Identifying Unacceptable Use Of Information and Communication Technologies Procedures

Section 1 - Introduction

(1) The University Information and Communication Technologies Acceptable Use Policy lists the following activities as forms of unacceptable use of the University's Information and Communication Technologies ICT:

a. system abuse or misuse;
b. copyright infringement;
c. intentionally viewing, downloading, copying or storing pornography;
d. equipment abuse or misuse; and/or
e. security breaches.

(2) This document is to be used to supplement the Information and Communication Technologies Acceptable Use Policy and Email Acceptable Use Policy and associated procedures by giving further, detailed definitions of these activities.

Section 2 - Compliance

(3) This is a compliance requirement under the University's Code of Conduct.

Section 3 - Intent

(4) The intention of this document is to define and clarify what is deemed as unacceptable use of University Information and Communication Technologies and applies to all staff, students and authorised visitors of the University (collectively known as 'Users').

Section 4 - Relevant Definitions

(5) In the context of this document:

a. Adjunct or honorary staff means staff who are associated with the University by appointment under the Honorary Appointment Procedures and through the Nominations, Honorary Awards and Legislation Committee;
b. Alumni means graduates of the University or its predecessor institutions;
c. Authorised visitor means bona fide visitors that the University may, from time to time, provide with access to facilities to enhance their ability to complete tasks for the University or to liaise with the University. Such visitors may include, but are not limited to: alumni; external auditors or consultants; potential clients or business partners; contractors or vendors; volunteers, conference delegates; and students and staff of other universities with reciprocal arrangements;
d. Copyright infringement means contravening the international legal protection of intellectual property protection

by breaching copyright, as defined in the Copyright Act 1968 (Commonwealth);

e. Defamatory material refers to the ordinary legal meaning;

f. Discriminatory material includes material, which may be of a sexist, racist, homophobic or otherwise prejudicial nature. Often it refers to content that stereotype, objectifies, patronises or threatens an individual or group of individuals because of their sex, race (including colour) nationality descent or ethnic background, religion, cultural background, gender identity, HIV/AIDS, industrial activity, marital status, parenthood, sexual orientation, pregnancy, age, physical features or disability. [Refer to Equal Opportunity Policy or contact the Complaints Management Unit for more information];

g. Information and Communication Technologies refers collectively to computers, printers, facsimiles, telephones (both mobile and landlines), scanners, photocopiers, e-mail, internet, intranet, web services, blogs, twitter, wiki, social networking sites such as, Facebook pages, portable electronic devices and any other similar resources;

h. ITMS means Information Technology Management and Support within the University;

i. Offensive or objectionable material includes material, which infringes socially accepted standards of good taste or good manners, such as insulting or aggressive language directed at another person or persons. This includes but is not limited to pornography;

j. Security breach means the use of computing facilities, which are controlled through a “user id” and access rights governed by a personal password or through the use of a staff or student card to areas such as computer labs. Passwords not kept confidential or allowing security cards to be used to permit access to University facilities for anyone other than the owner of the card are considered serious breaches of security. Users will be held responsible for unauthorised use of his or her privileges;

k. Senior Executive means a staff member of the University holding the position of Vice-Chancellor, Provost, Deputy Vice-Chancellor, Pro Vice-Chancellor or Chief Financial Officer or equivalent;

l. Senior Manager means a staff member of the University holding the position of Director or Head of School or equivalent;

m. 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;

n. 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;

o. Significant promulgation means the distribution of material to a wide audience; and

p. User means any staff, student enrolled at the University and authorised visitors to the University.

Section 5 - Procedures

Identifying and Defining Unacceptable Use

System Misuse

(6) Deliberate unauthorised access to facilities or data.

(7) Unauthorised use of data or information obtained from Information Systems.

(8) Violation of the privacy of personal information relating to individuals.

(9) Unauthorised disclosure of confidential or sensitive information (business or commercial) to unauthorised recipients.

(10) Use of University facilities to gain unauthorised access to third-party computing facilities.

(11) Transmission of unsolicited commercial advertising material or any other form of unsolicited commercial electronic message, including material commonly known as “spam”, or “junk e-mail”.

(12) Deliberate impersonation of another individual across the network by the use of their access, username, password, personal information or by any other means.

(13) Excessive downloading, storage, printing, scanning, photocopying or faxing of files or data not directly related to education or research, or required for the performance of the User's duties, or to meet the University's expectations of the User, or otherwise justified under the Information and Communication Technologies Acceptable Use Policy.

(14) Installing unauthorised software on University computers. [For the purposes of this document, "unauthorised software" includes games, applications or plug-ins that have not been cleared by ITMS].

(15) Intentionally downloading unauthorised materials such as:

a. software;
b. lengthy files containing picture images; and/or
c. live pictures or graphics is prohibited.

(16) This includes computer games, music files, feature films and accessing of radio or television stations broadcasting via the Internet.

System Abuse

(17) Deliberate, unauthorised corruption or destruction of ICT systems or data, including deliberate introduction or propagation of computer viruses or malicious software (for example worms, sniffers or any other virus), which may affect computing or network equipment, software or data.

(18) Providing a third and/or unauthorised party with access to University supplied username, password or identification details.

(19) NOTE: ITMS will never under any circumstances request usernames and/or passwords via email. Users should treat any such requests as 'phishing scams' and delete the email immediately. Under no circumstances are Users to supply any information with regards to usernames personal identification and/or passwords to a third party over the internet. Responding to such a request will be immediately considered as unacceptable use and Users will be subject to the relevant University disciplinary procedures.

(20) Utilising the University ICT systems or devices for personal and/or commercial purposes, private commercial gain or for the significant promulgation of private beliefs (unless utilised in connection with any one or more of these purposes is clearly required by the User's work, studies or other University responsibilities).

