Information and Communication Technologies Acceptable Use Policy

Section 1 - Preamble

(1) Charles Darwin University ('the University', 'CDU') provides information and Communication Technology (ICT) to support its functions and activities and is committed to ensuring those resources are used in a transparent and accountable manner. All members of the University community have a responsibility to use University ICT resources in a manner consistent with this commitment. Failure to meet this commitment may result in the introduction of threats that may impact the productivity, security and reputation of the University.

Section 2 - Purpose

(2) This policy articulates the expectations for the acceptable use of the University's ICT systems.

Section 3 - Scope

(3) This policy applies to all people granted access to the University's ICT systems, including staff, students, and other members of the University community, including honorary appointees, visitors, and volunteers.

(4) This policy also applies to all users of ICT equipment under the management or control of the University, and all equipment connected to the University's data and voice networks.

Section 4 - Policy

University user account responsibilities

(5) Users are responsible for any activity, transaction or publication of information which originates from their University account. A user must not perform any act that prejudices the security of their University user account, including disclosing their password to any other person or allowing another person to use their account.

(6) Users who inadvertently receive or access unacceptable material must take immediate action to cease such access and make a report to DTS.

Use of information and communication technology (ICT) resources

(7) The University provides ICT resources to support education, research and work purposes and expects that these resources will only be utilised for the appropriate and legitimate performance of these activities. Acceptable use of the University's ICT resources is any use that:

a. is consistent with Commonwealth, state and territory laws;
b. meets expectations of the Code of Conduct - Employees and Code of Conduct - Students, as applicable;
c. complies with any lawful direction provided by a university officer or an authorised office under the Charles

Darwin University Act 2003; and

d. maintains the security of the University's ICT resources and facilities.

(8) Unacceptable use of the University ICT resources is any use that:

a. breaches any Commonwealth, state and territory laws;
b. breaches the University's behavioural expectations, including not complying with the Code of Conduct - Employees or the Code of Conduct - Students;
c. disobeys any lawful direction provided by a University officer or an authorised officer under the Charles Darwin University Act 2003;
d. includes receiving, accessing, downloading, displaying, transmitting and/or making unacceptable material via any media including personal storage devices connected to a University network;
e. overloads or monopolises ICT resources in a manner which adversely affect other users, including unauthorised sending of electronic messaging to a large number of recipients that may initiate a service disruption;
f. breaches the University's expectations regarding personal responsibility for a user's account, including sharing authentication credentials or permitting others to access systems under their identity;
g. acts in a manner that compromises the security, confidentiality, integrity and availability of ICT resources;
h. contravenes software End User Agreements including copying software without authorisation from the copyright holder; and/or
i. constitutes excessive personal use of ICT resources.

Acceptable use of electronic mail

(9) Access to a University email account is provided for the purpose of sending and receiving emails related to the performance the user's work, studies or University responsibilities. Emails may constitute University records and must be managed in accordance with University recordkeeping requirements.

(10) Users of University email services are expected to respect the standards of courtesy and professionalism that apply to all University communications and to avoid aggressive or abusive messages, messages that could reasonably be viewed by others as offensive or objectionable, or messages containing content that is obscene.

Incidental personal use

(11) The University recognises that ICT resources may be used for incidental personal use. Incidental use must be infrequent, minimal, and must not interfere with University operations, employee performance, or study. Incidental personal use does not include the following:

a. maintaining or supporting a personal private business;
b. recruitment of members to, or soliciting donations for, political parties or religious groups;
c. transmission, viewing or publication of unacceptable material;
d. publication of internet sites or pages unrelated to university activities;
e. personal observations using inappropriate or offensive language or images;
f. downloading, uploading, accessing or sharing copyright material and media; and
g. any malicious or unlawful purpose.

Use of ICT resources for approved activities

(12) The University acknowledges that, as part of their employment or studies, staff and students may be required to use ICT resources to access unacceptable materials. Users must ensure approval for such activities is provided by the relevant Pro Vice-Chancellor or head of division and subsequently registered with DTS prior to access or use occurring.

Monitoring and detection

(13) The University may capture and inspect data stored or transmitted on ICT facilities for the purpose of maintaining system security, integrity, and investigating potential security incidents. This data is used to maintain system security and integrity and to prevent, detect or minimise unacceptable behaviour and may include information relating to user activity, including email and internet usage, file operations and content stored on connected storage devices.

Section 5 - Non-Compliance

(14) Non-compliance with governance documents is considered a breach of the Code of Conduct - Employees 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.

(15) Complaints may be raised in accordance with the Complaints and Grievance Policy and Procedure - Employees and Complaints Policy - Students.

(16) 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	Current
Effective Date	19th May 2026
Review Date	19th May 2029
Approval Authority	Vice-Chancellor
Approval Date	18th May 2026
Expiry Date	Not Applicable
Responsible Executive	Rick Davies Vice-President Corporate and Chief Financial Officer
Implementation Officer	Andrew Tully Chief Information and Digital Officer
Enquiries Contact	Andrew Tully Chief Information and Digital Officer

Glossary Terms and Definitions

"University" - Charles Darwin University, a body corporate established under section 4 of the Charles Darwin University Act 2003. The University is comprised of the various faculties, CDU TAFE, organisational units, and formal committees, including the governing University Council and Academic Board.

"Governance document" - means policy or procedure published in the Governance Document Library. Policies and procedures are collectively called ‘governance documents’ and are often referred to as ‘policy’ or ‘University policy’.