Privacy Policy

Authority Source: Vice-Chancellor

Approval Date: 07/09/2018

Publication Date: 12/09/2018

Review Date: 07/09/2021

Effective Date: 12/09/2018

Custodian: General Counsel and University Secretary

Contact: legal@canberra.edu.au

Accessibility: Public

Status: Published

In developing this policy the University had regard to the provisions of section 40B(1)(b) of the Human Rights Act 2004 (ACT).

PURPOSE:

This Privacy Policy (Policy) outlines the personal information handling practices of the University of Canberra 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.

SCOPE:

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.

This Policy incorporates and is to be read in conjunction with the University's Privacy Management and Data Breach Plan (Appendix 2) as well as the Data Classification Schedule (Appendix 3).

Definitions

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).

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.

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.

Private information includes but is not limited to business unit process and procedure, unpublished intellectual property, ITC system design and configuration information, a limited range of Personal Information such as student numbers.

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.

PRINCIPLE:

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

- 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
- 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
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.

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

- **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 Faculty of Health Clinic;
- **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;

- **because of an individual's previous or current relationship with the University** – through the University's advancement, alumni relations and philanthropy activities; and
- **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.

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

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:

- to lessen or prevent a serious threat to life, health or safety;
- to review CCTV cameras on University premises;
- to take appropriate action in relation to suspected unlawful activity or misconduct;
- 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
- when establishing or defending a legal or equitable claim, or participating in a confidential dispute resolution process.

How the University discloses Personal Information

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

- 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;
- certain student administration matters;
- the University of Canberra College;
- 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;
- a returning officer or other appointed electoral body for conducting elections of representatives to official University panels, committees, boards and associations;
- publications about some examination results and the award of some prizes and scholarships;
- 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);
- 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;
- publications about research activities at or involving the University in which an individual has elected to be involved;
- 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*

(Cth) ('ESOS'), and Universities Australia;

- reporting to the Australian Tax Office about Commonwealth-supported fee liabilities or to facilitate income tax assessment;
- 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;
- 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;
- 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;
- the Australian National Audit Office for auditing purposes; and
- if the University is required by law to disclose the information.

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.
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
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.

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
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
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.

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:

- the viewer's browser's internet IP address;

- the date and time of the visit to the site;
- the pages accessed and documents downloaded;
- the previous site visited;
- the type of browser the viewer is using; and
- the username entered if accessing a restricted site.

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

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

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

The University collects individuals' non-University of Canberra 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 of Canberra 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.

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.

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

Anonymity

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.

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 (GDPR)*. The GDPR, which took effect on 25 May 2018, replaces the previous European data protection legislation.

Collection from other people

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

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. Appendix 1 lists the overseas locations of providers where University data is held.

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

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* (ACT) and Disposal Authorities issued pursuant to that Act.

Access and correction of Personal Information

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.

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.

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.

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

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.

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.

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.

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

Related Documents

Charter of Conduct and Values
University of Canberra Compliance Register
Data Governance Framework
Delegations Policy Framework
Enterprise Agreement
Fraud and Corruption Control Plan
Australian Capital Territory Public Interest Disclosure Guidelines 2014
DITM and Records Management Policy Manual

LEGISLATION:

Information Privacy Act 2014 (ACT)
Privacy Act 1988 (Cth)
Health Records (Privacy and Access) Act 1997 (ACT)
Territory Records Act 2002 (ACT)
General Data Protection Regulation
Freedom of Information Act 2016 (ACT)
Higher Education Support Act 2003 (Cth)
Education Services for Overseas Students Act 2000 (Cth)
Social Security (Administration) Act 1999 (Cth)
Spam Act 2003 (Cth)

SUPPORTING INFORMATION:

APPENDIX 1

Locations of overseas recipients of Personal Information

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

APPENDIX 2

Privacy Management and Data Breach Plan

Purpose

The Privacy Policy is implemented by this Privacy Management and Data Breach Plan (Plan), which outlines the University of Canberra's approach to the protection of information.

