PRIVACY POLICY

Approved by:	Executive Director Legal and Governance	**Date:**	8 February 2018
Date Effective:	8 February 2018	**Date of Next Review:**	8 February 2021
Document No:	UOWE-LGL-POL-03	**Version:**	8
Custodian:	Executive Director Legal and Governance		
Supporting Documents, Procedures & Forms:	Cyber Security Policy (UOW) IT Server Security Policy (UOW) Privacy Management Plan and Procedure (UOWE) Privacy Management Procedure (UOWD) Records Management Policy (UOWD) Records Management Policy (UOWE) Server Security Policy (UOWD)		
References & Legislation:	Australian Privacy Principles (APP) *Government Information (Public Access) Act 2009* (NSW) (GIPA) *Health Records and Information Privacy Act 2002* (NSW) (HRIPA) *Independent Commission Against Corruption Act 1988* (NSW) Law No. (26) of 2015 Regulating Data Dissemination and Exchange in the Emirate of Dubai (United Arab Emirates) *Privacy and Personal Information Protection Act 1998* (NSW) (PPIPA) *Privacy Act 1988* (Cth) *Public Interest Disclosure Act 1994* (NSW) *State Records Act 1998* (NSW)		

UOW
ENTERPRISES

Contents

1 Purpose

1.1 The primary purpose of this Policy is to establish a privacy framework across the UOW Enterprises Group which:

i. Promotes the protection of the privacy of the individual;

ii. Promotes responsible and transparent handling of personal information;

iii. Facilitates the free flow of information across national borders; and

iv. Provides a means for individuals to complain about an alleged interference with their privacy.

1.2 This Policy evidences UOW Enterprises commitment to privacy and compliance with relevant Australian and UAE privacy laws.

2 Scope

2.1 This Policy applies to UOW Enterprises operations, staff and students at:

i. UOW College;

ii. UOW in Dubai; and

iii. UOW Enterprises Corporate Offices.

(*collectively*, UOW Enterprises)

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

2.3 This Policy applies to technological infrastructure managed by Information Management and Technology Services (IMTS) on behalf of UOW Enterprises.

2.4 This Policy should be read in conjunction with any and all obligations arising from UOW Enterprises Privacy Management Plan, and/or the UOWD Privacy Management Procedure.

2.5 This Policy does not apply to CCCU in Hong Kong, which maintains a separate privacy policy developed in line with relevant privacy ordinances in the Hong Kong SAR.

3 Definitions

Word/Term	Definition
Data Breach	Access to information will be considered a data breach where there is a loss of, unauthorised access to, or unauthorised disclosure of, information.
Eligible Data Breach	An eligible data breach is a data breach in which both of the following conditions are satisfied:

	i. There is unauthorised access to, or unauthorised disclosure of, the information; and ii. A reasonable person would conclude that the access or disclosure would be likely to result in serious harm to any of the individuals to whom the information relates. Loss of data in the following circumstances also constitutes an eligible data breach in the following circumstances: i. Unauthorised access to, or unauthorised disclosure of, the information is likely to occur; and ii. Assuming that unauthorised access to, or unauthorised disclosure of, the information was to occur, a reasonable person would conclude that the access or disclosure would be likely to result in serious harm to any of the individuals to whom the information relates; then iii. The loss is an eligible data breach and an individual covered is *at risk* from the eligible data breach.
Health Information	Defined in HRIPA to include information that is in the possession or control of UOW Enterprises which is: i. Personal information that is information or an opinion about; a) The physical or mental health or a disability (at any time) of an individual; or b) An individual's express wishes about the future provision of health services to them; c) A health service provided, or to be provided, to an individual. ii. Other personal information collected to provide, or in providing, a health service; and iii. Other personal information about an individual collected in connection with the donation, or intended donation, of an individual's body parts, organs or body substances; or iv. Other personal information that is generic information about an individual arising from a health service raided to the individual in a form that is or could be predictive of the health (at any time) of the individual or of any sibling, relative or descendant of the individual.
Information	Any health information, sensitive information and/or personal information that is collected by UOW Enterprises about a student or staff member in the course of its operations.
Misconduct	Academic misconduct and/or general misconduct under the relevant Student or Staff Conduct Policy.
Personal Information	Is defined by PPIPA and the Privacy Act to include:

	i. Information or an opinion about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion; ii. An individual's fingerprints, retina prints, body samples, or genetic characteristic. Personal information does not include information: • About an individual who has been dead for more than 30 years; • Which is publically available; • About an individual contained in a public interest disclosure under the *Public Interest Disclosure Act;* • An opinion about an individual's suitability for appointment or employment as a public sector official; or • Any information held in a library, museum, or gallery for the purpose of reference, study or exhibition.
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 individual's: 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	Whether an eligible data breach is likely to result in serious harm will be considered against the following: i. The kind or 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 of the individuals to whom the information relates; vi. The nature of the potential harm; and vii. Any other relevant matters.
Staff	Full-time, fixed term, part-time, sessional and casual employees of UOW Enterprises.

