UWA IT Policy:

SPAM Handling Policy

Purpose of document:

The statement of a UWA IT policy.

Document Control:

<table>
<thead>
<tr>
<th>Vs</th>
<th>Author</th>
<th>Date</th>
<th>Details</th>
<th>Reviewer</th>
<th>Date</th>
</tr>
</thead>
</table>

APPROVAL

Approved by the Executive Group on 23 August 2005

INTENDED AUDIENCE OF POLICY

All IT technical support staff at UWA – policy action.
All staff and students – policy awareness.

GENERAL INFORMATION

Unsolicited commercial email, or spam, is a problem facing all organizations that make use of internet-enabled email. The risks and problems arising from reception of spam range from lost productivity, failure in communications when real emails are missed in a flood of spam, to legal liability when employees are exposed to offensive or pornographic messages.

Spam is an increasing problem at UWA. In August 2004, anti-spam software was implemented at the central level. This software tags any email displaying recognised spam characteristics but does not delete it. The decision not to automatically delete was made because of the fear of deleting legitimate mail that had been incorrectly marked as spam, so-called “false positives”. Tagged spam is passed to the relevant business unit email server along with the untagged email. Some business units filter off the tagged spam before delivering email to the users’ inboxes; others leave it up to the user to delete any tagged spam.

On average, the University receives about 650,000 emails per day. About 150,000 of those are “tagged” as spam. Amongst the items tagged as spam, only 4 or 5 per month are formally reported as false positives, although a much larger number of false positives are not being reported.

The current devolved arrangement for handling of tagged spam email at the business units has resulted in a variety of implementations ranging from doing nothing, to deleting all tagged spam on receipt.
This policy has become necessary to ensure a minimum standard and associated practices for handling spam are in place across UWA to protect staff and students. Those areas not already meeting or doing more than the practices outlined in this policy need to put the policy measures in place as soon as possible, but no later than 30 September 2005.

**Policy Statement**

Any business unit that is running a mail server must take proactive measures to protect staff and students from offensive spam and the time-consuming task of deleting tagged spam. The minimum measures that must be put in place are:

- Any tagged spam should be archived into a separate area so that it is not delivered to the user’s inbox.
- A mechanism should be provided to allow the user to review and retrieve archived spam emails if the user fears that there may be false positives.
- Archived spam emails should be automatically deleted after a reasonable period of time, not less than 14 days.
- An opt-out option may be provided for those staff or students who do not wish to have any spam email archived and are willing to manage tagged spam themselves.
- Tagged spam will not be forwarded to an external email address, such as a personal hotmail address. This is to prevent the University from being blacklisted as a sender of spam.
- Business units should provide support and guidance to all staff and students to enable them to manage spam, including the reporting of false positives.