(21) Intentionally damaging hardware.

(22) Unauthorised attempts to identify or exploit system weaknesses.

(23) Unauthorised attempts to interfere with the operation of, or make University ICT systems or services unavailable.

(24) Use of University facilities in unauthorised attempts to make third-party computing facilities unavailable.

(25) "Spamming" or sending unsolicited group email.

(26) "Spoofing" or deliberately changing the "sender" field of email.

(27) Sending of chain letters or chain emails.

(28) Use which significantly degrades system performance for other uses.

(29) Excessive, unreasonable or constant use of internet or any other communications technologies (whether during work hours or not), for personal use and/or personal gain.

(30) Creation, solicitation, acquisition, transmission or public display of material, which is, or could reasonably be perceived as being, obscene, defamatory, discriminatory, offensive, objectionable in nature, or likely to cause distress to some individuals. If the material is a legitimate part of education and/or research, appropriate warning should be given if displayed or transmitted.

(31) Use that has the effect of harassing, bullying, intimidating, harming, distressing or threatening other individuals or groups, or is intended to have that effect, or is reckless in that regard.

(32) The transmission or downloading of any material that contravenes any relevant Commonwealth or Territory legislation.

Copyright Infringement

(33) Any use that contravenes the Commonwealth Copyright Act 1968, whether of the kind specified below or otherwise, will be deemed to be unacceptable use:

(34) Deliberately using or knowingly permitting the use of the University ICT systems or devices to infringe copyright laws as defined in the Copyright Act 1968.

(35) Downloading, sharing, copying, distributing and/or storing music, videos, movies or games from the Internet, unless it can be clearly demonstrated that explicit permission has been granted from the legitimate copyright owners, for example, if purchased from licensed websites or is made available by reliable sources. Proof of legitimate access may be required.

(36) Utilising file sharing or peer to peer software, unless it can be demonstrated to be necessary for legitimate research or work.

(37) Sharing or allowing access to copyright material with a third party without copyright owner's consent.

(38) Creating or distributing copies of CDs, DVDs, games or any other licensed material without explicit permission of the copyright owners.

(39) Copying software/computer programs without permission from copyright owners except with the express permission of the copyright holder, except to make a single backup copy.

(40) Installing software on to University computer facilities without appropriate authorisation.

(41) Using or viewing any illegally obtained software, CDs, DVDs or other media on University computing facilities.

Pornography

(42) The intentional accessing, downloading, transmission, storage, display or distribution of pornography is strictly prohibited, and will be considered serious misconduct by the University.

(43) NOTE: The possession and distribution of some forms of pornographic material, including but not limited to images of children, is a criminal offence and, if discovered on University computing facilities, will be referred to the relevant law enforcement authorities. Staff members or students whose legitimate area of research may involve collection and analysis of materials which are, or may be construed as, pornographic, should seek clearance in writing from their Pro Vice-Chancellor and should exercise caution, including the use of a secure drive, to avoid undue circulation or accessing of files and viewing of files in a public area.

Equipment Abuse or Misuse

(44) Deliberately using University equipment for purposes other than those deemed as appropriate or acceptable use.

(45) Deliberately causing physical damage to equipment or knowingly allowing or aiding a third party to damage University equipment.

(46) Using or permitting the use of equipment it would be reasonable to believe is dangerous to oneself or others.

(47) Not reporting any damage of equipment to appropriate personnel.

(48) Connecting any equipment to the University network (for example a modem) that will extend access or provide off-campus access to University ICT resources without the prior written approval of the Director Information Technology Management and Support or delegate, that such connection meets University security standards.

(49) Tampering with or moving installed facilities or equipment without authorisation.

Security Breaches

(50) For further information on University ICT security and passwords refer to the Information and Communication Technologies Security Policy and the Information and Communication Technologies Password Policy.

(51) Allowing a third party access to, or use of log-in ID, security card, keys or password information – verbally, by email or telephone.

(52) Knowing that an unauthorised person has gained access to, or use of log-in ID, security card, keys or password information – verbally, by email or telephone, and not reporting a breach in security protocols to a relevant authority.

(53) Allowing anyone without an access card entry or access to any of the University's secure areas such as computer laboratories.

(54) Deliberately using common words or names as a password or recording or displaying a password in an unsecure or easily accessed place.

(55) Not logging out of the University network when not utilising the system for extended periods of time.

(56) Allowing unauthorised access to the University's computing, communications or any other facilities using the University's network.

(57) Subverting or ignoring security measures and the integrity of University systems drives and files.

(58) Permitting unauthorised viewing or access to corporate or confidential data.

(59) Failing to provide identification (for example, by student or employee access card) when using University computing facilities, on request of a University staff member.

(60) Attempting to illegally hack into the University's computer system or access University data or accounts without authorisation or, knowingly allowing or aiding another person to do so.

(61) Deliberately accessing or targeting University computer or email systems in order to send spam messages or responding to spam messages by supplying confidential information.

(62) For information on disciplinary action and procedures for cases of unacceptable use of the University's information and communication technologies, refer to the University Handling Suspected Cases of Unacceptable Use of Information and Communication Technologies Procedures.

Status and Details

Status	Current
Effective Date	15th January 2022
Review Date	15th January 2023
Approval Authority	Vice-Chancellor
Approval Date	15th December 2021
Expiry Date	Not Applicable
Responsible Executive	Meredith Parry Deputy Vice-Chancellor and Vice-President Operations
Implementation Officer	Pat Gould Director Information Technology Management and Support
Author	Dianne Simons Project Officer +61 8 8946 6924
Enquiries Contact	Pat Gould Director Information Technology Management and Support