Email General Use Procedures

INTRODUCTION

The purpose of electronic mail (email) is to allow greater efficiency in teaching, learning, research, communication and administration at the University. Email is an increasingly important vehicle for cost effective and sustainable communication between members of the University community. Staff members, students and authorised visitors (collectively known as 'Users') are provided with a University email account to be used for University purposes. These emails become a formal University record and are governed by relevant legislation, by the University's stated values and standards of professional conduct, the *Code of Conduct* and by the protocols that apply to written communication.

The use of email requires attention to the needs of the University and its legislated responsibilities, consideration of the receiver, and regard for the demands of efficiency and professionalism.

Information Technology Management and Support (ITMS) are responsible for providing and supporting the University's electronic mail systems and mail agents on central servers. Use of and access to the University email services comes with obligations, limitations, responsibility and accountability.

All email users should be aware of the *Information and Communication Technologies Acceptable Use Policy* and the *Email Acceptable Use Policy*, individual responsibilities and legal obligations. All users are required to comply with these policies and are bound by law to observe applicable statutory legislation.

Like all University assets and services, email facilities should be used in an efficient, lawful and ethical manner.

Use of the University's email system indicates the User understands and accepts the University's conditions of use for computing and communication facilities.

COMPLIANCE

This is a compliance requirement under the University's *Code of Conduct*.

INTENT

This document has been developed to enhance the efficiency and clarity of electronic communication across the University and with outside parties. It aims to encourage good practice by reducing overall volume of electronic messages and by encouraging sensitivity and discretion. It outlines what is regarded as acceptable uses of University email facilities and the responsibilities of all email users.

RELEVANT DEFINITIONS

In the context of this document

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 emeritus, adjunct or honorary academic staff; alumni; external auditors or consultants; potential clients or business partners; contractors or vendors; conference delegates; and students and staff of other universities with reciprocal arrangements;

Email means a message, including any attachments, sent in an electronic format from one user to one or more other users via a computer network, using an email protocol;

Email address/email account means the officially recognised University email address as allocated by ITMS on enrolling as a student or joining the University as a staff member or as an authorised visitor;

Information and Communication Technologies (ICT) means collectively, computers, printers, facsimiles, telephones (both mobile and landlines), scanners, photocopiers, email, internet, intranet, web services, blogs, twitters, wikis, social networking sites such as, Facebook pages, electronic portable devices and any other similar resources;

Internet means the University intranet or network;

ITMS means the Office of Information Technology Management and Support within the University;

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 pornographic material;

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

Spam means irrelevant or inappropriate messages sent indiscriminately on the internet to a large number of recipients;

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; and

University Record (in the form of email) means any email that is in support of University business, whether or not the equipment, software, or facilities used to create, or store the email record, are owned by the University;

Use of email services means to create, send, forward, reply, copy, store, print, or possess email messages. For the purpose of this document, receipt of email is excluded from this definition to the extent that the email User does not have control over the email received; and

User means any staff member, student or authorised visitor to the University.

PROCEDURES

General

Electronic mail is a public communication medium that uses a store-and-forward mechanism to pass each message through multiple servers owned by other organisations and via many communication links world-wide. Email can be subject to misuse by individuals and organisations that send large numbers of unsolicited “spam” email messages to many email addresses.

As a result, the University cannot guarantee:

- The successful delivery of electronic messages travelling outside the University;

- The confidentiality of information contained in electronic messages travelling outside the University; and
- That all "spam" email messages are blocked from entry to the University email system.

Responsibilities of Users

Access to a University email account is provided for the purpose of sending and receiving emails related to the business of the University or to the course of study being undertaken by a student.

Emails sent and received by a User acting in his or her University capacity, are considered to be official records and must therefore comply with the University's *Records Management Policy* and Procedures as well as relevant legislated Retention and Disposal Schedules and relevant National and Territory legislation.

Use of email within the University is subject to the laws relating to copyright, freedom of information (*Information Act*), breach of confidentiality, privacy, spam and anti-discrimination. Users of a University email account are required to respect confidentiality, privacy, legal/professional privilege and the rights of others and to ensure that the content and dissemination of email does not jeopardise those protections.

Users of University email 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.

