THE UNIVERSITY OF NOTRE DAME AUSTRALIA

Policy:

Privacy

Effective: 5 August 2019

Audience: Students and Staff

Policy Category: Management
Policy Sub-category: Information Management and Privacy

Key words:	Privacy, Information Management
Policy Owner:	Deputy Vice Chancellor, Corporate
Responsible Officer:	General Counsel
Review Date:	5 August 2022

Contents

1 OBJECTS OF THE UNIVERSITY

The University's Objects are defined in Section 5 of its Act of Parliament:

In pursuing these Objects, the University seeks to be an outstanding Australian university, and one of the best Catholic universities in the world.

The Objects of the University are:

(a) the provision of university education, within a context of Catholic faith and values; and
(b) the provision of an excellent standard of -
    i. teaching, scholarship and research;
    ii. training for the professions; and
    iii. pastoral care for its students.

2 PURPOSE

Purpose

2.1 The *Privacy Policy* **(Policy)** outlines the policy on the collection, use, storage and disclosure of personal information at the University of Notre Dame Australia **(University)**.

2.2 As a provider of tertiary education and related services, and as an employer, the University is required to collect, use and disclose personal information. Personal information means information or an opinion, whether true or not and whether recorded in a material form or not, about an individual.

2.3 The purpose of this Policy is to provide information on the following:

2.3.1 The kind of personal information collected by the University;

2.3.2 The way in which personal information is collected and held;

2.3.3 The purposes for which personal information is collected, held, used and disclosed;

2.3.4 How an individual may access their personal information and request any correction in the information;

2.3.5 How an individual may make a complaint relating to the handling of personal information or a potential breach of the APPs and the process that will be adopted in handling a complaint;

2.3.6 Whether the University is likely to disclose personal information to overseas recipients and if so, the countries the recipients are likely to be located.

Privacy – Legal Requirements

2.4 The University is committed to protecting the privacy of personal information. The University is required to comply with a number of privacy laws including the Australian Privacy Principles (**APPs**) contained in the *Privacy Act 1988 (Cth)* (**Privacy Act**). The APPs regulate the manner in which personal information is handled by the University.

3 SCOPE

3.1 This Policy applies to students enrolled at the University, staff members employed by the University, and contractors.

4 PRINCIPLES

INFORMATION RELATING TO PRIVACY

4.1 Personal Information

4.1.1 Personal information collected by the University will depend on an individual's dealing with the University.

4.1.2 For students, personal information provided to the University will be information required by the University in order for the University to provide tertiary education and any related services. Personal information will only be used for the administrative or educational purposes of the University or in accordance with specific consent. Personal information will include information to enable the University to identify a student and communicate with a student in a legitimate and lawful way. The University will also collect information relating to a student's educational background, qualifications, academic results, banking and payment details, tax file numbers and Commonwealth Higher Education Student Support Number (**CHESSN**).

4.1.3 For employees of the University or a contractor, the University may collect personal information relating to identity, employment history and qualifications, business and any other information that may be legitimately requested to facilitate employment or engagement.

4.1.4 Sensitive information is a type of personal information which includes personal information relating to health information, racial or ethnic origin, criminal records, religious affiliation and political opinion. Sensitive information will only be collected when it is required by law (including collection on behalf of the Australian Government) or it is necessary for the University's administrative or educational purposes and consent has been obtained.

4.2 The Collection and Holding of Personal Information

4.2.1 In most cases the University collects personal information directly from individuals through verbal and written communication, enrolment and admission forms and other types of direct questionnaires and surveys. The University also collects its own information in the form of student and employment records.

4.2.2 To ensure the safety of the University's campus property, its students, staff and visitors, the University uses CCTV cameras. These cameras are located in public areas across the campuses. When these cameras are used, the footage taken will include personal information. This information will only be used for the purpose of ensuring safety and will not be disclosed to a third party unless required by law.

4.2.3 Information is also collected from third parties such as government departments, education providers and other parties authorised to provide information to.

4.2.4 When personal information is collected from individuals, the University will make every

effort to draw this collection and its use to the individual's attention at the time the information is collected.

4.2.5 The University stores and holds personal information in a secure and restricted manner. Personal information is stored both electronically and in hard form. Personal information may be archived or destroyed once no longer needed in accordance with the University's Records and Disposal Policy and permitted by the APPs. In both cases, access is restricted to only those individuals authorised by the University to access the information in order to carry out their responsibilities. Where personal information is stored by a third party data storage provider the University will ensure that the third party provider is bound by a contractual obligation of confidentiality and non- disclosure.

4.2.6 When a person visits the University's website, log files are generated which will include the person's IP address. The website does not provide facilities for the secure transmission of information across the Internet and individuals need to be aware of the inherent risks in transmitting personal information across the Internet. More information about the University's website limited use of Cookies is outlined in paragraph 4.7 below.

4.3 Purpose of Collecting, Using, Storing and Disclosing Personal Information

4.3.1 Personal information provided by you to the University will only be used by the University for the administrative or educational purposes of the University, or for another purpose for which consent has been specifically provided.

4.3.2 Examples of the administrative or educational purposes which the University will collect, use, store or disclose personal information are to provide a means of:

- Establishing proof of identity;
- Enabling communication;
- Providing emergency details, including next of kin;
- Facilitating student admission, enrolment, discontinuation of program and/or graduation;
- Obtaining payment of program fees, university services and accessing eligibility for fee support, grants and programs under the *Higher Education Support Act 2003*, and allocation of CHESSN;
- Obtaining information relating to University quality and compliance issues;
- Meeting any statutory legal obligation of the Australian Government relating to the administration of tertiary education for domestic and overseas students; and/or
- Any other purpose for which an individual has consented to.

