Privacy Policy

Section 1 - Purpose

(1) This Privacy Policy (Policy) outlines the personal information handling practices of the University of Canberra (University) and describes the framework to protect the privacy of all personal information or other data collected by the University in compliance with relevant privacy laws.

Section 2 - Scope

(2) This Policy applies to all members of the University, including its staff and controlled entities, unless otherwise agreed by Council and the Vice-Chancellor of the University. A reference to the University in this Policy is a reference to all such entities of the University.

(3) This Policy incorporates and is to be read in conjunction with the University's Privacy Management and Data Breach Plan as well as the Data Classification Schedule.

Section 3 - Definitions

(4) Highly Sensitive means data subject to regulatory control, University Legal Advice, Personal Information about persons under age of 18, Tax File Numbers, Credit card details, campus safety data, personnel and/or payroll records, student records, commercial data belonging to a third party (contracts and commercial in confidence), patent information, personal health information and clinical trial data. It also includes data identified under the Australian government security classification system as confidential or higher (refer to Protective Security Policy Framework).

(5) Personal Information means information or an opinion about an identified individual, or an individual who is reasonably identifiable, whether the information or opinion is true or not; and whether the information or opinion is recorded in a material form or not. It does not include personal health information.

(6) Personal health information is highly sensitive and means any Personal Information, whether or not recorded in a health record relating to the health, an illness or a disability of the individual; or collected by a health service provider in relation to the health, an illness or a disability of an individual.

(7) Private information includes but is not limited to business unit process and procedure, unpublished intellectual property, ITC system design and configuration information, a limited range of Personal Information such as student numbers.

(8) Sensitive information means in relation to an individual, information or an opinion about an individual's racial or ethnic origin, immigration status, political opinions, memberships of political, professional and trade associations and unions, religious and philosophical beliefs, sexual orientation or practices, criminal history, health information, and genetic and biometric information. In relation to the University, it means organisational financial data, exam material and results, internal directories and organisational charts, internal planning documents, research data (containing Personal Information), and data considered commercial in confidence.

Section 4 - Principles

(9) The University will strive to create, promote and maintain a culture of respect for the privacy of all individuals.

(10) Through the management of privacy and incorporating privacy requirements into processes, procedures and information systems, the University aims to foster and support a relationship of trust between the University and its staff, students and members of the community.

The University's Approach

(11) The University will only collect, hold, use and disclose Personal Information to enable the University to meet legal obligations and where it is reasonably necessary or related to one or more of the University's functions or activities. These include:

a. for students (includes past, current and future): to administer enquiries, admission, enrolment, academic progress, academic integrity, discipline, graduation, accommodation, access to University facilities and services, library loans, fees, visa, immigration, taxation and financial support purposes, and in relation to graduates, for alumni activities; and
b. for employees, affiliates, visitors and sub-contractors: to administer pay, entitlements, performance, teaching, research, access to University facilities and services, visa, immigration and taxation purposes, and in relation to work health and safety, or rehabilitation and compensation matters.

How the University Collects and Holds Personal Information

(12) Personal Information is considered to be 'held' by the University if the University is in possession or control of the information, or the information is in the possession or control of a person employed or engaged by the University in the course of that employment or engagement.

(13) The University collects and holds information in a number of ways including:

a. because it is required to provide a service which has been requested – for example, to implement a reasonable adjustment plan or if an individual becomes a client of the Medical and Counselling Centre or a University Health Clinic;
b. because it has been provided to the University – for example, by applying for admission or employment, participating in mobility or exchange programs, participating in or commenting on online forums, registering to attend an event, asking the University a question or making a complaint or;
c. because of an individual's previous or current relationship with the University – through the University's advancement, alumni relations and philanthropy activities; and
d. because the University is required by law to collect it – for example, because of higher education and immigration laws or monitoring and logging of metadata from an individual's use of IT and online services and facilities provided by the University.

(14) Sometimes the University may use or disclose Personal Information in circumstances where it would be reasonably expected to use or disclose it.