Users of University email must not use language that could reasonably be viewed as defamatory or discriminatory, or that may intimidate, vilify, harass or humiliate the receiver or any other person.

Email resources should not be used in a way that causes excessive strain on the University's Information Systems, including use that consumes a large amount of bandwidth.

Users must be aware that email messages, which they send may be construed as representing the University's position. Where a User does not have authority, is not aware of the University's position, or where his or her personal view may differ from that of the University, the message should state that the opinion expressed is that of the writer and does not necessarily reflect the views of the University.

Users of electronic messaging services must be aware of his or her responsibilities in regard to the creation, capture, retention and disposal of University records.

NOTE: All users must be aware of and note that the University regards activities that constitute unacceptable use of the University's information and communication technologies as potentially serious matters which the University may address by resorting to the applicable staff and student disciplinary procedures; reference to law enforcement agencies; or otherwise as it may see fit in the particular circumstances.

As all Users will be bound by these procedures and associated policies, a username and password for the system will not be issued until he or she has read these documents.

Availability, Use and Purpose of Email Services

Limited personal use of a University email account is permitted provided that such use is legal, consistent with the University *Information and Communication Technologies Acceptable Use Policy* and the *Email Acceptable Use Policy* and does not detract from, or conflict with, University business.
Personal use of a University email account must:

- Be infrequent;

- Be trivial in terms of amount of University resources used;
- Not interfere with performance of the User's work, studies or other University responsibilities; and
- Not be used for personal commercial purposes, private commercial gain or for the significant promulgation of private beliefs, unless use in connection with any one or more of these purposes is clearly required by the User's work, studies or other University responsibilities.

University email services are provided to all Users and are intended to support and facilitate University business. The University recognises that email may be used for incidental personal purposes, but stipulates that such use must not:

- Interfere with University operation of information technologies or electronic mail services;
- Burden the University with incremental costs;
- Interfere with the user's employment or other obligations to the University; and
- Infringe upon any other condition of employment or University policies and procedures.

Email accounts may also be used for the submission and return of student assignments and other specific uses, but only where the relevant Faculty or Department has specifically authorised this, and where the guidelines and conditions for such submission/return, which have been specified by that Faculty or Department, have been fully complied with.

The Deputy Vice-Chancellor, Operations, in conjunction with the Director, ITMS is responsible for ensuring that the *Information and Communication Technologies Acceptable Use Policy* and *Email Acceptable Use Policy* and supporting documents are observed and enforced.

The head of each Faculty or Department is responsible for ensuring that all Users associated with his or her area are made aware of the Email Acceptable Use Policy and these procedures.

The University may, at its discretion use electronic mail as a formal means of communication with Users for legitimate University purposes.

Unacceptable Use of Email

Email services must be used in accordance with the University's *Information and Communication Technologies, Acceptable Use Policy* and associated procedures.

Any suspected breaches of these procedures or associated policies will be governed by the University's *Handling Suspected Cases of Unacceptable Use of Information and Communication Technologies Procedures*.

The University considers the following to be **examples of unacceptable use** of email services:

- 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";
- Deliberate impersonation of another individual across the network by the use of his or her access user name, password, personal information or by any other means;
- Emailing confidential files or files of a sensitive nature (business or commercial) to unauthorised recipients;
- Providing a third and/or unauthorised party with access to University supplied user name, password or identification details;

- Excessive, unreasonable or constant use of University email facilities or any other communications technologies (whether during work hours or not), for personal use and/or personal gain;
- Forwarding emails that are confidential or classified in nature or contain copyrighted material without the owner's permission;
- Deliberately and knowingly accessing emails to which you are not the intended recipient;
- Accessing, viewing, downloading, saving, copying, distributing or forwarding material of a pornographic or offensive nature via email;
- Knowingly promulgating software viruses or similar contaminant software or taking any action that would lead to denial or impairment of access to, or effective use of, any information technology resource, such as flooding the mail system with junk mail (Spam);
- Taking any action that would or might lead to circumventing or compromising security of any of the University's information technology resources;
- Perpetuating chain letters, virus warnings or hoax messages; and/or
- Deliberately accessing or targeting University computer or email systems in order to send spam messages or responding to spam messages by supplying confidential information.

