Investigating Unacceptable Use of ICT Procedure

Section 1 - Preamble

(1) Charles Darwin University ('the University', 'CDU') has an obligation to ensure appropriate security for all Information and Communication Technology (ICT) data, equipment, and processes in its domain of ownership and control so that information can be protected to a level commensurate with its value to the organisation, while still being made available to those who need it.

(2) CDU routinely gathers, stores, maintains, processes, transmits and disposes of records containing information that must be protected. This information plays a vital role in supporting the University's business processes and customer services, by contributing to operational and strategic business decisions and in conforming to legal and statutory requirements.

Section 2 - Purpose

(3) This procedure provides definitive instruction on the investigations of possible breaches of the Information and Communication Technologies Acceptable Use Policy. This procedure enacts the principles of the Information Security and Access Policy.

Section 3 - Scope

(4) This procedure applies to all staff members and students, to all University associates and members of the University community with access to CDU ICT equipment and resources, and to all clients of ICT equipment owned or leased by the University.

(5) This procedure also applies to all information assets encompassing facilities, data, software, paper documents and personnel, and to all equipment connected to the University's data and voice networks.

Section 4 - Procedures

(6) The Chief Information and Digital Officer/Chief Information Security Officer (CIO/CISO) is responsible for authorising and overseeing all monitoring of CDU ICT systems and all investigations of suspected unacceptable use of ICT.

(7) Unacceptable use of ICT systems is defined in the Information and Communication Technologies Acceptable Use Policy.

(8) All information, files, records and data accessed by authorised ITMS staff must be treated as confidential and may only disclosed to relevant third parties as required, in line with CDU's Privacy Policy.

Detection

(9) The Information Technology Management System (ITMS) team and authorised external parties will perform regular monitoring of the University's information and communication technologies and report any suspected unacceptable

use of ICT to the CIO/CISO.

(10) All ICT users are required to report suspected unacceptable use of ICT and breaches of the Information Security and Access Policy to their supervisor, lecturer, manager or directly to DTS.

(11) All reports of suspected unacceptable use of ICT will be forwarded to the CIO/CISO, who will determine whether an investigation is warranted.

Suspected Infringement

(12) If unacceptable use of ICT is suspected or identified during of regular ICT monitoring, or after receiving a report of or a request for investigation into suspected unacceptable use of the ICT, the CIO/CISO will direct specific staff member or request an authorised external party to monitor the suspected user and their accounts.

(13) A specific staff member is a member of the ITMS team authorised by the CIO/CISO to investigate cases of suspected unacceptable use. The specified staff member may undertake specific actions (for example, accessing personal files or monitoring internet use) against specified users within the scope and for the duration of the investigation. The specified staff member may not undertake further actions or investigate other users without the approval of the CIO/CISO, and all such actions must cease once the investigation is concluded.

(14) The specified staff member or external party will investigate all relevant ICT assets, including but not limited to computer systems, applications, log data, usage history, and cache files, and provide all relevant data to the CIO/CISO for review and assessment.

(15) If the CIO/CISO determines that unacceptable use has occurred, they will produce a report for the relevant Member of the Vice-Chancellor's Advisory Committee regarding the nature and severity of the incident.

(16) In certain circumstances, such as finding evidence of criminal activity, the CIO/CISO is required to notify relevant statutory authorities. In these circumstances, notifying the statutory authorities takes precedence over notifying and reporting to the University.

(17) The CIO/CISO will make recommendations on responding to the incident to the relevant Member of the Vice-Chancellor's Advisory Committee or statutory authority, who will determine what further actions, if any, are to be taken. This may include, but is not limited to:

a. a formal or informal reprimand;
b. further training on acceptable use of ICT;
c. temporary or permanent suspension of ICT user privileges;
d. suspension or termination of employment or enrolment;
e. referral of the incident to relevant statutory authorities, including police; and/or
f. any other response deemed appropriate to the situation.

(18) Responses to incidents will be proportional to the degree of non-compliance, and consideration will include matters such as whether the incident was intentional, whether the incident was illegal, and the degree of risk and/or damage caused by the incident.

(19) Consideration of responses to an incident will involve all relevant executives and responsible officers, and may include representatives or executives of People and Culture, Student Services and VET, Faculty Pro Vice-Chancellors, and direct line managers.

Immediate threat

(20) Where a user's actions pose an immediate threat to the security of the University through its ICT systems the CIO/CISO will:

a. take immediate action to mitigate the potential risk to the University;
b. consider the available evidence and determine whether or not to commission an investigation into the matter;
c. make a recommendation on the severity of the infringement, in consultation with the relevant Member of the Vice-Chancellor's Advisory Committee; and
d. report the matter to the relevant authorities or agencies as require

Record keeping

(21) The University must keep a record of:

a. all investigations into suspected infringement where unacceptable use is identified;
b. all suspected and unusual ICT activity that may indicate that unacceptable use is taking place.

(22) Records are to be maintained in accordance with the Records and Information Management Policy and Procedure and associated procedures.

Section 5 - Non-Compliance

(23) Non-compliance with Governance Documents is considered a breach of the Code of Conduct – Staff or the Code of Conduct – Students, as applicable, and is treated seriously by the University. Reports of concerns about non-compliance will be managed in accordance with the applicable disciplinary procedures outlined in the Charles Darwin University and Union Enterprise Agreement 2025 and the Code of Conduct – Students.

(24) Complaints may be raised in accordance with the Code of Conduct – Staff and Code of Conduct - Students.

(25) All staff members have an individual responsibility to raise any suspicion, allegation or report of fraud or corruption in accordance with the Fraud and Corruption Control Policy and Whistleblower Reporting (Improper Conduct) Procedure.

Status and Details

Status	Historic
Effective Date	15th January 2022
Review Date	29th November 2024
Approval Authority	Vice-Chancellor
Approval Date	1st December 2021
Expiry Date	27th April 2026
Responsible Executive	Penny Szybiak Vice-President Corporate
Implementation Officer	Andrew Tully Chief Information and Digital Officer
Enquiries Contact	Andrew Tully Chief Information and Digital Officer

This policy document may be varied, withdrawn or replaced at any time. Printed copies, or parts thereof, are regarded as uncontrolled and should not be relied upon as the current version. It is the responsibility of staff printing this document to always refer to the Governance Document Library for the latest version.