

# Information Privacy Policy



**Policy Number** UP14/10

**Approval Date** 08 December 2023

**Assessment Date** 08 December 2024

**Approver** Senate

**Steward** Vice-Chancellor

**Custodian(s)** Director Governance and General Counsel

**Administrator(s)** Manager Information Governance

**TRIM File** F57176

## 1 Purpose

- (1). The purpose of this **Policy** is to —
- (2). protect the University Community from the misuse of Personal Information and Sensitive Information;
- (3). provide alignment with the Australian Privacy Principles; and
- (4). contribute to upholding the rights of members of the University Community to fair treatment.

(B). In this Policy —

1	Purpose.....	1
2	Scope .....	2
2.1	Institutional Scope.....	2
2.2	Individual Scope .....	2
3	Personal Information .....	2
4	Collection and Use of Personal Information.....	3
5	Disclosure of Personal Information .....	4
6	Management of Personal Information .....	4

University of Western Australia  
[uwa.edu.au/policy](http://uwa.edu.au/policy)

This is a UWA official document authorised or intended for public access.

7	Access and Correction of Personal Information .....	5
8	Privacy Collection Notice .....	5
9	Website Privacy .....	5
10	General Data Protection Regulations (GDPR) .....	6
11	UWA Privacy Office .....	6
12	Personal Information Requests and Complaints .....	6

- (C). This Policy is to be read in conjunction with the following —
- (1). Information Privacy Guide - Policy Guideline; and
  - (2). Privacy Collection Notices.

## 2 Scope

### 2.1 Institutional Scope

- (A). The scope of this Policy applies to the entire **University**.

### 2.2 Individual Scope

- (A). The scope of this Policy applies to all **Employees** when collecting, holding, accessing, utilising and correcting Personal Information and Sensitive Information on behalf of the University.
- (B). **Contractors**, consultants and agents of the University may also be required under the terms of their agreement with the University to comply with this Policy, and/or the terms of the Australian Privacy Principles in collecting, holding, using or disclosing Personal Information on behalf of the University.

## 3 Personal Information

- (A). Personal Information means information or an opinion about an identified, or an individual who is reasonably identifiable, whether true or not and whether recorded in a material form or not.
- (B). Sensitive Information means information or an opinion about an individual's racial or ethnic origin, political opinion, religious beliefs, association memberships, sexual orientation, criminal record or health, genetic or biometric information that is also Personal Information.
- (C). The University will list the types of Personal Information and Sensitive Information in the Information Privacy Guide - Policy Guideline.

University of Western Australia  
[uwa.edu.au/policy](http://uwa.edu.au/policy)

This is a UWA official document authorised or intended for public access.

- (D). The University will collect and hold different types of Personal Information and Sensitive Information depending on the circumstance and relationship between the University and an individual.

## 4 Collection and Use of Personal Information

- (A). The University will collect and use Personal Information where that information is reasonably necessary for the performance of one or more functions and/or activities as a provider of education and research and as an employer.
- (B). The University will collect and use Personal Information by lawful, fair and transparent means and, where possible, directly from the individual.
- (C). The University will collect Personal Information that is adequate, relevant and limited to what is required for University purposes.
- (D). The University may collect Personal Information in a number of ways, including but not limited to —
- (1). enrolment, registration or subscription process;
  - (2). direct contact in the course of providing services or administration of **University Activity** and/or **University Business**;
  - (3). forms that are submitted by individuals (including via online portals);
  - (4). from CCTV cameras on **University Property**;
  - (5). from cookies set from web browsers visiting the University's websites;
  - (6). from Google applications including AdWords;
  - (7). from public health databases where the relevant consent processes described in the national research and ethics codes are reviewed and approved;
  - (8). from an individual's usage of University's **IT Assets** and **IT Services**;
  - (9). from third parties with which the University collaborates; and
  - (10). when undertaking research.
- (E). The University will not collect Sensitive Information unless —
- (1). it has obtained the individual's consent;
  - (2). an exemption exists under, or it is required or authorised by Australian law or court/tribunal order.
- (F). The University will only collect and use an individual's Personal Information or Sensitive Information —