Principles

Personal information management and use

Personal Information will only be collected in line with the Plan and where:

- collection is relevant and necessary in accordance with the Principles of this policy; and
- a privacy notice and/or consent as relevant to the situation is included as part of the collection process.

Personal Information may only be used or disclosed in line with the Plan.

Data breach reporting

The University takes all reasonable steps to protect the security of the Personal Information it holds from both internal and external threats by regularly assessing the risk of misuse, interference, loss, and unauthorised access, modification or disclosure. Measures taken may be physical, electronic, or procedural. University staff, contractors, affiliates and students are advised to treat Personal Information with care, and in accordance with this Privacy Policy and other applicable laws.

All University staff have an obligation to implement the privacy principles established by the relevant privacy laws in their day to day practices by complying with such laws and their obligations under this Policy in the course of collecting, managing, using, disclosing and securing Personal Information and data.

Definitions

a. **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;

b. **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;

c. **Direct marketing** means issuing marketing or promotional materials about the University or other parties directly to an individual (e.g. by post, email, SMS);

d. **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;

e. **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).

Responsibility for using Personal Information

Where the University discloses, transfers or stores Personal Information outside the University, it is the responsibility of the relevant data and/or information systems stewards to ensure (in line with the Privacy Policy) that:

- all privacy impacts are assessed and addressed, including the disclosure, transfer or storage of Personal Information outside Australia or to a Commonwealth agency, and
- all contractual obligations with relevant third parties are imposed through an enforceable contract, appropriately managed and monitored.

Personal Information may only be retained for as long as it may legally be used in line with the purpose for which it is collected and/or for which consent is received. Minimum legal retention requirements as outlined in Section 2.3 Records Management of the DITM and Records Management Policy Manual also apply.

Exemptions to privacy requirements may only be applied where appropriate in the circumstances and in line with the Plan and the Privacy laws.

A. **Privacy Management**

The University is subject to the *Privacy Act 1988* (Cth) (the Privacy Act) and the *Information Privacy Act 2014* (ACT). Through its Privacy Policy and this Plan the University describes how it will keep its practices consistent with the Australian Privacy Principles (the Principles), as well as providing guidance to University staff on the application of the Principles. This Plan also describes the application of the Principles and the University’s own policy to everyday decision making by University staff.

1. Collection of Personal Information - [Privacy Policy principle 1.1, 1.3]

Information must be reasonably necessary or directly related to the University’s functions or activities. In practice, this means Personal Information should not be collected ‘just in case' it may be useful in the future and must be collected by fair means.

Example: If an individual is compiling a mailing list of people who want to receive information about the University and only intends on sending that information by email, their home address or phone number should not be requested.

Example: Clinical placement hosts usually require students to have a working with vulnerable people card and a criminal history check. A school may ask to sight these documents, but it is not necessary for a school to retain copies however.

2. Notifying individuals of collection - [Privacy Policy principle 1.5]

Where Personal Information is collected or solicited from forms or websites or in person, University staff must notify individuals.

Example: A link to the Privacy Statement must be included in online or written forms.

3. Sensitive information and Personal Health information - [Privacy Policy principle 1.3]

Generally University staff should only collect Sensitive Information with the individual's consent and when the information is reasonably necessary for one or more of the University's functions or activities.

However, staff may collect Sensitive Information without an individual's consent in limited circumstances if staff reasonably believe it is necessary to do so and it would be impracticable to obtain consent or give prior notice.

Example: Police have attended Student Central. A staff member has been asked to provide information about a student's course enrolment, social club membership, mobile phone number and last known residential address. The police state they are concerned the student is missing.

Example: The 'gender' field on forms should not be present or mandatory unless the University requires that information to provide specific services to the individual.

University staff should seek advice from the Legal office before relying on an exemption in order to disclose or collect Sensitive Information without an individual's consent.