(15) The University will not collect, hold, use or disclose sensitive information or personal health information, unless with the individual's consent or if an exemption exists or is authorised by law. However, the University may collect, use or disclose personal, health or sensitive information in situations where it may be impracticable to obtain an individual's consent or give prior notice, if the University reasonably believes it is necessary to do so, such as:

a. to lessen or prevent a serious threat to life, health or safety;

b. to review CCTV cameras on University premises;
c. to take appropriate action in relation to suspected unlawful activity or misconduct;
d. for enforcement related activities conducted by, or on behalf of, an enforcement body; for example, to assist authorities to locate a person reported as missing; or
e. when establishing or defending a legal or equitable claim, or participating in a confidential dispute resolution process.

How the University Discloses Personal Information

(16) Common situations in which the University discloses Personal Information include, but are not limited to:

a. other higher education institutions, if a student is involved in a student mobility, exchange, cross-institutional or joint program, or if a student is transferring to another institution;
b. certain student administration matters;
c. the University of Canberra College;
d. accommodation service providers; for example, a Lodge, College or Hall of Residence; if a student's accommodation is dependent on academic progress or affected by any Statutes, Rules, or policies of the University;
e. a returning officer or other appointed electoral body for conducting elections of representatives to official University panels, committees, boards and associations;
f. publications about some examination results and the award of some prizes and scholarships;
g. when requested, for example, when a person graduates from the University (the record of a person's graduation from the University is a public document);
h. releasing information pursuant to the University's Statutes, Rules, policies and procedures, or pursuant to a contractual obligation to which an individual has agreed to, such as Work Integrated Learning placements;
i. publications about research activities at or involving the University in which an individual has elected to be involved;
j. releasing statistical information to Australian Government Departments who are authorised to require it, the Tertiary Education Quality and Standards Agency (TEQSA), state and territory governments, Tertiary Admissions Centres (TACs), Higher Education providers for the purposes of the Higher Education Support Act 2003 (Cth) ('HESA') or the Education Services for Overseas Students Act 2000 2000 (Cth) ('ESOS'), and Universities Australia;
k. reporting to the Australian Tax Office about Commonwealth-supported fee liabilities or to facilitate income tax assessment;
l. reporting to Australian Government Departments with portfolio responsibility for social security and/or veterans' entitlement matters about an individual's income or a student's attendance if the University is legally required to do so;
m. reporting to Australian Government Departments with portfolio responsibility for child support matters about an individual's income if the University is legally required to do so;
n. if an individual is not an Australian citizen, reporting to Australian Government Departments with portfolio responsibility for migration and immigration, employment, higher education, research and technology, and related matters;
o. the Australian National Audit Office for auditing purposes; and
p. if the University is required by law to disclose the information.

(17) The University may disclose Personal Information to an external review body if an individual seeks an external review of a University decision or makes a complaint to an external complaint handling body such as the ACT Ombudsman.

(18) If an individual makes a complaint or report an incident to the University about another individual at the University, in some circumstances; the University may be required to disclose some Personal Information to the individual about whom a complaint has been made. It may be that sometimes the University is unable to act on a complaint or allegation unless consent is given to this kind of disclosure.

Engagement with Third Parties

(19) The University does not disclose Personal Information about students to a student's relatives or other relevant party without the student's consent. Students under 18 years of age and/or students who are registered with Inclusion and Engagement may consent to such disclosures of Personal Information in writing.

(20) When the University engages third parties to perform services that involve handling any of the Personal Information held by the University, the University engages the third-party service provider in accordance with the obligations that apply to the University under the Privacy laws.

Social Media

(21) If an individual chooses to communicate with the University or access information about the University through a social network service or app, the social network or app provider and its partners may collect, hold, use or disclose Personal Information, in Australia or overseas, for their own purposes and according to their own policies. This Policy does not apply to those services.

Collecting through Websites

(22) Entry to some University web services is restricted by user log-in protocols. The University requires individuals to use their University ID to access these sites to help the University keep the information accessible through these sites secure from unauthorised alteration, use or disclosure, to resolve problems with the University's IT systems, and to keep an auditable record of who has accessed this information.

(23) The University has a public website. When the website is viewed, the server makes a record of the visit and logs some or all of the following information:

a. the viewer's browser's internet IP address;
b. the date and time of the visit to the site;
c. the pages accessed and documents downloaded;
d. the previous site visited;
e. the type of browser the viewer is using; and
f. the username entered if accessing a restricted site.

