PRIVACY POLICY

Current version in effect from:	20 Jun 2019
Approved by Council:	25 Nov 2015
Revised by Council:	19 Jun 2019

Related Documents

Freedom of Information Act 1982 (Vic)

Health Records Act 2001 (Vic)

Privacy Act 1988 (Cth)

Privacy and Data Protection Act 2014 (Vic)

1. Scope

1.1 This Policy covers all members of the University and all personal data handled by the University.

2. Objectives

2.1 This Policy assures compliance with relevant privacy legislation and establishes principles of transparency and fairness for the management of personal information at the University of Divinity.

2.2 This Policy guides University staff in the responsible collection, handling, use, disclosure and storage of personal information.

2.3 This Policy informs individuals of their right to access information that the University holds about them and how errors in that information may be corrected.

3. Definitions

3.1 **Personal information**: Information or an opinion (including information or an opinion forming part of a database), whether true or not, that is recorded in a material form, about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion, but does not include health information.

3.2 **Health information**: In the University context health information is 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.

3.3 **Sensitive information:** Information or 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 preferences or practices, or criminal record that is also personal information.

3.4 **Primary Purpose**: The purpose for which the information is collected. This covers the primary use and primary disclosure of the information. This must be only what is necessary to discharge the function or undertake the activity.

3.5 **Secondary Purpose**: Another purpose for which the information is used or disclosed and must relate to the primary purpose for which it was collected. If sensitive information is involved, the secondary purpose has to be directly related to the primary purpose.

4. Principles

4.1 The University respects individuals' privacy and is open and transparent about how it handles all personal and health information provided by staff, including casual staff and contractors, students and members of the public.

4.2 The University collects, uses, discloses and manages personal and health information in accordance with the relevant legislation above.

4.3 The University collects and uses sensitive information only in accordance with the law.

4.4 The University assigns and uses student and staff identification numbers only where necessary to facilitate efficient management of its business.

5. Collection of Information

5.1 The University collects personal and health information only where necessary for its functions or activities, including where government requires the information for statistical analysis and reporting purposes.

6. Use and Disclosure of Information

6.1 The University must not use or disclose personal information about an individual for a purpose other than the primary purpose of collection without the consent of that individual, unless the secondary purpose is related to the primary purpose and a person would reasonably expect such disclosure.

7. Retention of Information

7.1 Information must be retained only for as long as it is needed and then deleted, de-identified or destroyed, whichever is applicable.

8. Management

8.1 The University must take reasonable steps to inform a person of what personal information it holds and how it collects, handles, uses and discloses that information. To this end, this Policy and related information must be published on the University's website.

8.2 Individuals may seek to access or make corrections to their personal information held by the University.

8.3 The University must provide training in this Policy to relevant staff.

8.4 The University must take appropriate measures to ensure its information technology systems and information held on such systems are suitably protected against risk of security breaches.

9. Responsible Officer

9.1 The Vice-Chancellor is responsible for the development, compliance monitoring and review of this Policy and any associated procedures, and for the promulgation and implementation of this Policy in accordance with its scope. Enquiries concerning interpretation of this Policy should be directed to the Vice-Chancellor.

9.2 The Vice-Chancellor is responsible for compliance with this Policy by the staff within the Office of the Vice-Chancellor.

9.2 College Principals are responsible for compliance with this Policy by the staff within their respective Colleges.

10. Procedures

10.1 The Vice-Chancellor may approve procedures to give effect to this Policy.

11. Review Date

11.1 This Policy is to be reviewed no later than 31 December 2022.