4. Collection of information from a third party - [Privacy Policy principle 1.3, 1.5]

In accordance with the Privacy Policy, where Personal Information about an individual is collected from a third party source, even if the information is collected from a publicly available source, University staff must take reasonable steps to ensure that the individual is or has been made aware:

a. that the University has collected the information and the circumstances of the collection; and
b. of the University's Privacy Statement.

Example: A researcher obtains names and addresses from the ACT electoral roll in order to survey persons in a specific electorate. The survey must explain where the researcher has obtained an individual's details from, and include the University's Privacy statement.

5. Anonymity and use of a pseudonym - [Privacy Policy principle 1.7]

Wherever it is practicable and lawful, the University must provide individuals with the option of not identifying themselves, or of using a pseudonym.

Example: If UC Life hold a competition on a social media platform the University should provide options for anonymity or the use of a pseudonym.

Example: The 'name' field on survey forms should not be mandatory unless the University intends to make follow-up contact with the individual.

6. USE AND DISCLOSURE - [Privacy Policy principle 2.1, 2.2]

What is the Purpose?

The University can only use or disclose personal information for the purpose for which it is collected. This is the '*primary purpose'*. To use the information for another purpose (a '*secondary purpose'*) the following must apply:

- the individual would reasonably expect the University to use or disclose the Personal Information for the Secondary purpose;
- the Secondary purpose is related to the Primary purpose (or in the case of Sensitive Information, directly related to the Primary purpose); or
- another exemption exists at law.

For example, in order to administer enrolment of students and deliver welfare services, the University may need to share Personal information with the UC College. This information may also be required to coordinate student accommodation with UniLodge and CLV.

Disclosure is also permitted if it is unreasonable or impracticable to obtain the individual's consent to the use or disclosure **and** the University reasonably believes that the use or disclosure is necessary to lessen or prevent a serious threat to the life, health or safety of any individual, or to public health or safety.

Examples of activities where disclosure is permitted:

- A student applies to enrol in a program that is clearly advertised as being jointly delivered by the University with other universities and that applications will be considered by all collaborating universities.
- An individual submits an entry to a University-run competition. The competition rules clearly state that entries will be judged by an independent panel.
- The University is served with a subpoena to produce personnel records of a staff member or a student who is involved in a motor vehicle accident case.
- The Vice-Chancellor's office receives an email from Centrelink, acting under the *Social Security (Administration) Act 1999* (Cth), requesting that the University provides enrolment information about a student.
- The University's Student Life (pastoral care) team forms a reasonable belief that a student is at risk of self-harming. The University can notify the ACT Mental Health Crisis Team triage service and provide location and other sensitive information so that it can determine whether to take action to locate the student and provide intervention.

7. Permitted disclosure to third parties [Privacy Policy principle 2.4] including Overseas recipients – [Privacy Policy principle 2.5, 2.6]

The University is permitted to disclose Personal Information to third parties in the manner described in the Privacy Policy. However, in order to protect the Personal Information of individuals, the University must ensure that there is a contract in place with the third party which contains obligations on that party to comply with the Australian Privacy Principles.

Examples of permitted third party disclosure include:

- *Providing government departments and agencies with Personal Information to satisfy reporting requirements.*
- *Sharing date of birth, course information and reasonable adjustment plans with the University's controlled entities or the University of Canberra College so that services can be provided to a student.*

- *Sharing student names and email addresses with a Canadian software provider in order to establish user accounts to enable students to have access to the University's internet-based education resources and assessment tools.*
- *The Faculty of Health organises clinical placements for students and the placement provider requires police checks, names and emergency contact details of the attending students.*
- *Sharing research data containing Personal Information with an overseas collaborating institution.*

Examples where third party disclosures **are not** permitted include:

- *storing electronic files with Personal Information on a server located overseas where the University does not have a contract with this organisation; eg*
    - *downloading information to 'Dropbox',*
    - *storing research data on Google Drive*
- *disclosing a student's grades to a prospective employer*
- *informing a parent about student class attendance or welfare*

8. Direct marketing - [Privacy Policy principle 2.7]

Direct marketing is not permitted under privacy laws, **unless:**

- consent has been obtained from the individual via an opt in process;
- the marketing is directly related to the purpose it was collected for; or
- the individual would reasonably expect us to use or disclose the Personal Information for that purpose.