Students	Any person who is enrolled in any course or program offered at, or in conjunction with, the College or UOWD.
Use (of information)	Means the communication or handling of information within UOW Enterprises

4 Policy Principles

4.1 UOW Enterprises is committed to ensuring that privacy is protected and will take all reasonable steps to ensure that the collection, use, disclosure and handling of information by UOW Enterprises complies with all relevant laws.

5 Collection of Information

5.1 UOW Enterprises will collect information in an open manner, including informing individuals why the information is being collected and how it will be used.

5.2 UOW Enterprises will only collect information lawfully, and for a purpose that is directly relevant and reasonably necessary to carry out its operations.

5.3 UOW Enterprises will ensure that information collected is relevant, accurate and does not intrude to an unreasonable extent on the personal affairs of the individual.

5.4 UOW Enterprises will collect information directly from the individual to which it relates, unless:

i. The person has consented to information being collected on their behalf by someone else;
ii. The person is under 16 years of age; or
iii. It is unreasonable or impractical to do so.

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

i. The identity of UOW Enterprise and how to contact the organisation;
ii. The fact that individuals are able to obtain access to their information;
iii. The purpose for which that information is being held;
iv. The organisations (or type of organisation) to which UOW Enterprises may disclose information of that kind;
v. Any law(s) which require the information to be collected; and
vi. The main consequences for the individual if all or part of the information is not provided or is incorrect (if applicable).

5.6 UOW Enterprise will not collect sensitive information, including health information, unless:

i. The individual has consented;
ii. The collection is required by law;
iii. The collection is necessary to prevent or lessen a serious and imminent threat to life or health of an individual; of
iv. The collection is in relation to a legal claim.

6 Use and disclosure of information

6.1 UOW Enterprises will only use and disclose information for the primary purpose of collection unless use or disclosure for another purpose is lawfully permitted or required, or the person whose information is being disclosed has consented to the disclosure.

6.2 UOW Enterprises will only disclose information about an individual to third parties (including their related entities and/or government agencies) without an individual's consent in limited circumstances, including:

i. Where the information is directly related to the purpose for which it is collected and UOW Enterprises have no reason to believe that the person would object to its disclosure;
ii. The individual is reasonably likely to have been aware, or has been made aware, that information of that kind is usually disclosed to the third party and related entities;
iii. UOW Enterprises believes on reasonable grounds that the disclosure is necessary to prevent or lessen a serious and/or imminent threat to the life or health of the individual concerned or another person;
iv. Exchanging information for law enforcement purposes, or for the protection of public revenue; or
v. Disclosure is required by law.

7 Access, Accuracy and Amendment

7.1 UOW Enterprises takes all reasonable steps to ensure that the information it holds is complete and accurate.

7.2 A person can access their information and request the correction of information.

7.3 UOW Enterprises will respond to a request for access within a reasonable period.

7.4 UOW Enterprises will not deny access unless it would be unreasonable or impractical to fulfil the request.

7.5 Where access is denied, written reasons for the refusal must be provided to the individual.

7.6 Individuals have the right to appeal a refusal under the relevant grievance policy.

8 Retention and Security

8.1 UOW Enterprises takes all reasonable steps to ensure that information is:

i. Held for no longer than is necessary, subject to the *State Records Act 1998* (NSW);

ii. Disposed of securely in accordance with approved methods; and

iii. To the extent reasonable in the circumstances, information is protected from loss, unauthorised access, use, modification, disclosure or other misuse.

8.2 Staff should refer to UOW Enterprises Records Management Policy for information on the retention of information.

9 Transnational data flows

9.1 In the course of its operations, UOW Enterprises may be required to provide information to organisations outside of Australia.

9.2 For the purposes of this policy, this includes the transfer of information from UOW Enterprises in Australia to its international operations.

9.3 Where data is transferred overseas, UOW Enterprises will to the best of its ability:

i. Ensure that the recipients of information treat information in the same way as would be required under Australian law;

ii. Ensure UOW Enterprises offshore operations adhere to the Australian Privacy Principles; and

iii. Comply with local laws to discharge privacy obligations.