- (1). for the purpose for which it was collected (the primary purpose);
  - (2). for a secondary purpose that is related to the primary purpose (if the information is sensitive information, it will only be used or disclosed for a secondary purpose which is directly related to the primary purpose) and that the individual would reasonably expect his or her information to be used or disclosed for this secondary purpose;
  - (3). with the individual's consent; or
  - (4). as otherwise allowed, required or authorised by law.
- (G). The University may amalgamate, consolidate and aggregate Personal Information with other **University Information** and will, where appropriate, ensure such information is anonymised.

## 5 Disclosure of Personal Information

- (A). The University may disclose Personal Information to the following types of recipients —
- (1). Internal functions within the University beyond that which collected the information where this is in accordance with section 4 of this Policy;
  - (2). collaborating parties, to the extent that such personal information is required for the collaborative activity to be undertaken (e.g. collaborative research; jointly delivered courses or programs);
  - (3). an individual's home or host institution, or sponsor overseas, or their international agent, where that individual is involved in an exchange, mobility, study abroad program or joint program with an institution overseas, or where an individual is sponsored by or transfers to another institution overseas;
  - (4). external service providers, which may be located overseas, to the extent that the information is required to provide services to the University (e.g. software-as-a-service, cloud providers, website hosts);
  - (5). government departments and agencies to satisfy reporting requirements;
  - (6). a nominated emergency contact, emergency services or other person necessary to respond in the case of an emergency; and
  - (7). to law enforcement agencies to provide information for law enforcement purposes where required or authorised by law.

## 6 Management of Personal Information

- (A). The University will manage Personal Information by appropriate and reasonable means, ensuring a proactive approach to protecting such information from invasive events, embedding privacy into design of processes and systems and establishing accountabilities and responsibilities for Personal Information.
- (B). **Information Stewards** must ensure reasonable steps are taken in regards to University

Information, whether electronic or physical, to comply with this Policy.

- (C). **Information Custodians** will be responsible for implementing and monitoring all reasonable steps that the University may take to manage University Information in accordance with this Policy.
- (D). **Information Users** must ensure their collection, use, disclosure and correction of Personal Information is in accordance with this Policy.

## 7 Access and Correction of Personal Information

- (A). The University must, upon request by an individual, provide access to, or correction of, Personal Information we hold about that individual, unless providing that individual with access would have an unreasonable impact on the privacy of others or would contravene the University's other legislative obligations.
- (B). The University must take all reasonable measures to amend or remove Personal Information if it can be proved that having regard to the purpose for which the information is held, the information is inaccurate, out of date, incomplete or misleading.

## 8 Privacy Collection Notice

- (A). The University will, where it collects Personal Information, provide a privacy collection notice or reference to where the notice can be accessed, to inform the individual of the intended use of their Personal Information.
- (B). A privacy collection notice is a practical summary of the personal data being collected, its purpose, how it may be used or disclosed and the individual rights relating to the data.
- (C). UWA privacy collection notices can be accessed through the Information Privacy Policy Guideline.

## 9 Website Privacy

- (A). The University collects logs relating to activity on its websites which record limited information relating to visitors' details and activities. These logs will be managed in accordance with this Policy and the University's' record keeping obligations.
- (B). The University's websites also utilise digital cookies on its websites which may be used to provide personalised experiences and re-targeted advertising as explained in the Information Privacy Policy Guideline.

## 10 General Data Protection Regulations (GDPR)

- (A). The University must, in addition to all other sections of this Policy, ensure that in limited circumstances personal information it holds may permit an individual to —
- (1). withdraw their consent at any time in accordance with the Privacy Policy Guideline; and
  - (2). exercise the right to erasure, data portability and the right to object.

