Privacy Policy

Section 1 - Background Information

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

Section 2 - Policy Statement

(2) 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 and other privacy laws as relevant. It adheres to the Australian Privacy Principles (APPs) set out in Schedule 1 of the Privacy Act 1988 (Cth).

(3) Personal information that directly relates to the employment of an ACU employee, being:

a. a current or former employment relationship between ACU and an individual employed in Australia; and
b. a current or historical employee record held by ACU relating to an individual employed in Australia;

is an Employee Record and is exempt from the Act. The Employee Record may include health, recruitment and selection, terms and conditions of employment, performance, discipline, resignation and taxation, banking or superannuation details. Personal information about the employee other than that in the Employee Record (such as social club membership, ACU gym membership or bank statements to their ACU email address) is subject to the Privacy Act.

(4) To the extent that ACU collects personal information from Individuals who are physically located in Europe (EU) and United Kingdom (UK) from activity targeting Individuals in these locations, the University is also subject to the requirements of the EU's General Data Protection Regulation (GDPR) and in addition for the UK, its equivalent implementation, the Data Protection Act 2018 (GDPR) with the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019. The employee record is covered by the GDPR.

(5) To the same extent, the University is also subject to the requirements of the Personal Information Protection Legislation of the People's Republic of China, or any other privacy legislation in a territory in which ACU carries out its activities.

Section 3 - Policy Purpose

(6) This Policy sets out how ACU collects, holds, uses and discloses personal information including sensitive information and Employee Records.

(7) This Policy does not solicit or imply an Individual's consent. If consent is required in relation to an activity or action, ACU will ask for that consent via a Collection Notice (see clause 24).

Section 4 - Definitions

(8) In this Policy, the following terms are used as defined:

Term	Definition
Access Procedure	means the Access to and Correction of Personal Information Procedure promulgated under this Policy.
Act	means the Privacy Act 1988 (Cth) (the Act).
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. Under the GDPR, the term used is personal data breach and involves the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to personal data.
Data Protection Impact Assessment (DPIA)	means an assessment carried out under GDPR, mandatorily if Art (35) of GDPR is met, to determine risks to Individuals from high-risk processing of personal information, taking into account the nature, scope and reasons for processing in the way the processing is intended to occur.
Data Subject	means the identifiable Individual to whom the personal information relates.
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 records from the Act and the Privacy Amendment (Private Sector) Act 2000 (Cth), but are covered under the GDPR(EU and UK).
Garante Privacy (Garante Per La Protezione Dei Dati Personali)	means the Italian privacy regulator relevant to ACU due to its establishment in Rome (Rome campus) under GDPR.
GDPR	means, as applicable, the General Data Protection Regulation ((EU) 2016/679) (EU GDPR) or the United Kingdom's implementation of the GDPR (UK GDPR) being the Data Protection Act 2018 (UK), Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 (SI 2019/419). The GDPR has extra-territorial reach and applies to, as applicable, any organisation established in the EU or UK, offering goods or services to, or monitoring the behaviour of, Individuals located in the EU or UK.
Information Commissioner's Office (ICO)	means Information Commissioner's Office (ICO) is the UK privacy regulator for Individuals located in the UK, under UK GDPR.
Individual	means the identifiable person to whom personal information applies. The term used under the GDPR is Data Subject.
International Data Transfer Assessments (IDTA)	means International Data Transfer Assessments (IDTA) which are required by UK's ICO for transfers of personal information out of the UK.
Loss	means accidental or inadvertent loss of personal information likely to result in the 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 a Notifiable Data Breach.
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 (Cth). The term used under GDPR is personal data breach.
Office of the Australian Information Commissioner (OAIC)	means the Australian regulator for Privacy.

Term	Definition
Permitted general situation	has the same meaning as provided for in section 16A of the Act and referred 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. Personal data is the term used under GDPR.
Privacy breach	
Privacy Impact Assessment (PIA)	is an assessment of the likely or known impacts, particularly high-risk impacts, to privacy and recommendations to manage or avoid identified impacts. Often occurs as part of Privacy by design process, in response to a law change, new project, data transfers, mergers and acquisitions; and/or in Australia. (Refer DPIA for GDPR.)
Privacy Inquiry and Complaints Procedure	means the Privacy Inquiry and Complaints Procedure promulgated under this Policy.
Privacy by design	means the deliberate consideration of privacy in a process, software or project design and its requirements from the outset.
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. For the Purposes of GDPR, ACU's Privacy Officer is also the Data Protection Officer. The Privacy Officer may delegate the management of any or all of the inquiries and complaints arising under this Policy to the Privacy Coordinator.
Procedures	means the Access to and Correction of Personal Information Procedure ("Access Procedure"); Privacy Inquiry and Complaints Procedure; and Data Breach Procedure and Response Plan.
Processing	means the collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of personal data. Used under GDPR and PIPL.
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. Special category data is the term used under the GDPR.

