Name of Policy	Privacy Policy
Description of Policy	This policy sets out how ACU manages privacy obligations and reflects the 13 Australian Privacy Principles (APPs) from Schedule 1 of the *Privacy Amendment (Enhancing Privacy Protection) Act* 2012 (Cth), which amends the *Privacy Act* 1988 (Cth).
Policy applies to	☒ University-wide ☐ Specific (*outline location, campus, organisational unit etc.)*
	☒ All Staff ☒ All Students ☒ Third Parties
Policy Status	☐ New Policy ☒ Revision of Existing Policy

Approval Authority	Vice-Chancellor and President
Governing Authority	Chief Operating Officer
Responsible Officer	Director, Governance

Approval Date	1 January 2014
Effective Date	1 January 2017
Approval Date of Last Revision	18 December 2017
Effective Date of Last Revision	1 January 2018
Date of Policy Review*	1 January 2020

** Unless otherwise indicated, this policy will still apply beyond the review date.*

Related Legislation, Policies, Procedures, Guidelines and Local Protocols	*Privacy Act* 1988 (Cth) *Privacy Amendment (Enhancing Privacy Protection) Act* 2012 (Cth) *Privacy Amendment (Notifiable Data Breaches) Act 2017* *Health Records and Information Privacy Act* 2002 (NSW) *Health Records Act* 2001 (Vic) *Health Records (Privacy and Access) Act* 1997 (ACT) *Access to and Correction of Personal Information Procedure* *Privacy Inquiries and Complaints Procedure* *Privacy Breach Procedure* *Records Management and Archive Policy* 2002 *Retention and Disposal Schedule* 2014 *Employee Records Privacy Policy* 2008

Table of Contents

1. Background Information

1.1 Australian Catholic University (**ACU**) is subject to the Commonwealth *Privacy Act* 1988 (**Act**). The *Privacy Amendment (Enhancing Privacy Protection) Act* 2012 which commenced in March 2014 made significant changes to the Act. This Policy complies with the new requirements imposed by the Act.

2. Policy Statement

2.1 ACU is committed to managing personal information in an open and transparent way. ACU is a registered company and is subject to the requirements of the Act. It adheres to the Australian Privacy Principles (**APPs**) set out in Schedule 1 to the Act.

3. Policy Purpose

3.1 This Policy sets out how ACU collects, holds, uses and discloses personal information including sensitive information.

4. Application of Policy

4.1 Subject to clause 4.2, this Policy applies to all personal information and sensitive information collected and held by ACU.

4.2 Despite clause 4.1, any act done or practice engaged in by ACU directly related to:

- a current or former employment relationship between ACU and an individual, and
- a current or historical employee record held by ACU relating to an individual

are exempt from this Policy in accordance with the Act and the APPs.

4.3 Employee records are governed by the provisions of ACU's *Employee Records Privacy Policy*.

5. Privacy Principles

5.1 Personal information collected and held by ACU

ACU collects personal information for the purposes of ACU's functions and activities. It collects personal information about staff, students and other individuals who have dealings with ACU for administrative need, to conduct its business, for legislative compliance or for research purposes.

The information may include residence and contact details, date of birth, details of next of kin, identifying information, including photographs, records of injuries, criminal checks, student enrolment information and academic performance, qualifications, financial information, information concerning individuals who apply to the University for appointment or admission, and information collected from or concerning human research subjects.

Some of the personal information that ACU collects and holds is sensitive information. ACU only collects sensitive information where it is necessary for the purpose for which it is being collected and with the individual's consent unless the collection is required or authorised by law.

5.2 How ACU collects and holds personal information

ACU collects and holds information from a number of sources. Where reasonably possible, ACU will only collect information from the individual to whom it relates. Frequently this will be collected through official University administrative processes but it may also be collected from email, letters or other forms of communication.

ACU also holds personal information about individuals that it generates in the course of its operational activities, such as recruitment information, student placement information, research grant applications, academic feedback and examination results and library loan records.

Personal information is held in both paper and electronic form, including databases.