For example:

- *The University sends an email to all enrolled students to advertise a public event being held by the University of Canberra Union.*
- *The Marketing team sends a tweet about new course offerings in the upcoming semester to all students.*

Hardcopy direct marketing material must contain a contact point for the individual to opt out of receiving further direct marketing communications from that area of the University issuing the direct marketing communication. Direct marketing material requires an opt-out mechanism where it is sent by email and SMS to comply with the *Spam Act 2003* (Cth). Once an individual has made a request to opt out of receiving information from a particular area (e.g. advancement), the University must not issue any further direct marketing communications to the individual about those matters.

9. ACCURACY OF INFORMATION - [Privacy Policy principle 3.1, 4.4, 4.5, 4.6]

In accordance with the Privacy Policy, Personal Information the University collects, uses or discloses is accurate, up-to-date, complete, relevant and not misleading.

To assist the University in meeting this obligation, the University's online portals should allow employees, students and alumni to update Personal Information directly.

If staff become aware or are notified that Personal Information in the University's possession is not accurate, the staff member must notify the area responsible for managing the Personal Information, and other areas that may have copies of the Personal Information, so that steps can be taken to correct the information.

For example: *The Faculty of Education sends a letter to a student using the address within Callista which is returned to sender and marked "Not at this address". Student Services should be notified so that the*

address can be removed and an email can be sent to the student reminding them to update their details.

10. SECURITY OF PERSONAL INFORMATION - [Privacy Policy principle 3.1]

Storage

The University must take such steps as are reasonable in the circumstances to protect Personal Information in its possession from misuse, interference, loss, and unauthorised access, modification or disclosure. Personal Information must only be made accessible to, and must only be accessed by, those University Personnel who have a need to access it to perform their duties.

Example: Student files in TRIM should only be accessible by University Personnel within the security group established by Records Management Office.

Hardcopy records containing Sensitive Information should be stored in locked furniture when not in use. Hardcopy staff or student files should not be left on desks when offices are unattended, or in places where they are visible to students or members of the public.

Destruction - [Privacy Policy principle 3.1]

If the Personal Information is no longer needed for the purpose it was collected, and the University is not otherwise required to retain the information under any law, regulation or code, that information must be destroyed in a secure manner or de-identified (e.g. *Territory Records Act 2001* (ACT); Australian Code for the Responsible Conduct of Research). Staff should seek advice from the Legal Office if assistance with understanding applicable laws is required.

11. DEALING WITH REQUESTS FOR ACCESS TO PERSONAL INFORMATION - [Privacy Policy principle 4.1, 4.3]

Requests from Individuals

Individuals are entitled to request access to their own Personal Information in writing or email without the need for a formal application under the *Freedom of Information Act 2016 (ACT)*.

Requests from lawyers (other than the University's lawyers)

Lawyers do not have a special right to access information held by the University. Personal Information must not be disclosed in response to a lawyer's request unless it is accompanied by written consent of the person to whom the information relates, or if required by law or a court/tribunal order.

An example where records **should not be released**:

The Faculty of Arts and Design receives a letter from a law firm requesting attendance and academic records pertaining to a former student. The letter states the documents are urgently required for a hearing in the ACT Supreme Court.