(24) The University uses this information for statistical purposes, for system administration tasks to maintain this service and to personalise the user's experience in future visits to the site. The University may use that information to identify and resolve problems with the University's IT systems, and to keep an auditable record of who has accessed the University's IT systems for security purposes. The University does not attempt to identify individuals unless prior consent is given. However, in the unlikely event of an investigation, the University, a law enforcement agency or other government agency may exercise its legal authority to inspect the University's server's logs or require reporting by the University.

Building Access

(25) If an individual enters any University building or room that requires the individual to swipe their University ID card to gain entry, the University may collect and use that information to keep an auditable record for safety and security purposes.

Library Loans

(26) If an individual borrows material from the University library, the University collects and uses Personal Information to manage priority course-based access to materials and to communicate with individual's about their library loans. The University does not keep this information after borrowed library material is returned.

Email Lists

(27) The University collects individuals' non-University email address (and other contact details) when these are provided to the University. The University will only use this information to contact individuals for administrative purposes related to their engagement with the University. The University will use graduates email addresses to send information about University alumni and philanthropy activities. Graduates can opt out of alumni related activities at any time by clicking on the unsubscribe link included in all such emails.

(28) If an individual registers to attend an event, the University usually collects the contact details provided at registration to communicate with individuals about the event registered for. The University may also communicate with individuals about other events the University thinks individuals might be interested in. Individuals can opt out of receiving further emails at the time of registering for an event, by telling the sender by return email that they do not want to receive further emails, or the individual can unsubscribe from further events emails using the link in the email, according to how the event registration process is administered.

(29) The University also collects individuals' non-University email address for purposes of sending student notifications and issuing passwords.

Anonymity

(30) Where practicable and lawful, the University will allow individuals to interact with the University anonymously or using a pseudonym. However, for most of the University's functions and activities the University usually needs an individual's name and contact information or University ID number, and enough information about the particular matter to enable the University to respond to the inquiry, request, application, donation or complaint.

(31) The University will also allow individuals to request the destruction of the Personal Information the University holds where practicable and lawful in line with the lawful principle of the 'right to be forgotten' under the European Union (EU) General Data Protection Regulation. The General Data Protection Regulation, which took effect on 25 May 2018, replaces the previous European data protection legislation.

Collection from Other People

(32) In the course of the University's day to day activities as an employer and a higher education provider, the University may collect Personal Information about individuals indirectly from publicly available sources, or from third parties. The University also collects Personal Information from publicly available sources to enable the University to identify and contact stakeholders who may be interested in the University's endowment and philanthropy programs.

Overseas Disclosure

(33) In performing and managing its functions and activities, the University may need to make personal information available to third party services providers, including providers of cloud services and website hosts. These third parties may be located overseas. The University will take reasonable steps to ensure that any third parties located overseas whom the University engages to handle Personal Information are bound by substantially similar privacy standards and obligations as the University.

(34) The overseas locations of providers where University data is held is as follows:

- United States of America
- Canada
- United Kingdom
- European Union
- Japan
- Singapore
- Hong Kong
- India
- Vietnam
- China

(35) If a student is involved in a mobility, exchange, cross-institutional or joint program with an institution in another country, or if a student is transferring to another institution overseas, the University will disclose Personal Information to the student's home or host institution overseas, including matters which impact on the student's ability to participate in the program, such as misconduct.

Storage and Security of Personal Information

(36) Most of the information the University creates or handles is contained in, or forms part of, an Australian Capital Territory Record. The University takes reasonable steps to destroy or de-identify Personal Information in a secure manner when the University no longer needs it. The University is required to deal with most of its records in accordance with the Territory Records Act 2002 and Disposal Authorities issued pursuant to that Act.

Access and Correction of Personal Information

(37) The University will make its best effort to ensure the Personal Information it holds is accurate and complete when collected and kept up to date for the period in which it is used.

(38) An individual has a right to know what Personal Information is held about them and a right to access that information for review or correction where appropriate.

(39) If requested, the University will give individuals access to their Personal Information, unless there is a law that allows or requires the University not to.

(40) If the University makes a correction to the information it holds and discloses the incorrect information to others, an individual can request that the University informs the individual about the correction. The University will do so unless there is a valid reason not to. If the University refuses to correct Personal Information, an individual can ask the University to attach a statement to it stating that the individual believes the information is incorrect and why.