Term	Definition
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 (Cth): 1. the kind or kinds of information; 2. the sensitivity of the information; 3. whether the information is protected by one or more security measures; 4. if the information is protected by one or more security measures—the likelihood that any of those security measures could be overcome; 5. the persons, or the kinds of persons, who have obtained, or who could obtain, the information; 6. if a security technology or methodology: 1. was designed to make the information unintelligible or meaningless to persons who are not authorised to obtain the information; 2. was used in relation to the information; and 3. 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 ACU, an 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 1988 (Cth). For example, an 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.

Section 5 - Application of Policy

(9) Subject to clause 5 below, this Policy applies to all personal information and sensitive information collected and held by ACU.

(10) Whilst exempt from the Act, the Employee Record is subject to this Policy.

Section 6 - Privacy Principles

Personal Information Collected and Held by ACU

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

(12) 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 including banking and tax details, information concerning Individuals who apply to the University for appointment or admission, and information collected from or concerning human research subjects.

(13) Some of the personal information that ACU collects and holds is sensitive information, such as medical 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.

(14) ACU generally relies on the following legal grounds to process your personal information under both the ACt and the GDPR:

a. it is necessary to pursue ACU's legitimate interests – this is the usual basis on which ACU carries out its functions and activities for the purposes set out in clause 27 below and includes when ACU carries out research, conducts direct marketing or otherwise communicate with an Individual;
b. under a contract with an Individual;
c. with an Individual's consent – where required, we will only use personal information for the purposes for which consent was given; or
d. to comply with laws that apply to the University – ACU may use and process personal information where it is legally required or authorised to do so.

(15) Under 14 (a) and 14(d), ACU does not require an Individual's consent, but will assess the risk to you and your personal information, and where practicable, notify you. From time to time, ACU will ask for consent even where it is not legally required to in order to meet community expectation.

How ACU Collects and Holds Personal Information

(16) 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, such as the enrolment of students and employment of employees, but it may also be collected from email, letters or other forms of communication.

(17) An Individual may authorise the collection of information from a third party or, in the case of a person under the age of 16, authorisation may be given by a parent or guardian of that person under the ACU Authority to Act Policy and procedure.

(18) If ACU collects personal information about an Individual from a third party, reasonable steps must be taken to ensure that the Individual, including is or has been made aware of the collection and the reason for the collection.

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

(20) Personal information is held in both paper and electronic form, including in databases and in the computing cloud.

(21) ACU's campuses are protected by Closed Circuit Television (CCTV). ACU collects personal information about Individuals in the form of images through CCTV footage. By attending on-site, an Individual consents to the collection of their image. ACU also collects information about an Individual's movements around or location on a campus, via devices, applications and activity logs such as swipe card readers, the personal safety application and ACU technology system usage including wi-fi connection and enterprise platform usage.

(22) 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.

(23) ACU's website uses cookies to:

a. identify unique visitors to the site;
b. improve ACU's services and assist the user, ACU may store information about users of its website creating a digital profile and providing them with information specific to them;
c. obtain Web Analytics 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;
d. enable a chat service, including resuming conversation and sending emails about an Individual's enquiry, and to improve this service. The information generated by the cookie about an Individual's use of the ACU chat is transmitted to and stored by our third party service provider on servers located within and outside Australia.

(24) Individuals generally have the option of accepting or rejecting non-essential cookies via the cookie manager on the ACU website.Rejecting cookies may sometimes impact upon the functionality of the ACU website or ACU's ability to service your request.

(25) 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 this Policy or associated Procedures.

Notification of Collection of Personal Information

(26) When ACU collects personal information it will advise 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 this Policy and about the right of Individuals to access and correct personal information.

(27) 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.

(28) When ACU receives personal information without having solicited it ('unsolicited personal information'), ACU 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.