When an individual accesses the ACU website, log files ("cookies") are created by the web server that contain certain information including the Internet Protocol (IP) address of the visitor, the previous site visited, the time and date of access and pages visited and downloaded. Cookies allow a website, such as the ACU website, to temporarily store information on an individual's machine for later use. ACU's website uses cookies to identify unique visitors to the site.

In order to improve ACU's services and assist the user, ACU may store information about users of its website to create a digital profile and provide them with information specific to them.

ACU also uses Web Analytics to obtain statistics about how its website is accessed. Web Analytics relies upon cookies to gather information for the purpose of providing statistical reports to ACU. The information generated by the cookie about an individual's use of the ACU website is transmitted to and stored by Web Analytic service providers on servers located within and outside Australia, but it does not include any personally identifying information.

Individual users generally have the option of accepting or rejecting cookies by adjusting the settings in their web browsers. However, rejecting cookies may impact upon the functionality of the ACU website.

The ACU website may contain links to other websites. ACU cannot control the privacy controls of third party websites. Third party sites are not subject to ACU's Privacy Policy or Procedures.

5.3 Notification of collection of personal information

When ACU collects personal information it will advise the individual why it is collecting that information and how it uses it, whether the collection of the information is required or authorised by law and the consequences for the individual if the personal information is not collected. It will also provide information about ACU's Privacy Policy and about the right of individuals to access and correct personal information. If ACU collects personal information in circumstances where the individual may not be aware of the collection it will seek to advise the individual of the collection.

5.4 The purposes for which ACU collects, holds, uses and discloses personal information

ACU collects and uses personal information for a variety of different purposes relating to its functions and activities including:

- enrolling, teaching, examining and graduating its students

- enhancing and assessing the student experience and providing a range of services to its staff and students including library access, health and counselling services, and recreational activities
- maintaining contact with its alumni and with other stakeholders in the community
- community engagement
- Government reporting
- commercial application of its intellectual property and professional expertise
- undertaking staff and student recruitment activities
- undertaking research
- handling complaints
- conducting its business and improving the way in which it conducts its business
- purposes directly related to the above.

5.5 Use or disclosure for secondary purposes

ACU does not use or disclose personal information for purposes other than the purpose for which it was collected (**the primary purpose**) unless:

5.5.1 the individual has consented to a secondary use or disclosure, or

5.5.2 the secondary use or disclosure is related to the primary purpose (in the case of personal information that is not sensitive information) or is *directly* related to the primary purpose (in the case of sensitive information), or

5.5.3 it is otherwise required or authorised by or under an Australian law or a court/tribunal order,or

5.5.4 a permitted general situation exists (as described in clause 9 of this policy), or

5.5.5 ACU reasonably believes that it is necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body.

In ordinary circumstances, any disclosure of personal information for a secondary purpose under scenarios 5.5.3, 5.5.4 and 5.5.5 must be approved by the Privacy Officer.

5.6 Security

ACU applies both physical and information and communications technology (ICT) security systems to protect personal information.

In relation to electronic records, personal information is collected via ACU's systems including web-based systems. ACU has put in place measures to protect against loss, misuse and alteration of electronic information. Where necessary, ACU also uses encryption technology to protect certain information and transactions.

5.7 Remaining anonymous or using a pseudonym

ACU understands that anonymity is an important aspect of privacy and that in some circumstances some people may prefer to use a pseudonym when dealing with ACU. People have the right to remain anonymous or to use a pseudonym when dealing with ACU. However for a significant proportion of its activities (e.g. matters relating to enrolment, teaching and assessment of individual students) it is impracticable for ACU to deal with individuals who have not identified themselves or who have used a pseudonym.

5.8 Unsolicited personal information

When ACU receives unsolicited personal information it will assess whether it is personal information that it could legally collect. If it is, it will treat it according to the APPs. If it is not, it will, if lawful to do so, destroy or de-identify it as soon as practicable.

5.9 Direct marketing

ACU will only use personal information for direct marketing with the individual's consent or when authorised by law.

5.10 Destruction of information that does not need to be retained

When ACU no longer needs to retain personal information, and is lawfully able to do so, it will destroy or de-identify that information.

