

Privacy and Confidentiality Policy

POLICY STATEMENT

This document sets out a framework for the protection of personal privacy and confidentiality consistent with the University's obligations and commitment to protecting the privacy of all members of the University community.

The University will act responsibly to collect, manage, use and disclose personal information in accordance with the Northern Territory [Information Act 2002](#).

POLICY PRINCIPLES

1. Collection of Personal Information

- 1.1. The University will only collect personal information that is necessary for one (1) or more of its functions or activities.
- 1.2. The University will only collect personal information in a lawful, fair and not unreasonably intrusive way.
- 1.3. When personal information is collected from an individual, the University will take reasonable steps to ensure that the individual is:
 - Aware of the University's identity and how to contact it;
 - Able to have access to the information;
 - Aware of the purpose for which the information is collected;
 - Aware of the persons or bodies, or classes of persons or bodies, to which the University usually discloses personal information;
 - Aware of any law that requires the collection of the information; and
 - Aware of any consequences for the individual if they do not provide all or part of the information.
- 1.4. If it is reasonable and practical to do so, the University will only collect personal information about an individual from that individual. If the University collects personal information about an individual from another person, it will take reasonable steps to ensure the individual is or has been made aware of the matters listed above unless making the individual aware of these matters would pose a serious threat to the life or health of a person.
- 1.5. The University may use and disclose personal information only in the following instances, after a written note of the use or disclosure is made:
 - The use or disclosure is related or directly related to the purpose for collecting it and the individual would reasonably expect the University to use or disclose it for that purpose;
 - With the individual's consent;
 - The use or disclosure is necessary for research or the compilation or analysis of statistics in the public interest, and:
 - Only where the research will not be published in identifiable form; and



- The individual's consent cannot be reasonably obtained; and
- The recipient of the information will not disclose the personal information; and
- Where any health information is only used or disclosed in accordance with guidelines issued by the Information Commissioner under section 86(1)(a)(iv) of the [Information Act](#).
- To lessen or prevent a serious and imminent threat to a person's life, health or safety, or of harm to or exploitation of a child, or serious threat to public health or safety;
- When required in the investigation or reporting of unlawful activity, or assisting a law enforcement agency;
- Where the use or disclosure is required or authorised by law; or
- In connection with the performance of the functions of the Australian Security Intelligence Office (ASIO) or Australian Secret Intelligence Service (ASIS) where authorised in writing.

2. Trans-border data flows

2.1. The University will not transfer personal information about an individual to a person (other than the individual) outside the Northern Territory unless:

- The transfer is required or authorised under a law of the Northern Territory or the Commonwealth; or
- The University reasonably believes that the person receiving the information is subject to a law, or a contract or other legally binding arrangement, that requires the person to comply with principles for handling the information that are substantially similar to the Information Privacy Principles and Australian Privacy Principles; or
- The individual consents to the transfer; or
- The transfer is necessary for the performance of a contract between the organisation and the individual or for the implementation of pre-contractual measures taken in response to the individual's request; or
- The transfer is necessary for the performance or completion of a contract between the organisation and a third party, the performance or completion of which benefits the individual; or
- All of the following apply:
 - The transfer is for the benefit of the individual;
 - It is impracticable to obtain the consent of the individual to the transfer;
 - It is likely that the individual would consent to the transfer; or
- The organisation has taken reasonable steps to ensure that the information will not be held, used or disclosed by the person to whom it is transferred, in a manner that is inconsistent with the Information Privacy Principles or Australian Privacy Principles.

2.2. The University will ensure that any contracts with third parties where personal information may be transferred, contain privacy clauses requiring compliance with the [Information Act](#) and the Information Privacy Principles and/or the [Privacy Act](#) and the Australian Privacy Principles.

3. Data Quality

3.1. The University will take all reasonable steps to ensure that the personal information it collects, uses or discloses is accurate, complete and up to date.