## 11 UWA Privacy Office

- (A). The University Privacy office provide assurance over the University's management of personal information and compliance reporting to the University's Audit and Risk committee.
- (B). The UWA Privacy office undertakes the responsibilities as outlined in the Information Privacy Policy Guidelines including -
- (1). University's Information Privacy policy, Guideline and other controls; and
  - (2). Managing privacy requests, complaints and enquires as below; and
  - (3). Investigating breaches of this Policy.
- (C). The UWA Privacy office's decisions in relation to requests and complaints as below are subject to an appeals process as operated by the UWA Integrity and Standards Unit.

## 12 Personal Information Requests and Complaints

- (A). An individual may contact the University to lodge a Privacy Request or complaint using the UWA Privacy Office using the contact details set out in the Information Privacy Policy Guidelines where they —
- (1). seek to access or correct their Personal Information; or
  - (2). seeking to exercise their rights under the GDPR; or
  - (3). believe that the University has breached this Policy in its collection, use or management of personal information; or
  - (4). suspect there has been a data breach.

# Breach of Policy

- (A). The University will investigate all suspected breaches of this Policy.

University of Western Australia  
[uwa.edu.au/policy](http://uwa.edu.au/policy)

This is a UWA official document authorised or intended for public access.

- (B). The University will, where such an investigation indicates the potential or actual unauthorised access to, disclosure of, or loss of personal information, assess whether —
- (1). the breach is an eligible data breach; and
  - (2). the types of notifications required.
- (C). An eligible data breach is any unauthorised access, disclosure of or loss of personal data which requires mandatory data breach notification under an applicable law.
- (D). Where the breach is categorised as an eligible data breach the University will notify —
- (1). the Office of the Australian Information Commissioner or other statutory authority; and/or
  - (2). an affected individual
- (E). Failure to comply with this Policy may result in disciplinary action.

## Definitions

**Affiliates** means incorporated or unincorporated bodies, that are legally recognised as outside the control of Senate but are under the influence of University Employees and/or predominately employ University Employees via a University Enterprise or common law employment contract.

**Contractor** means any individual (excluding Employees) or an organisation working under contract with the University.

**Employee** means an individual employed by the University under a —

- University of Western Australia Academic Employees Agreement;
- University of Western Australia Professional and General Employees Agreement; or
- common law employment agreement.

**Information Custodian** means an Employee who is a subject matter expert for a specific type of University Information and is responsible for implementing and monitoring all reasonable steps the University may take to manage that University Information.

**Information Steward** means a senior Employee with accountabilities for University Information and for ensuring reasonable steps are taken in regards to that University Information, whether electronic or physical Information Custodian.

**Information User** means a member of the University Community that creates, captures, receives or uses University Information.

**IT Asset** means any tangible or intangible thing, belonging to, or contracted to the University or members of the University Community, which is worth protecting and used to access, process, store or transmit data.

**IT Services** means the combination of processes, expertise and resources by which Uni IT deliver value to the University Community to enable the achievement of their business objectives.

**Personal Information** is defined in section 2 and the Information Privacy Guide - Policy Guideline

**Policy** means the formal and binding expression of behaviours or practices, expected by the University and University Community, on specific Policy Factors as published on the University Policy Library.

**Policy Factor** means a group of behaviours or practices expressed within a Policy that are unique to that Policy.

**Sensitive Information** is defined in section 2 and the Information Privacy Guide - Policy Guideline

**University** is defined Part 1 section 2 of the University of Western Australia 1911 (WA) and does not include **Affiliates**.

**University Activity** means engaging in study, work, recreation or other activities and services and performance of official duties for the University regardless of the location.

**University Business** means any work or official duties on behalf of a Business Unit.

**University Community** means all individuals who engage in University Activity and/or use University Property.

**University Information** means all data, records and information created, captured, processed, stored, shared and/or disposed of, by the University Community or on behalf of the University, in any format or medium.

**University Property** means tangible and non-tangible things, belonging to, or contracted to the University or members of the University Community, including campuses, facilities and service.

# End