more security measures or technology;</li> <li>iv. The persons, or the kinds of persons, who have obtained or who could obtain the information;</li> <li>v. The likelihood of the person who has obtained the information causing harm to any individuals to whom the information relates;</li> <li>vi. The nature of the potential harm; and</li> <li>vii. Any other relevant matters.</li> </ul>
<b>Employee</b>	All persons employed by UOW Pulse of any seniority and including those in continuing, part-time, maximum term, casual, trainee or contract roles.
<b>Students</b>	A person registered for a course at the University of Wollongong.
<b>Use (of information)</b>	Means the communication or handling of information within UOW Pulse.
<b>Visitor</b>	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.

## **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 [uow-pulse@uow.edu.au](mailto:uow-pulse@uow.edu.au).

## **9 Notifiable Data Breach**

- 9.1. UOW Pulse is required to notify individuals and the Australian Privacy Commissioner where there has been an eligible data breach that has the potential to cause serious harm to the individuals, whose information is involved in the breach.
- 9.2. The following process would be implemented:
  - 9.2.1. Step 1: Contain the breach and make a preliminary assessment
    - 9.2.1.1. Take immediate steps to contain breach;
    - 9.2.1.2. Designate person/team to coordinate response;
  - 9.2.2. Step 2: Evaluate the risks for individuals associated with the breach
    - 9.2.2.1. Consider the personal information involved'
    - 9.2.2.2. Determine whether the context of the information is important;
    - 9.2.2.3. Establish the cause and extent of the breach;
    - 9.2.2.4. Identify what is the risk of harm;
  - 9.2.3. Step 3: Consider breach notification
    - 9.2.3.1. Risk analysis on a case-by-case basis;
    - 9.2.3.2. Not all breaches necessarily warrant notification;
  - 9.2.4. Step 4: Review the incident and take action to prevent future breaches
    - 9.2.4.1. Fully investigate the cause of the breach;
    - 9.2.4.2. Consider developing a prevention plan;
    - 9.2.4.3. Make appropriate changes to policies and procedures;
    - 9.2.4.4. Revise all staff training practices

## **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](mailto: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.