The Purposes for Which ACU Collects, Holds, Uses and Discloses Personal Information

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

a. enrolling, teaching, examining and graduating its students;
b. administering practical placements for students;
c. enhancing and assessing the student experience and providing a range of services to its employees and studentsincluding library access, health and counselling services, and recreational activities;
d. supporting or managing the welfare of students and employees where appropriate to do so;
e. maintaining contact with its alumni and with other stakeholders in the community;
f. community engagement;
g. government reporting;
h. accreditation of the University and its courses;
i. commercial application of its intellectual property and professional expertise;
j. undertaking staff and student recruitment activities;
k. undertaking research;
l. handling complaints;

m. conducting its business and improving the way in which it conducts its business, including market research; and
n. purposes directly related to the above.

Further purposes related to students are outlined in the Enrolment Privacy Collection Statement.

ACU will not use the information for a purpose other than that for which it was collected unless:

a. the Individual, including an employee, to whom the information relates has consented to the use of the information for that other purpose;
b. the other purpose for which the information is used is directly related to the purpose for which the information was collected;
c. the use of the information for that other purpose is necessary to prevent or lessen a serious and imminent threat to the life or health of the Individual or of another person;
d. the use is exempt by law (such as in the case of the Employee Record); or
e. if directed by law, whether:
    i. in response to a court or tribunal order, including a warrant or subpoena; or
    ii. as required or authorised to do so under an applicable law.

Use or Disclosure for Secondary Purposes

(30) ACU will only use or disclose personal information for purposes other than the purpose for which it was collected if:

a. the Individual has consented to a secondary use or disclosure; or
b. 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
c. if directed by law, whether:
    i. as required or authorised to do so under an applicable law.
    ii. in response to a court or tribunal order, including a warrant or subpoena; or
    iii. a permitted general situation exists (as described in Section 9 of this Policy); or
    iv. ACU reasonably believes that it is necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body.

(31) In ordinary circumstances, any disclosure of personal information for a secondary purpose under scenarios in clause 29, c, d., and e., must be approved by the Privacy Officer.

(32) ACU's internal processes for receiving and assessing third party requests for personal information are contained in the Third Party Access to Personal Information Protocol.

Disclosure of Personal Information to Third Parties

(33) ACU may disclose information to third parties to:

a. provide services to the Individual;
b. for purposes of research to improve its operations and services;
c. facilitate national surveys carried out in relation to the higher education sector;
d. promote its activities;
e. if permitted or required by law;
f. per (28)c, to prevent serious and imminent threat of harm to an Individual or others where a reasonable concern is held; or

g. otherwise with the consent of the Individual.

(34) Where ACU discloses personal information to third parties, it will require restrictions on the collection, use, disclosure and storage of personal information equivalent to those required of ACU by the Privacy Act 1988 (Cth), in so much as ACU has an agreement with the third party enabling ACU to do so.

Disclosure of Personal Information to Overseas Recipients by ACU

(35) In accordance with the purposes outlined in clause (32) above, ACU may disclose personal information to overseas recipients located in any country.

(36) ACU may disclose personal information to overseas recipients such as:

a. a 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;
b. service providers for research, technology or other purposes, including application use and data storage;
c. as required or authorised by law.

(37) The Act will usually not apply to overseas recipients. The GDPR may apply to overseas recipients. However, in accordance with clause 33 (above) and 37 (below), ACU will assess and minimise the risk to personal information by requiring that that appropriate data handling and security arrangements are in place.

(38) Where ACU transfers the personal information of a GDPR-applicable Individual out of the EU or UK, the transfer will be made in accordance with the GDPR and clause 14 of the Policy; and for a UK GDPR-applicable Individual, an IDTA may be conducted.

Privacy By Design

(39) ACU is required to take reasonable steps to implement practices, procedures and systems that will ensure compliance with the APPs or any other applicable privacy law.

(40) Privacy Impact Assessments (PIA) are undertaken in advance of:

a. procuring or developing software;
b. commencing a new project; or
c. making changes to existing systems, processes or activities;

that collects, handles, processes or discloses personal, particularly high risk, information, to identify and minimise the privacy risks associated with collecting, holding, using and disclosing personal information. Information and communications technology (ICT) security may also be assessed in the case of technology.

(41) Data Protection Impact Assessments (DPIA) and International Data Transfer Assessments (IDTA) are also conducted, as required (as part of the PIA process) under the GDPR.

Security

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

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

Remaining Anonymous or Using a Pseudonym

(44) 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, placement and assessment of individual students or the employment of employees; and matters assessed and treated by medical, allied health and services clinics), it is impracticable for ACU to deal with Individuals who have not identified themselves or who have used a pseudonym.

Direct Marketing

(45) ACU will only use personal information for direct marketing with the Individual's consent or when authorised by law. Individuals have the right to opt out of direct marketing (withdraw their consent).

