Electronic messaging (Email) policy

1 Scope

This Email Policy applies to the use of University facilities by staff, students and authorised users for the purposes of sending and/or receiving email messages and attachments.

2 Audience

This document is for the use of ACU staff and Students and other authorised users that utilise the Email services provided by the University.

3 Purpose

This Email Policy provides standards and guidance for the acceptable usage of the University's email messaging facilities. The Policy also describes the standards that users are expected to observe when using these facilities for email. This policy is an adjunct to the University's Computer and Internet Acceptable Use Policy.

4 Appropriate Use

4.1 Permissible use.

The use of electronic mail must be related to University business, teaching, learning, and research. Incidental and occasional personal use of electronic mail is permissible provided that in each case the personal use is moderate in time and does not incur significant cost for the University. In addition any personal email that is sent must contain a disclaimer that states that the views of the sender are not necessarily representative of those of the University. The use of electronic email for personal use is subject to the provisions of this policy and the University's Computer and Internet Acceptable Use Policy.

4.2 Prohibited use.

The University's electronic mail resources shall not be used for:

- any purpose(s) that is restricted by University regulations and/or policies, and/or any applicable State and/or Federal regulations or laws.
- personal monetary gain or for commercial purposes not directly related to University business.
- sending copies of electronic works in violation of copyright laws or the inclusion of the work of others into electronic mail communications in violation of copyright laws.
• sending electronic mail to harass or intimidate others or to interfere with the ability of other users to conduct University business.

• sending unsolicited bulk email.

• disseminating confidential information about the University.

• knowingly causing interference with or disruption to any computer, computer network, information service, equipment or any user thereof.

• disseminating personal contact information of colleagues, staff or students without their written consent.

5 Privacy

The University keeps and monitor logs of email usage for performance and system maintenance purposes. The information logged may reveal information such the email addresses of those with who staff and students have communicated with. The information logged will not reveal the subject or the content of the email. The University will not engage in real-time surveillance and will not monitor the content of email messages sent or received by its staff or students, unless a copy of the message is sent or forwarded to the University by its recipient or the sender. The University will not disclose any of the logged, or otherwise collected information to a third party except under compulsion of law.

6 Usage

6.1. Email Disk Storage

Staff and students may store their email on University provided email servers. However the volume of email that can be stored is limited by the availability of server disk space. To ensure equitable use of disk space resources the following disk storage quotas will be implemented.

6.1.1. Storage quota for staff email servers.

• Academic and general Staff email accounts – 200mb

• Head Of School and Department Managers – 400mb

• Generic accounts (e.g. team mail accounts) - 200mb

• Discussion groups (e.g. mailing lists) - 50mb

Once a storage quota has been exceeded staff will be able to send email but not receive any email. Sent email will no longer be saved in their sent mailbox. Staff will need to regularly archive their email to the network, CD & DVD.
6.1.2. Storage quota for student email servers.

- Student email accounts - 30mb

Once a storage quota has been exceeded staff and students will be able to send but not receive any email. As the student email server is a web based system there is no facility for students to archive their emails. Students are therefore advised that if they want to have permanent copies of their email they can do so by either printing out their emails or by copying their emails to a text based word processor.

6.2. Email format

Any email messages sent must contain the following information.

- A signature notice that details the sender's full name, department, telephone/fax number, the University address, University ABN number and the CRICOS provider number.

- A confidentially notice. The following is recommended: -

"This correspondence is for the named person's use only. It may contain confidential or legally privileged information or both. No confidentiality or privilege is waived or lost by this transmission. If you receive this correspondence in error, please immediately delete it from your system and notify the sender. You must not disclose, copy or rely on any part of this correspondence if you are not the intended recipient."

6.3. Email broadcasts

Emails sent to Campus or University wide mailing lists must meet one of the following guidelines:

- be relevant to the University or campus as a whole, representing corporate information, or to all staff within one of the major groupings such as academic, general or research.