Privacy Complaints

(41) If an individual wishes to make a complaint about how the University has handled their Personal Information, this should be done in writing. For assistance in lodging a complaint, please contact: privacy@canberra.edu.au.

(42) If the University receives a complaint about how Personal Information has been handled, the University will determine what (if any) action should be taken to resolve the complaint.

(43) Privacy complaints will be referred for resolution to the relevant data and/or information system stewards in the first instance. The University will promptly indicate that the complaint has been received and will endeavor to respond to the complaint within 30 days.

(44) If an individual is not satisfied with the University's response, a review by a more senior officer within the

University can be requested, or a complaint can be lodged at the Office of the Australian Information Commissioner.

Contacts

Telephone: +61 2 6201 5569
TTY: +61 2 6251 4601 (for hearing impaired callers)
Email: privacy@canberra.edu.au
Mail: Privacy Contact Officer
University of Canberra
BRUCE ACT 2601
Australia

Section 5 - Procedure

(45) Nil.

Section 6 - Definitions

Terms	Definitions
Data Breach	means, for the purpose of this Plan, when Information is lost, stolen or subjected to unauthorised access, modification, disclosure, or other misuse or interference, whether accidentally or intentionally.
Direct marketing	means issuing marketing or promotional materials about the University or other parties directly to an individual (e.g. by post, email, SMS).
Highly Sensitive	means data subject to regulatory control, University Legal Advice, Personal Information about persons under age of 18, Tax File Numbers, Credit card details, campus safety data, personnel and/or payroll records, student records, commercial data belonging to a third party (contracts and commercial in confidence), patent information, personal health information and clinical trial data. It also includes data identified under the Australian government security classification system as confidential or higher (refer to www.protectivesecurity.gov.au).
Notifiable data breach	means a data breach that is likely to result in serious harm, which must be notified to affected individuals and the Office of the Australian Information Commissioner (OAIC).
Personal health information	is highly sensitive and means any Personal Information, whether or not recorded in a health record relating to the health, an illness or a disability of the individual; or collected by a health service provider in relation to the health, an illness or a disability of an individual.
Personal Information	means information or an opinion about an identified individual, or an individual who is reasonably identifiable, whether the information or opinion is true or not; and whether the information or opinion is recorded in a material form or not. It does not include personal health information.
Private information	includes but is not limited to business unit process and procedure, unpublished intellectual property, ITC system design and configuration information, a limited range of Personal Information such as student numbers.
Real Risk of Serious Harm	includes risk of physical, psychological, emotional, reputational, economic or financial harm to an affected individual, for the avoidance of doubt this includes, but is not limited to, risk of identity theft, financial fraud, health fraud, embarrassment, discrimination or disadvantage and blackmail.
Sensitive information	means in relation to an individual, information or an opinion about an individual's racial or ethnic origin, immigration status, political opinions, memberships of political, professional and trade associations and unions, religious and philosophical beliefs, sexual orientation or practices, criminal history, health information, and genetic and biometric information. In relation to the University, it means organisational financial data, exam material and results, internal directories and organisational charts, internal planning documents, research data (containing Personal Information), and data considered commercial in confidence.

Serious Breach	includes where: (i) multiple individuals are affected by the breach or suspected breach; (ii) there are, or there may be, a Real Risk of Serious Harm to the affected individual(s); (iii) the breach or suspected breach indicates a systemic problem in the University's processes or procedures; (iv) there could be media or stakeholder attention as a result of the breach or suspected breach; or (v) the risk rating is "Medium", "High" or "Extreme" as identified in Annexure 3: Data Classification Assessment of this Response Plan.

Status and Details

Status	Current
Effective Date	18th April 2023
Review Date	18th April 2024
Approval Authority	Vice-Chancellor
Approval Date	18th April 2023
Expiry Date	To Be Advised
Responsible Executive	Eric Wells General Counsel and University Secretary
Responsible Manager	Nick Markesinis Manager, Policy and Compliance
Author	Jerrin Mathew Policy and Compliance Coordinator
Enquiries Contact	Nick Markesinis Manager, Policy and Compliance --- Office of General Counsel