



Privacy policy

Section 1 - Preamble

(1) This Policy is effective from 31 May 2022.

Section 2 - Purpose

(2) This Policy outlines the University's obligations for and commitment to the responsible management of personal information held about its staff, students, and individuals with whom it interacts.

Section 3 - Scope

(3) This Policy applies to all collection, use, disclosure, storage and destruction of Personal or Health Information by the University and also includes procedures addressing unauthorised access, modification or loss of personal information.

Section 4 - Policy

Statement of commitment

(4) The University is committed to the responsible management of Personal and Health Information. This commitment arises not only from a wish to comply with its legal obligations but also in recognition of and commitment to information privacy as one of the foundations of human dignity.

(5) In undertaking its core functions of teaching and research and in conducting the activities which support these functions, the University will balance the public interest in the free flow of information with the protection of the privacy of Personal and Health Information that the University collects.

Obligation

(6) All University staff, honorary staff and associates of the University must in performing the duties of their employment, appointment or engagement by the University:

- a. respect the privacy of Personal and Health Information that they collect, use or disclose; and
- b. comply with the requirements of all applicable personal data protection laws, this policy and its related procedures.

(7) The University complies with

- a. the [Privacy and Data Protection Act 2014](#) (Vic), the [Health Records Act 2001](#) (Vic),
- b. the [Privacy Act 1988](#) (Cth), where required by contract or legislation; and
- c. the General Data Protection Regulation (Regulation (EU) 2016/679 of the European Parliament and of the

Council of 27 April 2016) (GDPR), where the University processes personal information of an individual located in the European Economic Area.

The Privacy Officer

(8) The Privacy Officer or nominee will:

- a. provide advice on issues related to information privacy
- b. develop information privacy resources for use throughout the University
- c. receive enquiries about Personal and Health Information privacy at the University
- d. assess requests to exercise data subject rights from residents in the European Economic Area/United Kingdom
- e. assist University staff in responding to privacy breaches, monitor breach investigations and provide privacy breach reports in accordance with the [Privacy Breach Management procedure](#)
- f. advise on and monitor completion of privacy impact assessments in accordance with the [Privacy Impact Assessment procedure](#)
- g. liaise with the Office of the Victorian Privacy and Data Protection Commissioner, the Victorian Health Services Commissioner, the Australian Information Privacy Commissioner, and with a Data Protection Authority appointed under the General Data Protection Regulation where required
- h. establish and maintain a publicly accessible resource containing a privacy policy, privacy statements applicable to University staff, students and stakeholders, and information relevant to privacy at the University.

(9) General Counsel is the University's:

- a. Privacy Officer and
- b. Data Protection Officer for the purposes of the General Data Protection Regulation.

Collection

(10) Personal and Health Information must be collected only:

- a. where necessary and relevant to the University's functions and activities and where there is a specific and immediate need to do so
- b. in a lawful, fair and not unreasonably intrusive way.

(11) Sensitive information must only be collected where the individual has provided consent, or where the collection:

- a. is required by law
- b. is otherwise authorised under the [Privacy and Data Protection Act 2014 \(Vic\)](#) or the [Health Records Act 2001 \(Vic\)](#).

(12) When collecting Personal and Health Information directly from an individual, whether by verbal, written or electronic means, all reasonable steps must be taken to ensure that the individual providing such information is made aware of how their information will be used and with whom it might be shared or communicated in an appropriate collection statement.

(13) The Privacy Officer or nominee will develop and maintain a series of collection statements to inform individuals of the ways in which the University uses and discloses, and may reasonably anticipate the University to use or disclose, their Personal or Health Information.

(14) The collection statement must include:

- a. the purpose for which the information is being collected (the proposed use) and to whom it might be disclosed
- b. the area collecting the information and how to contact it
- c. that the individual is able to gain access to the information
- d. any law that requires the particular information to be collected
- e. the main consequence (if any) for the individual if all or part of the information is not provided to the University.

(15) University websites, forms, and publications that collect Personal or Health Information must include a collection statement, which must be prepared using a template approved by the Privacy Officer.

(16) Personal or Health Information must not be collected from individuals if it is reasonable and practicable to transact with them without collecting this type of information.

Use and disclosure

(17) Personal and Health Information collected in the course of the University's activities must be used only for the primary purpose of collection, a related secondary use reasonably anticipated by the individual, where an individual has consented, or where authorised by law.

(18) University staff and associates must only access Personal or Health Information to the extent necessary to perform their job.

(19) University staff must seek advice from the Privacy Officer prior to any use or disclosure that is not for the primary purpose of collection or a related secondary use that would be reasonably anticipated by the individual.

(20) University staff must refer all requests that require disclosure by law to the Privacy Officer.

(21) The reference in the Victorian privacy law to personal information being 'recorded in any form' does not diminish the obligation of University staff and associates to hold in confidence all information of a personal nature obtained in any manner, including verbally, in the course of their employment, appointment or engagement.

(22) University staff and associates must take reasonable steps to ensure that Personal and Health Information collected, used or disclosed is accurate, complete and up to date.

Data security and disposal

(23) University staff and associates must ensure that Personal and Health Information for which they are responsible is:

- a. kept secure and protected from unauthorised use, access, disclosure, modification or loss, whether deliberate or inadvertent; and
- b. subject to the University's obligations under the [Public Records Act 1973 \(Vic\)](#) and other legislation, destroyed or permanently de-identified when it is no longer needed by the University.

(24) An individual has the right to complain to the Privacy Officer about the unauthorised use, access, disclosure, modification or loss of their personal information by the University, whether deliberate or inadvertent. A complaint will be managed in accordance with the provisions of the [Privacy Breach Management procedure](#).

