Privacy and Confidentiality Policy

INTRODUCTION

The University is committed 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*.

The University also commits to comply with the Commonwealth *Privacy Act*, as if it were a Commonwealth organisation where required to abide by the Australian Privacy Principles under contracted funding agreements from Commonwealth agencies and the *Higher Education Support Act* when handling students' personal information.

STATEMENT OF AUTHORITY

The authority behind this policy is the *Charles Darwin University Act 2003* part 3, section 15.

COMPLIANCE

This is a compliance requirement under the *Information Act 2002* and *Privacy Act 1988*.

INTENT

This document sets out a framework for the protection of personal privacy and confidentiality consistent with the University's obligations to comply with the Northern Territory Information Privacy Principles (IPPs), the Australian Privacy Principle and obligations of confidence.

RELEVANT DEFINITIONS

In the context of this document

Australian Privacy Principles (APPs) means the principles that set out standards, rights and obligations in relation to handling, holding, accessing and correcting personal information as contained in Schedule 1 of the *Privacy Act 1988*;

Eligible data breach means a breach of personal data security that is likely to result in serious harm to any of the individuals to whom the data relates, and the University has been unable to prevent the likely risk of serious harm with remedial action;

Consent means, according to the *National Statement on Ethical Conduct in Human Research* and Privacy Law, agreement that is informed, specific, current and voluntary;

Governance documents means formally approved documents that outlines non-discretionary governing principles and intentions, in order to guide University practice. Governance documents are a formal statement of intent that mandate principles or standards that apply to the University's governance or operations or to the practice and conduct of its staff and students. They include the CDU Act, by-laws, policies, procedures, guidelines, rules, codes and the Enterprise Agreement;

Information Privacy Principles (IPPs) means the rules for the collection, handling, access and correcting of personal information (including sensitive information) as contained in Schedule 2 of the *Information Act* ;

Information and Communication Technologies (ICT) means communications, computers, enterprise software, middleware, storage, and audio-visual systems which enable users to access, store, transmit, and manipulate information;

Notifiable Data Breach Scheme means established requirements for entities to notify individuals and the Australian Information Commissioner of eligible data breaches, as per the *Privacy Act 1988* .

Person means an individual and includes a deceased individual within the first five (5) years after death;

Personal information means information prescribed in section 4A of the *Information Act* that is government information that discloses a person's identity or from which a person's identity is reasonably ascertainable, except to the extent that:

- The person's identity is disclosed only in the context of having acted in an official capacity for the University or another public sector organisation; and
- The government information discloses no other personal information about the person;

Public sector organisation means an organisation prescribed in section 5 of the *Information Act* and includes the University;

Sensitive information means information prescribed in section 4 of the *Information Act* relating to racial or ethnic origin, political opinions or membership of a political association, religious beliefs or affiliations, philosophical beliefs, membership of a professional or trade association, membership of a trade union, sexual preferences or practices, a criminal record, or health information;

Staff member means anyone employed by the University and includes all continuing, fixed-term, casual, adjunct or honorary staff or those holding University offices or who are a member of a University committee;

Student means a person prescribed as a student of the University in By-law 2 of the *Charles Darwin University (Student of the University) By-laws*; and

University community means officials and individuals carrying out University business. This includes, but is not limited to, all staff members, researchers, peer reviewers, students, volunteers, consultants, agents and contractors.

POLICY

Collection of Personal Information

The University will only collect personal information that is necessary for one (1) or more of its functions or activities.

The University will only collect personal information in a lawful, fair and not unreasonably intrusive way.

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.

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.

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.

Trans-border data flows

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.

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.

Data Quality

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.

Data Breaches

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.

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.

Information Security

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.

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.

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*.

Privacy and Confidentiality Obligations

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.

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.

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.

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.

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.

Information and Communication Technologies Facilities

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.

Access and Correction

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.

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.

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.

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.

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.

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

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;

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*.

Notification of correction to third parties

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.

Sensitive Information

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.

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.