A letter of this nature should be accompanied by a subpoena from the court or written consent from the student concerned. **All Such Requests Should Be Forwarded to the University's Legal Office.**

The University may limit access

Documentation produced to third parties or individuals may be withheld or redacted if the University determines that access would not be appropriate. Permitted reasons include:

- unreasonable impact on the privacy of other individuals (e.g. personally identifying information of referees on a staff appointment file)
- the request for access is frivolous or vexatious

- documents are subject to confidentiality obligations or legal professional privilege, granting access would compromise the University in anticipated legal proceedings or commercially sensitive decision-making processes
- the release of the information may create serious risk of harm (*Health Records (Privacy and Access) Act 1997* (ACT)).

12. Responding to a data breach - [Privacy Policy principle 5.1]

If a University staff member becomes aware of or is alerted to a data breach, that staff member must immediately notify their line manager and the Privacy Officer. The University must take immediate action to contain the loss or unauthorised disclosure or access where possible (e.g. by stopping the unauthorised practice; recovering the records; advising persons who have received the information by mistake to destroy that information).

The breach will be entered on the University's Compliance Register. The Privacy Officer will investigate as necessary and determine what further steps are necessary, having regard to the Data Breach Plan.

B. Data Breach Response Procedure

Loss or unauthorised disclosure of Personal Information or Confidential Information ("data breach") may occur in a variety of ways. It may be inadvertent or deliberate or malicious, for example:

- mistakenly emailing Personal Information to the wrong person
- loss or theft of laptops, removable storage devices or physical files
- hacking of the University's DITM systems
- staff accessing Personal Information outside the requirements of their employment.

Summary of Procedure

Data breaches have the potential to result in harm to the individuals affected and expose the University to legal, financial or reputational risk.

There is no single method of responding to a data breach. Data breaches must be dealt with on a case-by-case basis, by undertaking an assessment of the risks involved, and using that risk assessment to decide the appropriate course of action.

There are five key steps to consider when responding to a breach or suspected breach:
STEP 1: Contain the breach and do a preliminary assessment
STEP 2: Evaluate the risks associated with the breach and mitigate those risks
STEP 3: Notification to OAIC and affected individuals
STEP 4: Notification to University insurer Unimutual
STEP 5: Prevent future breaches

1. Identification of a breach

An identified or suspected data breach must be responded to and reported to the University's Privacy Officer (privacy@canberra.edu.au) and the relevant data and/or information system stewards, in line with the Data Breach Plan and the University's data breach response procedures.

Where a serious data breach occurs these procedures, along with the University's Business Continuity Plan, including the Critical Incident Management Team (CIMT) Plan are to be followed.

Where a data breach is a public interest disclosure, refer to the Fraud and Corruption Control Plan

(incorporating the *Public Interest Disclosure Guidelines 2017* (ACT)).

Any immediate steps available to contain the breach must be identified and implemented in discussion with the Privacy Officer. Reducing the scale and impact of a data breach can prevent the need for notification to the OAIC. All known or suspected data breaches must still be notified internally to the University's Privacy Officer.

2. Assessment of a breach

Not all data breaches are serious, notifiable and/or place the University's reputation, commercial or legal interests at risk. Identification of the classification of the data which has been compromised will inform the assessment of the breach *[refer to the Data Classification Framework in Appendix 3.]*.

A breach which involves sensitive, personal health or commercial or legal information will usually be regarded as a serious breach.

The University's Privacy Officer will seek information to assess the suspected breach. In assessing a suspected breach, the Privacy Officer may require assistance and information from other areas of the University depending on the circumstances.

Notifiable Breach

If, after an initial investigation, the Privacy Officer suspects a notifiable data breach may have occurred, a reasonable and expeditious assessment must be undertaken to determine if the data breach is likely to result in serious harm to any individual affected.

An assessment of a known or suspected breach must be conducted expeditiously and where possible should be completed within 30 days. The assessment must include:

1. an evaluation of the scope and possible impact of the breach;
2. determination if the breach is likely to be notifiable; and
3. a plan of action to minimise harm including, if required, notification to the OAIC.

Actions must be documented and acted upon as soon as possible.