Destruction of Information That Does Not Need to be Retained

(46) When ACU no longer needs to retain personal information, and is lawfully able to do so, it will destroy or de-identify that information. The Records Retention and Disposal Schedule contains information on the types of records that ACU is required to retain and the duration.

How an Individual May Access Personal Information About Them That is Held by ACU

(47) Subject to clause (5), anyone has a right under the Act to request whether personal information about them is held by ACU, know the nature of the information, the main purposes for which it is used and to seek access to it. Access to personal information is governed by the Access to and Correction of Personal Information Procedure.

(48) Access to personal information may include a summary of the information held, a copy, the opportunity to inspect records or take notes in the presence of an ACU representative.

(49) In accordance with the Act, ACU will provide access except:

a. in the case of personal information, other than health information, where providing access would pose a serious and imminent threat to the life or health of any Individual;
b. providing access would have an unreasonable impact upon the privacy of other Individuals;
c. the request for access is frivolous or vexatious;
d. providing access would reveal the intentions of the organisation in relation to negotiations with the Individual in such a way as to prejudice those negotiations;
e. providing access would be likely to prejudice an investigation of possible unlawful activity;
f. denying access is required or authorised by or under law; and/or
g. providing access would be likely to prejudice the outcome of an internal investigation.

(50) ACU will provide reasons for any denial of access or a refusal to correct personal information. ACU may consider whether the use of mutually agreed intermediaries would allow sufficient access to meet the needs of both parties.

(51) For a current or former ACU employee, access to their Employee Record is mandatory under the Fair Work Act 2009 (Cth). Access may be provided to the relevant staff member, their nominated supervisor or Executive Team member for positions in their line of responsibility. Access to time and wage information only may be provided to a Fair Work Inspector.

How Others May Access Personal Information About An Individual Other Than Themselves

(52) ACU will not disclose personal information about employees, students or other Individuals to anyone or any

organisation, unless:

a. the Individual has consented to the disclosure;
b. the disclosure is necessary to prevent or lessen a serious and imminent threat to life or health of any person;
c. the disclosure is in relation to a misconduct investigation or law enforcement process;
d. the disclosure is required by law, such as reporting to a government agency;
e. the disclosure is related to the purpose for which the information was collected and the Individual concerned is reasonably likely to have been aware, been notified, or is unlikely to be surprised by (object to) the disclosure,

(53) ACU will provide reasons for any denial of access or a refusal to correct personal information.

How an Individual May Seek to Correct Personal Information Held About Them by ACU

(54) 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 to and Correction of Personal Information Procedure.

How an Individual May Complain About a Privacy Breach by ACU

(55) Anyone may complain about a breach of the APPs, GDPR or any other applicable privacy legislation or regulation by ACU. Complaints should be made in accordance with the Privacy Inquiry and Complaints Procedure.

(56) ACU will deal with complaints about breaches in accordance with the Privacy Inquiry and Complaints Procedure.

How ACU Will Manage an Actual or Suspected Data Breach

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

Section 7 - Roles and Responsibilities

(58) The Chief Operating Officer and Deputy Vice-Chancellor (or delegate) is the designated Privacy Officer.

(59) The Privacy Coordinator is the designated Privacy Coordinator.

Section 8 - Policy Review

(60) ACU will review this Policy and the Privacy Inquiry and Complaints 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 Procedure.

(61) In line with the Policy Development and Review Policy, 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.

(62) Unless otherwise indicated, this Policy will still apply beyond the review date.

Section 9 - Further Assistance

Alternative Formats

(63) Access to this Policy in alternative formats is available through the Privacy Coordinator whose contact details are

listed below under “Contact details”.

Contact Details

(64) Contact for all matters related to privacy, including:

a. general enquiries;
b. requests to access or correct personal information held about Individuals;
c. requests to erase, request portability or restrict / object to processing of personal information held about Individuals under GDPR or other applicable privacy laws; and
d. complaints about breaches of privacy;

should be directed as follows:

> Privacy Coordinator
> E: privacy@acu.edu.au
> T: +617 3861 6415
> P: 1100 Nudgee Road, Banyo QLD 4014

Status and Details

Status	Not Yet Approved
Effective Date	To Be Advised
Review Date	To Be Advised
Approval Authority	
Approval Date	To Be Advised
Expiry Date	Not Applicable
Responsible Executive	Diane Barker Director, Legal, Assurance and Governance
Responsible Manager	Matthew Charet National Manager, Governance
Enquiries Contact	Natalie Koppe Privacy Coordinator Legal, Assurance and Governance Directorate