4.3.3 The University may disclose personal information to a third party where the disclosure is required to allow the University to operate and function in its capacity as a registered education provider and the purpose of the disclosure relates to the purposes set out above. For example, personal information may be disclosed to the Australian Government, contracted service providers, education providers and staff, and information technology providers. Where the University discloses personal information for the purposes outlined above the University will make every effort

to ensure the individual is advised of this disclosure at the time of collection of the personal information. Where personal information is disclosed for one of the purposes above the University will ensure that any disclosure to a third party is subject to the third party agreeing to use the personal information for the purpose disclosed and maintaining confidentiality.

4.3.4 The University will obtain specific consent to disclose personal information to marketing, communication and related third party agencies. Where an individual consents to the disclosure of personal information for marketing and communication purposes the individual will be provided with an ongoing opportunity to opt out of receiving any communications at any time.

4.3.5 In some cases the University may de-identify personal information for quality and statistical analysis. If we disclose this type of information we will do so in accordance with the APPS.

4.3.6 The University will not disclose staff personal information without the consent of the individual unless disclosure is permitted by law.

4.4 Requesting Access and Seeking Correction of Personal Information

4.4.1 Individuals have a right to request access to their personal information and to request its correction.

4.4.2 A request for access to an individual's personal information can only be made by the individual to whom the personal information relates and should be made in writing to the Campus Registrar if the request relates to a student's personal information or to the Legal Office of the relevant Campus if the request relates to a staff member or contractor. If the request is to seek a correction of personal information the individual seeking the correction must provide evidence to support the correction.

4.5 Making a Complaint About the University's Handling of Personal Information

4.5.1 If an individual wishes to make a complaint about the University's handling of personal information he or she should contact the Legal Office of the relevant Campus. The Legal Office will try to resolve the matter informally.

4.5.2 If a complaint cannot be resolved, the individual will be required to formally lodge the complaint in writing to the Legal Office with any supporting documentation attached to the complaint.

4.5.3 The University will deal with the complaint within 30 business days and advise the individual lodging the complaint of the outcome.

4.5.4 If the individual is unhappy with the outcome he or she may refer the complaint to the Office of the Australian Information Commissioner. Further information about the external dispute resolution can be found at www.oaic.gov.au.

4.6 Disclosure of Personal Information to Overseas Recipients

4.6.1 The University will use its best efforts to ensure that personal information is not disclosed to third party overseas recipients without express consent. Personal information collected by the University from staff and students is stored locally and

securely by the University.

4.6.2 In some limited circumstances, personal information may be disclosed to an overseas recipient, for example where the University enters into a contractual arrangement with an overseas service provider (such as international universities or education agencies) for the purpose of hosting students as part of a student exchange or study abroad study programs. In these circumstances the University will seek consent from the individual and the University will ensure that any third party agrees to collect, use or disclose personal information in accordance with the University's obligations under the Privacy Act.

4.7 Security and Use of University Website

4.7.1 The University holds personal information electronically and in hard copy form. Personal information held on electronic databases is protected by the University's Information and Communication Technology security. All financial transactions processed by the University and the use of payment details meet industry standards.

4.7.2 When accessing the University's website, log files are created by the web server that show the IP address of the visitor, time, date and pages visited. The information generated in web logs may be used to generate statistics about access to the University site. In limited areas (online areas where login is necessary) the website uses cookies an analytical service provided by Google. Cookies are text files placed on your computer, to help the website analyse how users use the site. This information will only be used for statistical purposes but will be transmitted to and stored by Google on servers in the United States. Visitors may refuse to use cookies by selecting the appropriate settings on their browser, however this may limit use of the website. By using the website in those limited areas the visitor consents to the processing of data about them by Google for the limited purpose above.

4.7.3 While the University has in place secure password protections for the University's website, there is always a possibility that any personal information disclosed online may not be fully protected. Individuals disclosing personal information online should ensure they take steps to be vigilant when using their University accounts and not disclose their passwords or login to third parties.

4.7.4 If an individual becomes aware of a security issue or has concerns about any information they may have disclosed on the website the University's Information Technology service desk should be contacted as soon as possible.

5 ROLES AND RESPONSIBILITIES

5.1 ***General Counsel or nominee*** is responsible for resolving internal complaints about the University's handling of personal information.

5.2 ***Chief Information Technology Officer*** is responsible for management of security of the University's website and Information Technology systems.

5.3 ***Academic Registrar*** is responsible for processes for the appropriate handling of student personal information.

5.4 ***Manager, Staffing (or equivalent)*** is responsible for processes for the appropriate handling of staff personal information.

6 CONTACTS

6.1 www.oaic.gov.au

6.2 legal@nd.edu.au

6.3 studentadmin@nd.edu.au

7 RELATED DOCUMENTS

7.1 The *Privacy Act* 1988 (Cth)
7.2 *Health Records and Information Privacy Act* 2002 (NSW)
7.3 *Privacy and Personal Information Protection Act* 1998 (NSW)
7.4 Australian Privacy Principles: http://www.oaic.gov.au/privacy/privacy-act.

8 DEFINITIONS

5.1 For the purpose of this Policy, the following definitions apply*:*

CHESSN means Commonwealth Higher Education Student Support Number.
University means The University of Notre Dame Australia.

Version	Date of approval	Approved by	Amendment
1	7 April 2014	Vice Chancellor	Effective date – new Policy.
2	May 2018	DVC, Academic	Updated nomenclature (Course to Program).
3	5 August 2019	Vice Chancellor	New section 4.2.2, minor editorial amendments, updated format to revised policy template, including clarification of roles and responsibilities.