5.11 How an individual may access personal information about the individual that is held by ACU

Subject to clause 4.2, anyone has a right under the Act to access personal information that ACU holds about them. Access to personal information is governed by the *Access to and Correction of Personal Information Procedure* (**Access Procedure**).

5.12 How an individual may seek the correction of personal information about the individual that is held by ACU

Subject to clause 4.2, anyone has a right under the Act to request corrections to any personal information that ACU holds about them if they think that the information is inaccurate, out of date, incomplete, irrelevant or misleading. Correction of personal information is governed by the Access Procedure.

5.13 How an individual may complain about a breach of the Australian Privacy Principles by ACU

Subject to clause 4.2, anyone may complain about a breach of an APP by ACU. Complaints should be made in accordance with the *Inquiries and Complaints Procedure* (**Inquiries and Complaints Procedure**).

5.14 How ACU will deal with complaints about breaches of the Australian Privacy Principles

ACU will deal with complaints about breaches of the APPs in accordance with the *Inquiries and Complaints Procedure*.

5.15 How ACU will manage an actual or suspected data breach under this policy

ACU will manage the process of dealing with an actual or suspected breach in accordance with the *Data Breach Procedure and Response Plan*

5.16 Disclosure of personal information to overseas recipients by ACU

ACU may disclose personal information to overseas recipients. For instance, ACU my disclose personal information to an overseas university which requires proof of the academic standing of an individual before it permits the individual to enrol or to facilitate staff or student exchange. ACU will only do this at the request of, or with the specific approval of, the individual whose personal information it is.

ACU will disclose personal information in these circumstances to an overseas recipient in any country.

ACU may also disclose personal information to overseas recipients who are service providers for research or purposes, including data storage. Australian law may not apply to those recipients. ACU will ensure that appropriate data handling and security arrangements are in place. Disclosure of personal information to overseas recipients may also be required or authorised by law.

5.17 Disclosure of personal information to third parties

ACU may disclose information to third parties to

- provide services
- for purposes of research to improve its operations and services
- facilitate national surveys carried out in relation to the higher education sector
- promote its activities
- if permitted or required by law, or
- otherwise with the consent of the individual.

Where ACU discloses personal information to third parties it will require restrictions on the collection and use of personal information equivalent to those required of ACU by the *Privacy Act 1988*.

6. Roles and Responsibilities

6.1 Approval Authority

The Vice-Chancellor and President is the Approval Authority for this Policy.

6.2 Governing Authority

The Chief Operating Officer is the Governing Authority for this Policy.

6.3 Responsible Officer

The Director, Governance is the Responsible Officer for this Policy.

6.4 Other Roles

The Chief Operating Officer is the ACU Privacy Officer.

The National Manager, Governance is the Privacy Coordinator.

7. Policy Review

7.1 Review

ACU will review this Policy and the Procedure regularly. It may amend the Policy and Procedure from time to time to ensure their currency with respect to relevant legislation and University Policy and Procedures and to improve the general effectiveness and operation of the Policy and Procedures.

In line with the University's *Policy on Policy Development* and *Policy Development Procedure*, this Policy is scheduled for review every five (5) years or sooner in the event that the Approval Authority or Governing Authority determine that a review is warranted. The Policy and Procedures will initially be reviewed one (1) year following the Effective Date.

7.2 Revisions made to this Policy

Date	Major or Minor Revision	Description of Revision(s)
22 December 2016	Major	Policy approved by the Vice-Chancellor and President
18 December 2017	Minor	To account for the Data Breach Procedure and Reponse Plan (5.15); clarify the Privacy Officer's authority in realtion to authorising the release of personal information (5.5); and to insert relevant definitions on account of mandatory reporting requirments under the *Privacy Amendment (Notifiable Data Breaches) Act 2017* (9)

8. Further Assistance

8.1 Alternative formats

Access to this Policy in alternative formats (e.g. hard copy) is available through the Privacy Coordinator whose contact details are listed under "Contact details" at the end of this Policy.