Access and correction

(25) An individual has the right to request that the University provide them with access to, or an opportunity to correct, their Personal or Health Information held by the University. Requests for access and correction will be managed in accordance with the provisions of the [Freedom of Information Act 1982 \(Vic\)](#).

(26) Operational areas of the University may, where appropriate, develop guidelines to enable staff, students and members of the public to access Personal or Health Information held about them by the University.

Data Subject Rights of European Economic Area/United Kingdom Residents

(27) In addition to the rights of access and correction above and subject to any conditions and exemptions in the GDPR, the University will respect the rights of residents of the European Economic Area and the United Kingdom to:

- a. object to processing of their personal information;
- b. request suspension of processing of their personal information
- c. transfer their personal information held in electronic form to them or a third party in a structured, commonly-used, machine-readable form;
- d. withdraw their consent to processing where Deakin's right to process is based only on their consent.

Contracts

(28) It is the responsibility of a contract sponsor to ensure that a contract entered into by the University includes appropriate safeguards for protection of Personal and Health Information. Advice from the Privacy Officer must be sought where Personal or Health Information is to be transferred outside of Australia.

Complaints

(29) An individual who believes that the University has engaged in an act constituting an interference with their privacy may make a privacy complaint to the University in accordance with subclauses a-d.

- a. complaints must be made within six (6) months of the time the complainant first became aware of the alleged breach
- b. where the complainant is a student of the University, any complaint will be dealt with under the [Student Complaints Resolution policy](#)
- c. where the complainant is a staff member of the University, any complaint will be dealt with under clause 60 of the [Deakin University Enterprise Agreement 2023](#)
- d. where the complainant is neither a currently-enrolled student nor a current staff member, complaints must be forwarded in writing to the Privacy Officer (via email privacy@deakin.edu.au). The Privacy Officer will be responsible for:
 - i. appointing an appropriate person to undertake an investigation of the complaint and to provide recommendations to the Privacy Officer as to an appropriate response;
 - ii. determining what actions the University will take;
 - iii. providing a written response in respect of the outcome to the complainant, and
 - iv. advising relevant University personnel of actions required to remedy the interference with the complainant's privacy (if any).

Training

(30) All University staff must undertake privacy training at induction and refresher training at least every two years unless the Privacy Officer or nominee is satisfied that the nature of their work at the University is such that additional privacy training is not required (eg lecturer in privacy law, solicitor employed by the Office of General Counsel). Faculties and Portfolios of the University are responsible for monitoring initial and refresher training of their staff.

Section 5 - Procedure

(31) The following procedures document how to comply with this Policy:

- a. [Privacy Breach Management procedure](#)
- b. [Privacy Impact Assessment procedure](#)
- c. [Surveillance and Location Tracking procedure](#).

Section 6 - Definitions

(32) For the purpose of this Policy:

- a. associates: contractors, consultants, volunteers, visiting appointees and visitors to the University.
- b. collection: includes any means by which the University obtains Personal or Health Information, including information that is volunteered, incidentally obtained or gathered from another organisation.
- c. collection statement: a statement of the University's practices when collecting, using, disclosing and otherwise managing Personal and Health Information collected in the course of its activities, which is provided at or near the time such information is collected. A collection statement may also be referred to as a privacy statement.
- d. health information: as defined in the [Health Records Act 2001 \(Vic\)](#),
 - i. information or an opinion about:
 - the physical, mental or psychological health (at any time) of an individual; or
 - a disability (at any time) of an individual; or
 - an individual's expressed wishes about the future provision of health services to him or her; or
 - a health service provided, or to be provided, to an individual - that is also personal information; or
 - ii. other personal information collected to provide, or in providing, a health service; or
 - iii. other personal information about an individual collected in connection with the donation, or intended donation, by the individual of their body parts, organs or body substances; or
 - iv. other personal information that is genetic information about an individual in a form that is or could be predictive of the health (at any time) of the individual or of any of their descendants.
- e. honorary staff: includes Honorary Professors, Honorary Associate Professors, Adjunct Professors, Adjunct Associate Professors, Honorary Fellows, Affiliate academics, Conjoint Clinical Professors and Conjoint Clinical Associate Professors.
- f. personal information: as defined in the [Privacy and Data Protection Act 2014 \(Vic\)](#) is information or an opinion (including information or an opinion forming part of a database), that is recorded in any form and whether true or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion, but does not include health information.
- g. privacy complaint: a complaint by an individual about an act or practice of the University in relation to the individual's Personal or Health Information that the individual believes is contrary to or inconsistent with the Information Privacy Principles set out in the [Privacy and Data Protection Act 2014 \(Vic\)](#) or the Health Privacy Principles set out in the [Health Records Act 2001 \(Vic\)](#).
- h. Privacy Officer: the person delegated with the responsibilities set out in clause 8 and is currently the General Counsel or nominee.
- i. sensitive information: a subset of Personal Information that constitutes information or an opinion about an individual's racial or ethnic origin; political opinions; membership of a political association; religious beliefs or affiliations; philosophical beliefs; membership of a professional or trade association; membership of a trade union; sexual orientation; or criminal record.

- j. staff: as defined in section 3, [Deakin University Act 2009 \(Vic\)](#): any person employed by the University.
- k. student: as defined in section 3, [Deakin University Act 2009 \(Vic\)](#)

Status and Details

Status	Current
Effective Date	31st May 2022
Review Date	31st May 2027
Approval Authority	Council Secretary
Approval Date	31st May 2022
Expiry Date	To Be Advised
Responsible Executive	Kerrie Parker Deputy Vice-Chancellor, University Services dvc-us@deakin.edu.au
Implementation Officer	Shirley Rooney General Counsel +61 3 52278560
Enquiries Contact	Office of General Counsel +61 3 52278533