NOTE: ITMS will NEVER, under any circumstances, request User names 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 User names, 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.

Email Users are expected to assist in the prevention of email misuse by:

- Verifying the authenticity of an email that proposes an unusual course of action;
- Not using email to convey sensitive personal or commercial information;
- Protecting his or her email accounts and passwords by not allowing others to access these;
- Not accessing other accounts without permission from the account holder;
- Being aware that by sending his or her email address to open groups, his or her email address will become public; and
- Being aware that it is possible for a forwarded message to be altered from the original one.

Staff Email as Official Records

Email messages sent or received by Users that refer to or contain information on or about University business, whether from within or outside the University and whether or not the equipment, software, or facilities used to create or store the email record are owned by the University, are official records of the University and must be managed as such. As official records, ownership of email messages rests with the University rather than with the individual.

Email is considered a business document and, as such, can be accessed under the Information Act. Use of email is also subjected to the laws relating to copyright, breach of confidentiality, privacy, spam and anti-discrimination. All staff members using email as a means of corporate communication have a legal responsibility, to capture and retain messages so that they are accessible as records to meet business and evidential needs over time (for further information see University Records Management Policy).

Emails are subject to the same retention and disposal requirements as electronic and paper based records. Therefore, it is important that all corporate emails are kept as evidence, and where appropriate are captured within the University's records management system.

Emails that are sent or received using a non-CDU address but which relate to official University business constitute official University records. In these cases, normal record keeping requirements must be observed.

Given the University's obligation to retain records under relevant legislation and policies, periodic deletion of corporate email messages irrespective of their content or the business activity they support is inappropriate (for information on secure storage options for electronic records please refer to ITMS).

Security and Monitoring of Email

The University may access email records including, but not limited to, access in the event of reasonable suspicion of criminal or unauthorised activity, potential or actual legal action involving the University, or in the exercise of its legal obligations to disclose or provide records or to protect the interests of the University.

Surveillance of email will be in accordance with appropriate Northern Territory and Commonwealth Government legislation.

The University seeks to protect the security of its email but cannot guarantee protection against the interception or alteration of communication by third parties.

The University monitors the email system and reserves the right to quota the size and volume of emails sent and received on the University system.

The Director, ITMS may deny access or restrict access to the University's email resources to prevent a breach of the law or a breach of policy, or to conduct an investigation into such a breach, or to protect the integrity of the University's information and communication systems.

The University may block emails that threaten the security of the system, involve the dissemination of spam, or include content that is contrary to the expectations of this and other relevant University governing documents.

The University does not log the content of email. However, logs of internet access and email are automatically generated and, in the case of email, include the time a message was received and the location of its origin, the time a message is retrieved by the User, the User name which was used to authorise the sending of a message, and the size of the message and the identity of the sender and receiver.

Access to these logs is available to a small number of ITMS technical employees solely for the management of the email resource, for diagnosis and resolution faults, or to detect and manage IT security breaches.

Consistent with the University's *Privacy and Confidentiality Policy*, information contained in these logs is released beyond this group only with authorisation of the Director, ITMS, or Deputy Chief Operating Officer, and only if:

- It must be released for law enforcement purposes;
- It is required to investigate breaches of University by-laws, policies and/or procedures; or
- If the University is legally compelled to provide the information, for example, by subpoena or to comply with a freedom of information request.

The University reserves the right to install and operate filtering equipment, software or procedures to prevent entry into the University, of email traffic that is contrary to law or which is incompatible with the objectives of the University.

Decommissioning of Email Accounts

Student Email Accounts

Student access to email ceases seven (7) days after the notified graduation ceremony date (or alternative completion date for courses without a graduation ceremony) or if a student fails to reenrol at the University.

(Note: The period of access to email accounts will be reviewed on an annual basis and adjusted as necessary in accordance with Commonwealth requirements).

Staff Email Accounts

An individual staff member and his or her immediate supervisor will be notified by ITMS, two (2) weeks prior to the staff member's account being disabled and computer access being removed. During this time the staff member may retrieve any personal emails or files.

Staff member email accounts will be terminated at midnight on the final day of employment or association with the University. ITMS will place an auto-forward on the departing staff member's email account, redirecting any incoming emails to the staff member's supervisor, for a period of three (3) months. The supervisor will monitor incoming emails for relevance or information that may be important to the University.