- provide information about issues, policies, events or decisions with a direct connection to the core work of the University and its Faculties and key organisational units.

- have some degree of urgency, to the extent that the message should be drawn to the attention of relevant staff prior to a specified deadline.

Generally, advertising events or causes or services, which are of relevance or interest to limited sections of the University or campus, should be sent to the University subscription only mailing lists.
6.4. The University has a national email structure (@acu.edu.au) and there is a requirement to ensure that accounts are unique, descriptive and relevant for a specific purpose.
   a. Staff accounts will be in the format of
      Firstname.Lastname@acu.edu.au unless there are conflicts in which case an additional unique identifier will be used such as the middle name or initial or numeric identifier.
   b. Generic accounts are required to convey the campus, department and the purpose of the account or one that clearly identifies a department or an ACU national function.

Generic accounts that represent a function that is not exclusive or unique to a user or department will not be allocated. An example of accounts that are not to be used but not limited to: papers@acu.edu.au, info@acu.edu.au, services@acu.edu.au

7 Security

7.1. Email borne viruses

The University has taken reasonable steps to minimise the impact of email and/or computer based viruses by ensuring that all networked University computers are protected by anti-virus software. However there will be instances where computer based viruses may not be detected in a timely manner and therefore the following additional precautions will need to be taken:

   a. To prevent the receipt and transmission of potential viruses incoming email messages will be automatically scanned for attachments. Those attachments that are not zipped will be automatically deleted.
   b. Staff and students should ensure that they have an effective anti-virus system operating on any computer that they use to access University IT facilities.
   c. Staff and students should not open email file attachments received from unsolicited or untrusted sources.
   d. Staff and students should not use email clients with inherent flaws that allow the spread of email viruses such as MS Outlook or Eudora.
   e. Staff and Student should use workstations with Virus Protection.

7.2. SMTP (TCP port 25) outbound restrictions.

All outgoing mail from ACU must be relayed via central email infrastructure. Only high volume email servers (typically relaying more than 1000 non-local messages per day) are allowed direct access to the internet. Each campus has access to a SMTP relay host and thus
all Servers, Network devices and Staff/Student PC’s must relay email through the designated email server for that Campus.

The reasons for this measure is:

a. To prevent unauthorised email servers access to the Internet. Mis-configured email servers can also be a risk to the overall security and reputation of the ACU network.

b. To minimise the increasing prevalence of viruses, worms and other exploits which make use of email to infect other systems or to distribute spam. Viruses, worms and other exploits often take advantage of direct outbound SMTP connectivity to the internet for delivering messages to other victims or to spam recipients. This can involve very large numbers of messages which can cause disruption to other Network devices such as Voice Over IP telephony.

c. When an ACU host is infected by a mass emailing virus or worm and used to attack or spam other sites, this is harmful to the reputation of ACU. It could potentially result in ACU’s entire network being "blacklisted" as a spammer or spam-friendly site.

d. Such events can also result in significant Internet traffic costs to ACU.

This measure will not prevent all malicious email from ACU systems, since some exploits may be capable of locating a local SMTP server for relaying messages. But this is generally easier to detect and stop via the email relay host than direct Internet relaying.

8 Automatic email account forwarding

Staff Email accounts shall not be forwarded to an outside destination that is not within the control of the University unless approved by the Director of ITCS. Staff must use their University provided email account for all electronic correspondence with Staff and Students and emails must contain a signature as in Point 6, 2.a.

Email may not be forwarded to an external destination for the following reasons (but not limited to):

a. The forwarding of email accounts to external email providers exposes the University to potentially inadvertent transmission of sensitive information.

b. Anti-spam and security measures employed at ACU may inadvertently block critical information when email is sent from an outside provider e.g. Blacklisted hosts.
c. The use of external email providers may negate security measures and
could cause a "backdoor" to virus and malware infections to the
internal network.
d. Forwarding of emails may negate any Email Retention legislation.

9. **Refer to Blackberry policy**

Last Revision: August 2007 authorised by the Director of ITCS