Commercial or Legal Information

These breaches are not notifiable unless the information also contains Personal Information. The Privacy Officer must assess this possibility as well as the risk to the University's reputation and legal interests to determine if the breach is serious. The Business Continuity Plan, including the Critical Incident Management Team (CIMT) Plan are to be followed if that determination is made.

Notification to Insurer

If a breach comes within the criteria required by our insurer (see relevant Product Disclosure Statement Part 6 – Cyber Protection) notification to Unimutual must occur as stipulated in that policy.

3. A notifiable breach

A breach which is assessed as likely to result in serious harm to individuals whose Personal Information is involved, is a notifiable data breach. Such data breaches must be notified to the affected individuals and the OAIC as soon as possible.

Notice must include information about the breach and the steps taken in response to the breach. Please

note that notification to the OAIC and internally within the University is the **responsibility of the Privacy Officer.**

The risk of serious harm will be assessed by considering both the *likelihood* of the harm occurring and the *consequences* of the harm. Some of the factors that should be considered are:

Factors	Considerations
The type of Personal Information involved in the data breach	Some kinds of Personal Information are more sensitive than others and could lead to serious ramifications for individuals if accessed. Information about a person's health, documents commonly used for identity fraud (e.g. Medicare card, driver's licence, Tax File Number) or financial information are examples of information that could be misused if the information falls into the wrong hands.
Circumstances of the data breach	The scale and size of the breach may be relevant in determining the likelihood of serious harm. The disclosure of information relating to a large number of individuals would normally lead to an overall increased risk of at least some of those people experiencing harm. The length of time that the information has been accessible is also relevant. Consideration must be given to who may have gained unauthorised access to information, and what their intention was (if any) in obtaining such access. It may be that there was a specific intention to use the information in a negative or malicious way.
Nature of possible harm	Consider the broad range of potential harm that could follow from a data breach including: • identity theft • financial loss • threat to a person's safety • loss of business or employment opportunities and • damage to reputation (personal and professional).

Notifications will follow the format identified by the OAIC in Data breach notification – A guide to handling personal information security breaches.

4. Prevention and Response team

The Critical Incident Management Team (CIMT) will be formed for a serious breach in accordance with the University's Business Continuity Plan and related CIMT Plan.

The Deputy Vice Chancellor and Vice-President responsible for Data Security will be informed when a CIMT is established.

5. Breaches that are not serious

Breaches that are not assessed as serious breaches must be reported to the Privacy Officer and may be handled by supervisors in consultation with the University's Legal Office.

6. Records

Information about data breaches and documentation will be stored in the University of Canberra Compliance Register for each suspected breach.

APPENDIX 3

Data Classification Schedule

Purpose

This Data Classification Schedule is the University of Canberra's framework for assessing data sensitivity and the treatment of associated risks in the storage and uses of that data. It has been created to help the University's community to effectively manage information on a daily basis.

1. System owner responsibilities

Physical and logical access to systems may be granted by the system owner if access is appropriately controlled, and formal procedures are implemented to permit access to the system.

The allocation and use of system privileges must be restricted and controlled. A formal review of user privileges must be conducted on a regular basis to ensure that these remain appropriate. Accounts that are no longer required or appropriate must be closed or disabled.

When users leave the University, University access must be removed. When users change roles, access rights on systems must be reviewed and adjusted appropriately.

2. User responsibilities

Portable computing devices owned by the University, or that contain non-public University information, must be physically secured when unattended by either; locked drawer or cabinet.

Users will:

- Appropriately classify emails and documents sent externally
- Store documents in locations appropriate to the data classification level (do not store University data in non-University systems, i.e Dropbox)
- Adhere to the treatment of risk actions required by the data classification level.

3. Classifications and Levels of Protection

All University of Canberra Systems must include Access control and Asset management measures to classify data and mitigate risk of data breach. The minimum level of protection necessary when performing certain activities is based on the classification of the information being handled.