4. Data Breaches



- 4.1. The Notifiable Data Breach Scheme, as detailed in the [Privacy Act](#) requires regulated entities to notify affected individuals and the Australian Information Commissioner about the occurrence of eligible data breaches.
- 4.2. As soon as possible after the breach has occurred, all suspected eligible data breaches must be referred to the University's [Privacy Officer](#) for actioning and reporting as they deem appropriate.

5. Information Security

- 5.1. The University will protect all personal information it holds from misuse, loss, unauthorised access, modification or disclosure by:
 - Implementing industry standards for the security and protection of personal information; and
 - Storing information in either electronic and/or hard copy forms with access restricted to authorised personnel only.
- 5.2. Security, integrity and accuracy of information is governed by the University's [Information and Communication Technologies Security Policy](#) and [Records Management Policy](#) and related procedures.
- 5.3. The University will take reasonable steps to destroy or permanently de-identify personal information if it is no longer needed for any purpose in accordance with the [Records Management - Retention and Disposal of University Records Procedure](#) and Disposal Schedules.

6. Privacy and Confidentiality Obligations

- 6.1. Staff members, students, researchers, contractors and any other third party who collect use or disclose personal information on behalf of the University have a responsibility to act consistent with the Information Privacy Principles and Australian Privacy Principles and to take appropriate measures to avoid a breach of confidence.
- 6.2. Under the [Higher Education Support Act](#), it is an offence (punishable by fine or imprisonment), if a staff member of the University discloses, copies or records personal information otherwise than in the course of official employment, or causes unauthorised access to or modification of personal information held by the University.
- 6.3. At any time during and after employment with the University, staff members must not use, divulge, copy or communicate any confidential information to any person without the University's consent, regardless of whether the other person is an employee of the University or not, except as required in the ordinary performance of the staff member's duties.
- 6.4. Unauthorised access to personal information must be reported to the University's [Privacy Officer](#) and, where relevant, to the responsible owner of the information system concerned. Failure to comply with this Policy may necessitate disciplinary action.
- 6.5. University matters relating to individuals or non-public information must not be discussed, except where directly related to the staff member's role, as this may constitute a breach of confidence and therefore misconduct.

7. Information and Communication Technologies Facilities

- 7.1. Users of the University's Information and Communication Technologies (ICT) facilities are reminded that anything that is written or recorded is potentially subject to subpoena or Freedom of Information requests or other authorised access. Inappropriate use of the University's Information and Communication Technologies (ICT) facilities may be subject to disciplinary action.

8. Access and Correction

- 8.1. On the request of an individual, the University will take reasonable steps to inform the individual of the kind of personal information it holds, why it holds the information and how it collects, holds, uses and discloses the information.
- 8.2. On the request of an individual, the University will provide access to their personal information, except to the extent that:



- Providing access would pose a serious threat to the life or health of the individual or another individual; or
- Providing access would prejudice measures for the protection of the health or safety of the public; or
- Providing access would unreasonably interfere with the privacy of another individual; or
- The request for access is frivolous or vexatious; or
- The information relates to existing or anticipated legal proceedings between the University and the individual and the information would not be accessible by the process of discovery or subpoena in those proceedings; or
- Providing access would reveal the intentions of the University in relation to negotiations with the individual in such a way that would prejudice the negotiations; or
- Providing access would be unlawful; or
- Denying access is required or authorised by law; or
- Providing access would be likely to prejudice an investigation of possible unlawful activity; or
- Providing access would be likely to prejudice one or more of the following by or on behalf of a law enforcement agency:
 - Preventing, detecting, investigating, prosecuting or punishing an offence or a breach of a prescribed law;
 - Enforcing a law relating to the confiscation of proceeds of crime;
 - Protecting public revenue;
 - Preventing, detecting, investigating or remedying seriously improper conduct or prescribed conduct;
 - Preparing for or conducting proceedings in a court or tribunal or implementing the orders of a court or tribunal; or
- Providing access would prejudice:
 - The security or defence of the Commonwealth or a State or Territory of the Commonwealth; or
 - The maintenance of law and order in the Territory.