After three (3) months, the computer account, email and home directory files are all deleted. Should the staff member or his or her supervisor require an extension of this period of access after the termination date, a request must be forwarded in writing to the Director, ITMS requesting the extension and listing the reasons for the request. The Director, ITMS will decide to grant or deny an extension on a case by case basis.

It is the responsibility of the Senior Manager of an area to ensure that corporate email records of a staff member who has resigned remain accessible and are retained for the period of time required by the University *Records Management – Retention and Disposal of University Records Procedures*.

Visitor Email Accounts

An authorised visitor who has been granted access to email whilst conducting business with the University will have his or her account access removed and the account will be disabled at midnight on the date that the visitor's work or association with the University has ceased.

Employee self-subscribe email distribution lists

Currently there are two (2) main email forums – All-Staff and CDU-Staff - that are utilised to communicate with staff and authorised Users across all campuses.

The All-Staff mailing list is moderated by the Vice-Chancellor's Personal Executive Assistant and is used by the Vice-Chancellor to convey messages to all staff members. Staff members are automatically subscribed to this list when he or she commences employment at the University.

The CDU–Staff-bounces mailing list is used by members of staff to convey work-related information that is specific to certain groups or may be of interest to certain groups within the University. Staff members are able to choose to subscribe to this mailing list.

The University also provides some email distribution lists, unmoderated forums or news groups to which Users may subscribe according to individual needs or interests. Users add or remove themselves from the self-subscribe lists via the relevant website. Some forums may allow any User to send an email message to subscribers (for example, CDU-General-Info) and where this can occur, messages should be relevant to the purpose of the list. CDU-General-Info list will only allow subscribers with University email addresses and declared partner institutions such as Menzies or BIITE, to access and post messages on the forum. The forum should be utilised to locate, sell or advertise goods and services; social and community events; and a general discussion forum.

The legal obligations of the User (Note: the User is also responsible for the content of items posted on behalf of a third party), the University *Information and Communication Technologies Acceptable Use Policy*, *Email Acceptable Use Policy* and *Email General Use Procedures* and rules of general etiquette, still apply to anything posted on these forums and lists.

ESSENTIAL SUPPORTING INFORMATION

Internal

Charles Darwin University and Union Enterprise Agreement

Electronic Messaging Guidelines

Email Acceptable Use Policy

Equal Opportunity Policy

Handling Suspected cases of Unacceptable Use of Information and Communication Technologies (ICT) Procedures

Identifying Unacceptable Use of Information and Communication Technologies Procedures

Information and Communication Technologies Acceptable Use Policy

Privacy and Confidentiality Policy

Records Management – Capturing University Records Procedures

Records Management – Discovery of University Records Procedures

Records Management – Retention and Disposal of University Records Procedures

Records Management – Security of University Records Procedures

Records Management Policy

University Centrally Managed Mailing Lists Guidelines

Disposal Schedules

External

Information Act (NT)

Document History and Version Control			
Last amendment:	15 Dec 2017	**Next Review:**	Sept 2015
Sponsor:	Deputy Vice-Chancellor, Operations		
Contact Officer:	Director, Information Technology Management and Support		

Version	Date Approved	Approved by	Brief Description
1.00	27 Oct 2011	Vice-Chancellor	Creation of original document and upload to CDU website.
1.01	7 Jul 2013	Governance	• Assigned document number • Converted to current template • Updated and add hyperlinks • Minor changes to wording, grammar and formatting
2.00	18 Sept 2013	Vice-Chancellor	• Review document with the following updates and amendments • Replace Code of Ethics with current Code of Conduct • Update definition of Senior Executive to reflect change in position titles, delete Senior Deputy Vice-Chancellor, and Executive Director and include Chief Operating Officer, Deputy Chief Operating Officer and Chief Financial Officer
2.01	15 Dec 2017	Governance	• Conversion to new Governance template due to new University branding • Updated hyperlinks • Amended Privacy Policy to Information and Privacy Policy • Amended Deputy Chief Operating Officer to Deputy Vice-Chancellor Operations • Added Sponsor Deputy Vice-Chancellor, Operations