10 Notifiable Data breach

10.1 UOW Enterprises is required to notify individuals and the Australian Privacy Commissioner where a there has been an *eligible data breach* of data collected or stored by UOW Enterprises' which has the potential to cause *serious harm*.

10.2 Where UOW Enterprises staff, UOW IMTS or UOWD ITTS become aware of a suspected or actual data breach involving information collected or stored by UOW Enterprises, the UOW Enterprises Privacy Officer must be informed so that they can determine whether the data breach is a notifiable breach.

10.3 Where the Privacy Officer has determined a breach is a notifiable data breach, they must:

i. Prepare a statement complying with s 26WK of the *Privacy Act*;

ii. Notify the individuals to whom the breach relates; and

iii. Notify the Australian Privacy Commissioner.

within 20 days of initial notification of a suspected or actual breach.

10.4 Notification must occur in this manner wherever there is a notifiable data breach, including where a notifiable breach occurs at offshore operations. This reflects the extra-territorial operation of the *Privacy Act*.

11 Re-identification of government data

11.1 In the course of its Australian operations, UOW Enterprises may be supplied with de-identified data by government agencies.

11.2 Staff members must not perform an act with the intention of achieving the result that the information is no longer de-identified, or an act which results in the information no longer being de-identified.

11.3 Under no circumstances can UOW Enterprises disclose de-identified data supplied by a government agency to any person or entity other than the agency responsible for the data.

11.4 Should any staff member become aware that:

i. De-identified data has been re-identified; or

ii. De-identified or re-identified data supplied by a government agency has been disclosed to any individual or entity;

they must notify the Privacy Officer immediately.

11.5 Following this notification, the Privacy Officer is to take all reasonable steps to notify the agency responsible that de-identified information has been re-identified.

11.6 Serious penalties apply where the provisions of this clause are contravened.

12 Privacy Complaints

12.1 The Privacy Management Plan and Procedure set out the process for onshore UOWE and UOW College staff and student to making and handling complaints relating to alleged breaches of privacy.

12.2 The UOWD Privacy Management Procedure provides the process for making complaints related to alleged breaches of privacy for staff and students at UOWD.

13 Roles and Responsibilities

Executive Responsibility

13.1 The Executive Director, Legal and Governance is the Primary Privacy Officer and is responsible for UOW Enterprises' overall compliance with its privacy obligations.

13.2 Operational responsibility for compliance for UOW College vests with the UOW College General Manager.

13.3 Operational responsibility for compliance for UOWD vests with the Director, Student Services and Academic Registrar.

Legal and Governance Division

13.4 UOW Enterprises Legal and Governance Staff are responsible for:

i. Providing privacy advice and education to UOW Enterprises Staff;

ii. Where delegated by the Principle Privacy Officer, respond to enquiries or complaints from individuals on privacy matters;

iii. Manage any required external privacy obligations.

Human Resources Division

13.5 UOW Enterprises Human Resources staff will provide information about staff member's privacy obligations during their induction.

UOW IMTS and UOWD ITTS

11.1 Ensure that UOW Enterprise data is protected and maintained in accordance with industry best practice.

11.2 Report any suspected or actual data breach to the UOW Enterprises' Privacy Officer in a timely manner; and

11.3 Provide all relevant and necessary support as required to manage the data breach.

All UOW Enterprises Staff

11.4 All UOW Enterprises staff are responsible for complying with privacy obligations outlined in this Policy, the supporting procedures, and the UOW Enterprises/UOWD Code of Conduct when managing information provided to, or collected by UOW Enterprises.

12 Version Control and Change History

Version Control	Date Effective	Approved by	Amendment
1	02/05/11	Vince Lendrum	New Policy
2	08/06/11	ITC Quality Manager	Address in section 11 updated
3	19/12/11	ITC Quality Manager	Purpose updated to include IFSS

4	10/3/14	Director Legal and Governance	Changes to company branding and legislative obligations confirmed.
5	17/08/2015	Policy Officer	Correction of Privacy Officer email details. (from itc.privacy@uow.edu.au to itc-privacy@uow.edu.au)
6	21/07/2016	Compliance Officer	Minor change only – College branding, position title and document formatting updated.
7	11/04/2017	Vanessa Bourne, Executive Director Legal and Governance	Policy refresh in line with legislative changes to privacy laws.
8	08/02/2018	Vanessa Bourne, Executive Director Legal and Governance	Amendments to ensure the Policy catered for UOWD operational environment.