8.3. However, where providing access would reveal evaluative information generated within the University in connection with a commercially sensitive decision-making process, the University may give the individual an explanation for the commercially sensitive decision rather than access to the decision.

8.4. If the University holds personal information about an individual and the individual establishes that the information is not accurate, complete or up to date, the University will take reasonable steps to correct the information so that it is accurate, complete and up to date.

8.5. If an individual and the University disagree about whether personal information about the individual held by the University is accurate, complete or up to date; and

- The individual requests the University to associate with the information a statement to the effect that, in the individual's opinion, the information is inaccurate, incomplete or out of date;
- The University will take reasonable steps to comply with that request.

8.6. The University will provide reasons for refusing to provide access to or correct personal information.

8.7. If an individual requests the University for access to, or to correct personal information held by the University,



the University will, within a reasonable time:

- Provide access or reasons for refusing access; or
- Make the correction or provide reasons for refusing to make it; or
- Provide reasons for the delay in responding to the request;

8.8. If the University charges a fee for providing access to personal information, the fee will not to be excessive. Access and amendment requests should be directed to the University's [Privacy Officer](#).

9. Notification of correction to third parties

9.1. If the University corrects personal information that the University previously disclosed to another entity, and the individual requests the University to notify the other entity of the correction, the University will take such steps as are reasonable in the circumstances to give that notification unless it is impracticable or unlawful to do so.

10. Sensitive Information

10.1. The University will not collect sensitive information about an individual unless:

- The individual consents to the collection; or
- The University is authorised or required by law to collect the information; or
- The individual is:
 - Physically or legally incapable of giving consent to the collection; or
 - Physically unable to communicate his or her consent to the collection; and
 - Collecting the information is necessary to prevent or lessen a serious and imminent threat to the life or health of the individual or another individual; or
- Collecting the information is necessary to establish, exercise or defend a legal or equitable claim.

10.2. However, the University may collect sensitive information about an individual if:

- The collection:
 - Is necessary for research, or the compilation or analysis of statistics, relevant to government funded targeted welfare or educational services; or
 - Is of information relating to an individual's racial or ethnic origin and is for the purpose of providing government funded targeted welfare or educational services; and
- There is no other reasonably practicable alternative to collecting the information for that purpose; and
- It is impracticable for the organisation to seek the individual's consent to the collection.

11. Complaints

11.1. Questions in relation to concerns about privacy, the University's management of personal information, or to make a complaint, should be directed to the University's Privacy Officer or the Northern Territory Information Commissioner.

NON-COMPLIANCE

Non-compliance with Governance Documents is considered a breach of the [Code of Conduct](#) and is treated seriously



by the University. Reports of concerns about non-compliance will be managed in accordance with the applicable disciplinary procedures

All staff members have an individual responsibility to raise any suspicion, allegation or report of bribery or improper conduct in accordance with the [Fraud and Corruption Control Policy](#) and [Whistleblower reporting \(Improper Conduct\) Procedures](#)

EXPLANATORY NOTES

RELATED AND SUPPORTING DOCUMENTS

Legislation	Charles Darwin University Act Higher Education Support Act 2003 (Commonwealth) Information Act 2002 (NT) Information Regulations 2010 (NT) National Statement on Ethical Conduct in Human Research 2015 (Commonwealth) Privacy Act 1988 (Commonwealth) Privacy Amendment (Enhancing Privacy Protection) Act 2012 (Commonwealth)
Policy	Email Acceptable Use Policy Information and Communication Technologies Acceptable Use Policy Information and Communication Technologies Security Policy Quality Policy Records Management Policy
Procedures	Identifying Unacceptable Use of Information and Communication Technologies Procedures
Definitions	CDU Glossary



GOVERNANCE

Owner	Director Strategic Services and Governance	
Category	Corporate	
Audience	Staff and Students	
Approving authority	Vice-Chancellor	
Effective date	1 December 2020	
Review date	30 November 2023	
Version	4.00	Pol - 032
	Document history and version control maintained separately.	
Content enquiries	governance@cdu.edu.au	

