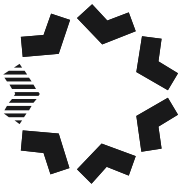
NATIONAL
COMPETITION
COUNCIL



Email Protocol & Internet Connection

NCC Policy document

June 2009

Table of Contents

NATIONAL COMPETITION COUNCIL EMAIL PROTOCOL

Email is a form of communication that is no less formal, permanent or influential than the same message sent through the post. You should, therefore, take as much care in composing email messages as with other communications.

The following covers your responsibilities with regard to emails; the content of emails and how best to treat your readers; email etiquette; and its issues. This protocol should be read in conjunction with the *Guidelines for Usage of your National Competition Council Internet Connection* (page 7).

Your responsibilities

1. You are responsible for what you send and for dealing appropriately with what you receive.

    - The *Privacy Act* is not applicable to messages, so users should have no expectation of privacy in relation to messages they send or store. Messages are able to be monitored and accessed, though this is not done as a matter of course.
    - If what you are sending is not something you would want to see revealed publicly and attributed to you or accessed under the *Freedom of Information Act*, don't send it.
    - Given the possibility that messages sent outside the Council might be misdirected, the following disclaimer is automatically attached to messages sent externally:

      USE OF THIS COMMUNICATION: The information contained in this email message and any attachments is for the use of the intended recipient only. This email and any attachments may be confidential or privileged, in which case neither is intended to be waived. If you are not the intended recipient, any use, disclosure or copying of this information is unauthorised. If you have received this email by error please notify the sender immediately by reply email and delete all copies of this communication together with any attachments.

      DISCLAIMER: It is the recipient's responsibility to check this email and any attachments for viruses or defects before opening them or sending them on. If this email is a private communication, it may not reflect the Council's views and the Council is not responsible for its contents or the contents of any attachment.

2. You need to bear in mind that:

   - email records can be used as evidence in a court of law in accordance with the Evidence Act 1995 and
   - email records may be treated as Australian Government Records for the purposes of the Archives Act 1983 and should be treated accordingly.

3. You should:

   - select the appropriate email classification, from the options in the drop down box, prior to sending a new email message
   - not send or forward emails from other people that contain information that bears a security classification or is otherwise confidential and
   - you should keep records of messages or sequences of messages which relate to business transactions in an appropriate record keeping system.

Email content

4. Be factual. This ensures that the chance of misinterpretation by the reader(s) is, as much as possible, kept to a minimum. In the absence of body language and/or voice tone recipients have less information with which to interpret an email message, so be cautious, particularly in communicating with people unfamiliar to you.

5. Be concise and to the point.

6. Before you send a message check it to ensure that it is of a sufficient standard to be sent.

Your readers

7. Respect other people's time and inbox space.

   - There is a significant tradeoff between deluging mailboxes on one hand and ensuring colleagues are fully informed on the other hand.
   - Consider using a link rather than attaching files so as to reduce the use of server space. Document links can be sent by following the sequence – *insert/hyperlink/(select appropriate file)/OK*. Document hotlinks from the internet can be sent by using the *File/Send/Link by email* function.

8. Consider including only one subject per email, this simplifies the task for the reader(s). Use the subject line to indicate the issue being addressed.

    - In the subject line the appropriate use of 'for your information' (fyi) and/or an accurate and meaningful description of the content of the message should be provided.
    - There are several appropriate message flags that can be attached. For instance the *Follow up flag* and/or *High or Low importance* can be selected from the drop down arrows under the *Message* / *Options* menu on the ribbon.

E-mail etiquette

9. Messages should be polite and should not contain material the reader may find offensive.

10. Check email regularly and respond to it promptly.

11. Consider alternative communication media – in some contexts a phone call or a personal visit could be more appropriate and effective.