8.2 Contact details

Contact for all matters related to privacy, including:

- general inquiries;
- accessing personal information held about you;
- requests to correct personal information held about you; and
- complaints about breaches of privacy,

should be directed as follows:

Privacy Coordinator
E: privacy@acu.edu.au
W: www.acu.edu.au/policy/governance/privacy_policy_and_procedure
T: 02 9465 9151
P: PO Box 968, North Sydney NSW 2059

9. Glossary of Terms

Access Procedure means the *Access to and Correction of Personal Information Procedure* promulgated under this Policy.

Act means the *Privacy Act* 1988 (Cth).

Australian Privacy Principles (APPs) means the 13 APPs set out in Schedule 1 of the Act.

Data breach means the loss, unauthorised access to, or disclosure of, personal information.

Employee record means a record of confidential personal information relating to the employment of a staff member. The employee record comprises information about employment, including health, recruitment and selection, terms and conditions of employment, performance, discipline, and resignation. Employee records are exempt from the provisions of the Act.

Inquiries and Complaints Procedure means the *Privacy Inquiries and Complaints Procedure* promulgated under this Policy.

Loss means accidental or inadvertent loss of personal information likely to result in unauthorised access or disclosure. For example, an employee leaves a copy of a document or a device on public transport. If data can be deleted remotely or is encrypted it will not constitute an NDB.

Notifiable Data Breach (NDB) is a data breach that is likely to result in serious harm to any of the individuals to whom the personal information relates.A NDB occurs when personal information held by an organisation is lost or subjected to unauthorised access or disclosure.In such circumstances, ACU must notify the Office of the Australian Information Commissioner (OAIC) and affected individuals as required under the Privacy Amendment (Notifiable Data Breaches) Act 2017

Permitted general situation has the same meaning as provided for in section 16A of the Act and refered to in APP 6.2(c). The permitted general situations are: lessening or preventing a serious threat to the life, health or safety of any individual, or to public health or safety; taking appropriate action in relation to suspected unlawful activity or serious misconduct; locating a person reported as missing; asserting a legal or equitable claim; conducting an alternative dispute resolution process.

Personal information means information or an opinion in any form about an identifiable individual, or an individual who is reasonably identifiable, whether the information or opinion is true or not.

Privacy Coordinator means the person appointed by ACU from time-to-time to manage and coordinate ACU's compliance with the Policy and the Procedures at the direction of the Privacy Officer.

Privacy Officer means the person appointed by ACU from time-to-time to manage all inquiries and complaints arising under this Policy. The Privacy Officer may delegate the management of any or all of the inquiries and complaints arising under this Policy to the Privacy Coordinator.

Sensitive information means information about 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 practices, or criminal record, or health information, genetic information or biometric information.

Serious harm is determined with regard to the following list of relevant matters as provided for in section 26WG of the *Privacy Amendment (Notifiable Data Breaches) Act 2017:*

- the kind or kinds of information;
- the sensitivity of the information;
- whether the information is protected by one or more security measures;
- if the information is protected by one or more security measures—the likelihood that any of those security measures could be overcome;
- the persons, or the kinds of persons, who have obtained, or who could obtain, the information;
- if a security technology or methodology:
    - was used in relation to the information; and
    - was designed to make the information unintelligible or meaningless to persons who are not authorised to obtain the information;

  the likelihood that the persons, or the kinds of persons, who:
    - have obtained, or who could obtain, the information; and
    - have, or are likely to have, the intention of causing harm to any of the individuals to whom the information relates;

  have obtained, or could obtain, information or knowledge required to circumvent the security technology or methodology;
- the nature of the harm;
- any other relevant matters.

Unauthorised access means personal information accessed by someone who is not permitted to have access. This could include an employee of the entity, a contractor or external third party (such as hacking).

Unauthorised disclosure means where an entity releases/makes visible the information outside the entity in a way not permitted by the Privacy Act. For example, N employee accidently publishes a confidential data file containing personal information on the internet.

Web Analytics means the measurement collection, analysis and reporting of web data for the purpose of understanding and optimising web usage.