Most information does not need increased security and may be marked 'Public' or left unmarked. This should be the default position for newly created material, unless there is a specific need to protect the confidentiality of the information.

University employees, and other covered individuals, staff and affiliates are to determine in which circumstances security classifications are to be applied to its information. Review by the relevant supervisor, Data Owner or Data Steward may be appropriate.

Individuals are not entitled to access information merely because it would be convenient for them to know or because of their status, position, rank, or level of authorised access. Sensitive and Highly Sensitive classified information has special handling requirements, especially during electronic transmission or physical transfer. Further it is only to be used and stored in physical and electronic environments that provide a fitting level of protective security.

Data Classification Assessment

Data Classification	Description of Risk	Examples	Treatment of Data Risk
Highly Sensitive	Data that if accessed without authority would have a **high** impact on the University's activities and objectives.	• Data subject to regulatory control • Legal Advice (subject to legal professional privilege) • Personal information about Persons under age of 18 • Credit card details • Personal health records and clinical trial data • Campus security data • Personnel and/or payroll records • Student records • Data classified under the Australian government security classification system as confidential or higher (refer to www.protectivesecurity.gov.au) • Data belonging to a third party • Contracts and commercial in confidence • Patent information.	• Dissemination is restricted on a need to know basis, and may only be accessed, transmitted, modified, or stored for legitimate academic, research or business purposes. • Hard copies must be stored in a locked drawer, cabinet, room or area where access is controlled or has sufficient access control measures. • Must be protected to prevent loss, theft, malicious activity, unauthorised access and/or unauthorised disclosure. • Electronic copies must be stored on a system that requires University of Canberra based user authentication. • Electronic copies must be encrypted when transferring to an external entity or recorded to an external data storage device.

			• Must not be stored on non-University of Canberra managed storage (that is storage which the University does not have a contract for) (includes Office 365 but excludes Dropbox, Google Drive). • When emailed must include classification and appropriate disclaimer.

Sensitive/ Private	Data that if breached would have a low or medium impact on the University's activities and objectives.	• Sensitive or Personal Information about Students or Staff • Organisational financial data pre-Annual Report • Exam material and results • Internal planning documents • Research data (containing Personal Information) • Data considered commercial in confidence Business unit process and procedure • Unpublished intellectual property • ITC system design and configuration information • Limited range of Personal Information – e.g. student numbers	• Dissemination of this data is based on strict academic, research or business need. • Encryption is required for the transmission of sensitive data. • Must be protected to prevent loss, theft, malicious activity, unauthorised access and/or unauthorised disclosure. • Must be protected by confidentiality agreements before access is permitted to third parties. • Hard copies of sensitive data must be stored in a closed container (filing cabinet, closed office, secure area etc.). • Sensitive data in electronic format must be stored on a system that requires user authentication. • When emailed must include classification and appropriate disclaimer. • Must not be stored on non-University of Canberra managed storage (that is storage which the University does not have a contract for) (includes Office 365 but excludes Dropbox, Google Drive).

Public (Unclassified)	Data that if breached would have an insignificant or minor impact on the University's activities and objectives.	• Faculty and staff directory Information about Course listings or Unit outlines • Published research data • publicly posted press releases • published research data • marketing materials • job announcements	• Public data is available to all members of the the University's community and all individuals and outside entities. • Encryption is not required for the transmission.

3. Alignment with Government Security Classification

The University of Canberra does not use dissemination limiting markers (DLMs) in its Data Classification. Alignment to the Australian Government and ACT Government security classification systems as follows:

University of Canberra	Commonwealth	ACT
Public	Information not requiring additional protection	Unclassified
		FOR OFFICIAL USE ONLY (OR FOUO)
Sensitive/Private	CONFIDENTIAL	SENSITIVE
		SENSITIVE:LEGAL
		SENSITIVE: PERSONAL
Highly Sensitive	SECRET	SENSITIVE: AUDITOR-GENERAL
NA	TOP SECRET	SENSITIVE: CABINET

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.