12. Do not edit an email you have received to change its meaning before re-transmission.

13. Don't forward messages without the permission of the sender unless permission can reasonably be assumed to have been given. There is a presumption permission can be considered as given with work-related email. Notwithstanding this, you should give some attention to this issue before you forward work-related messages. Senders have the option of attaching the 'Do not forward' flag to messages. This flag can be found under *Message / Follow Up* / *Flag for recipients' / Flag to / Do not forward.*

IT issues

14. Consider the size and number of attachments in an email.

    - The protocol SMTP (Simple Mail Transport Protocol) used to send email messages across the internet can suffer from transmission timeout errors when transferring large email messages.
    - Some internet service providers limit the size of user mailboxes.

The suggested maximum size of an email, including attachments, is 3 – 5 megabytes.

15. Be vigilant of the threat from computer viruses, trojans, and worms.

- As most email viruses will probably (unknowingly) come from a known source (friend, colleague, business contact, etc), be wary of unusual subject and message content. If the nature of the message is different from that usually received telephone the sender prior to opening the email to confirm its legitimacy.
- Inform IT staff of suspect email as the appearance of infected email in the user's mailbox could point to a problem with the email server or firewall systems.
- Be especially wary of email attachments with *.exe, *.com, *.vbs, *.scr, and *.html file extensions.

GUIDELINES FOR USAGE OF YOUR NATIONAL COMPETITION COUNCIL INTERNET CONNECTION

The Council's internet connection is an important resource which makes a significant contribution to the ease of timely access to information and to its transmittal. These guidelines set out your responsibilities with regard to the internet connection, legal and IT issues and monitoring.

The guidelines should be read in conjunction with the *National Competition Council Email Protocol*.

Your responsibilities

1. In using the internet connection, you should not compromise the security of the Council's information systems or prejudice their performance, functionality or reliability.

2. You should keep your log-in password confidential and renew it at regular intervals. Note that any access to the internet connection under a user's password will be attributable to that user. To avoid the possibility of misuse, don't leave your workstation unattended without a screen lock in force.

3. Please use the internet connection in an efficient manner. In particular, avoid keeping the connection open when it is not in active use.

4. The internet connection should not be used for private business gain. The connection is primarily for Council related work, but unavoidable and limited personal use is accepted.

5. You should not use the internet connection to transmit or publish any material (whether on the Council's home page or elsewhere):

    - except in accordance with the Council's policies and practices
    - so as to suggest that the material has an endorsement or a level of approval that it does not have, and
    - which has or is likely to have the effect of bringing the Council or the Australian Government into disrepute.

6. In using the internet connection, you should not conceal or misrepresent your identity. In particular you should identify messages, by including your name, designation and email address.

IT issues

7. You should not download software from any external internet site.

    - We need to maintain licencing agreements with all software loaded on our computer network. Software downloaded from the internet and used by staff may not be covered by a relevant licencing agreement, which would put the Council in breach of copyright laws.
    - All software programs and drivers need to be tested by IT staff to ensure safe and reliable operation on the computer network and
    - We need to bear in mind the capacity constraints of the Council's system and of individual PCs.

8. The Council's system runs a virus check on all incoming material, but to ensure maximum security users should run a virus check immediately after downloading or unzipping executable files or macros from the internet. In the event that a virus is detected, you should notify our IT consultant immediately.

Legal obligations

9. The internet connection should be used in accordance with the law. In particular, you should abide by all relevant laws relating to the following:

    - national security
    - fraud
    - misrepresentation
    - defamation
    - privacy
    - freedom of information
    - telecommunications
    - hacking (unauthorised access to information systems)
    - breach of confidence
    - copyright
    - censorship
    - pornography

- sexual harassment
- racial vilification
- privilege and contempt

10. In respect of Guideline 9, personal liability can arise from any unlawful activity with respect to the use of the internet, both under the common law or applicable legislation such as the Crimes Act 1914 or the Copyright Act 1968.

Monitoring

11. You should be aware that:

    - usage of the internet connection may be monitored to protect the Council's information systems from unauthorised access and to ensure performance, functionality and reliability of those systems and the internet connection and
    - unauthorised or improper use of the internet connection may result in your activities being recorded with any evidence of possible criminal activity being forwarded to law enforcement officials as required.

12. You should notify the Executive Director of any unauthorised use of the internet connection or breach of these guidelines by any other user which comes to your attention.