Complaints

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

Members of the University community must be aware of and note that the University regards any activity, which constitutes unacceptable access, use or disclosure as potentially serious matters that the University may determine as misconduct or serious misconduct. Non-compliance with this policy may result in disciplinary action and/or reference to law enforcement agencies in accordance with the relevant legislation and University Governance Documents.

ESSENTIAL SUPPORTING INFORMATION

Internal

Charles Darwin University Act

Data Breach Response Plan

Disposal Schedules

Email Acceptable Use Policy

Identifying Unacceptable Use of Information and Communication Technologies Procedures

Information and Communication Technologies Acceptable Use Policy

Information and Communication Technologies Security Policy

Quality Policy

Records Management Policy

External

Higher Education Support Act 2003 (Commonwealth)

Information Act 2002 (NT)

Information Regulations 2010 (NT)

National Stament on Ethical Condut in Human Research 2015 (Commonwealth)

Privacy Act 1988 (Commonwealth)

Privacy Amendment (Enhancing Privacy Protection) Act 2012 (Commonwealth)

Document History and Version Control

Last amendment:	02 May 2018	**Next Review:**	Dec 2020
Sponsor:	Director, Strategic Services and Governance		
Contact Officer:	Director, Strategic Services and Governance		

Version	Date Approved	Approved by	Brief Description
1.00	04 May 2017	Council	Creation of original document and upload to CDU website.
1.01	08 Feb 2010	Governance	• Change old policy into new format style. • Add statement of authority, relevant definitions, document history and version control and essential documents in keeping with new policy format. • Amend minor grammatical and spelling errors. • Amend Audit and Risk Committee to Finance, Risk and Review Committee to reflect change in committee title • Change Staff Services to PMD to reflect title change
1.02	29 Dec 2010	Governance	• Convert document to new template • Amend PMD to Office of Human Resource Services to reflect title change. • Corporate Services changed to Director, Strategic Services and Governance to reflect position responsibility change. • Senior staff changed to Senior Executive. Definition added. • Definition of Senior Manager added
1.03	28 Jan 2011	Governance	• Minor changes to spelling, grammar and formatting.
1.04	10 Jan 2012	Governance	• Amended position titles in accordance with new organisational chart. • Update hyperlinks • Minor changes to grammar and formatting • Removal of reference to Finance, Risk and Review Committee as no longer active
1.05	13 Feb 2013	Governance	• Converted document to new template • Updated and added hyperlinks • Minor changes to wording, formatting and grammar • Assigned document number • Added relevant definitions • Removed general responsibilities section
2.00	27 Aug 2014	Vice Chancellor	• Major review of Policy in line with NT Information Act • Privacy Policy changed to Information Privacy Policy in line with NT Information Act • Definition of Senior Executive amended to reflect changes to position titles

			• Definition of Sensitive Information updated to reflect definition in the Act • Additional definitions
2.01	27 Oct 2014	Governance	• Correction of minor grammatical errors and sentence structure • Addition of - To establish an individual's identity for the purposes of access to ICT systems under Collection of Personal or Other Information
2.02	05 Jul 2017	Governance	• Conversion to new Governance template due to new University branding • Updated definitions for senior executive, senior manage and staff member • Updated hyperlinks • Change title of reference from Northern Territory Government and Archives Management standards to Northern Territory Government Records Management Standards
3.00	13 Dec 2017	Governance	• Review and amend document for compliance with the Commonwealth Privacy Act and HESA ; • Amend name from Information Privacy Policy to Privacy and Confidentiality Policy • Add definitions for APPs, ICT, person, public sector organisation, student, university community • Amendment to definitions of IPPs, personal information, sensitive information and staff members, • Remove definitions for cookies, privacy, researcher, senior executive, senior manager and third party • Remove overseas disclosure paragraph and replace with trans-border data flows paragraph • Conversion to new template due to new University branding • Updated Hyperlinks
3.01	24 Jan 2018	Governance	• Removed duplicated paragraph
3.02	02 May 2018	Vice-Chancellor	• Addedd definitions for Eligible data breach and Notifiable Data Breach Scheme • Amended text to include a paragraph re the reporting of data breaches • Minor rewording Collection of Personal Information