DISCLOSED UNDER FOI

Commonwealth OMBUDSMAN

Email management policy

POLICY NO. 8|2008

DISCLOSED UNDER FOI

Document control

Client name: Commonwealth Ombudsman's office
Issued to: All staff
Document Email Management Policy
Pages changed: All
Modification history: Nil

Vers.	Date	Author	Changes
2.0	30 October 2008	Elizabeth Courtney-Frost	
3.0	16 April 2009	Elizabeth Courtney-Frost	Amended subject line advice

The Email Management Policy should be reviewed annually. The next review is due when the news electronic records management system is implemented in early 2009.

DISCLOSED UNDER FOI

Contents

DISCLOSED UNDER FOI

Introduction

The purpose of the policy is to establish a framework for the management of emails within the Commonwealth Ombudsman's office. Email is part of the official business communication of the office. Emails sent or received contain information about business activities and can function as evidence of business transactions that are part of the official records of the office. They must, therefore, be managed in accordance with the *Archives Act 1983*.

In addition, staff have a responsibility to assist in management of emails to ensure that the Outlook system runs efficiently.

This policy applies to all Ombudsman staff and contract staff.

Sending emails

Personal emails

Incidental personal use of office IT resources, including email is allowed so long as it is within reasonable limits. Personal emails should be deleted as soon as possible.

However, it is important that staff are aware that there are particular sensitivities associated with sending personal emails from our office systems. For instance it is possible that the mere association of a statement or opinion with the name of the office (as reflected in your email address) may appear to give an endorsement or authority that is not intended or is inappropriate.

Particular care should be taken when your personal concerns may intersect with a function of the office (such as a personal complaint to a Commonwealth or ACT Government department or agency). In addition, you should bear in mind that the mere inclusion of your email address on distribution lists of some organisations (for example clubs or political groups) may create an impression that is not consistent with the image of the office or the Australian Government. In such cases, do not use the office email system or email address.

If in doubt, please err on the side of caution and use your home email address for such purposes. If you have any questions on particular instances, please discuss with your manager, SAO or the SAO Corporate.

Inappropriate or offensive emails

Emails that contain material that is racist, sexist or otherwise offensive should not be sent. Sending such emails is a breach of the APS code of conduct and could lead to disciplinary action. If you receive offensive emails from someone in the office, you should let your supervisor or the SAO Corporate know. If you receive offensive emails from someone outside the office, please delete them immediately and contact the IT helpdesk if there appears to be a constant issue.

The filter rules on 'junk mail' are set out on the intranet in the Guidelines on SPAM control and management.

All staff emails

In general, information relating to more than one team should be placed on the news page on the intranet rather than being sent as an all staff email. This reduces the size of emails being sent and ensures that corporate information is retained in an accessible central repository. To arrange for documents to be published on the intranet, contact the Web Services Team via email or phone to discuss details.

DISCLOSED UNDER FOI

Occasionally it might be appropriate to send an 'All Staff' email containing important information that is of an urgent and short-term nature. Before doing so, approval should be obtained from your SAO or manager.

Storing emails

When is an email a corporate document?

A corporate document is 'information created, received and maintained as evidence and information by an organisation or person, in pursuance of legal obligations or in the transaction of business'. An email is a corporate document if it meets these criteria and should be recorded.

As with other documents, emails relating to simple organisational matters such as arranging meetings should be deleted once the meeting has occurred.

Emails and Resolve

As with other documents, the author of the email or the person who received an email from an external source is responsible for filing the email. Complaint related emails should be attached to *Resolve*. Other emails should either be attached to *Resolve* or printed and attached to a formal file.

All emails relating to an approach, whether incoming or outgoing, need to be stored in the *Resolve* documents area. You will need to drag and drop or copy and paste each email into *Resolve.* This also applies when replying directly to an email in *Resolve*. Replies are automatically saved in Outlook. However all emails need to be manually saved as *Resolve* documents.

Once an email has been recorded on *Resolve* or attached to a formal file, it should be removed from Outlook.

When to file a mail thread

A mail thread is where there is an initial email and a response has been added to that initial email (that is, a reply with history).

It is often not clear when to file a mail thread and it is not possible to make 'hard and fast' rules. Making a record after each addition to the thread will often waste time and possibly paper and result in duplication of records.

It is suggested that you consider that the intent is to make a record of corporate documents so that a third person should be able to look at a case and understand what has occurred. Remember that other staff are unable to access the mail thread when it remains only in your personal Outlook folder. However if the mail thread is bouncing backwards and forwards in a short space of time, it is time-wasting to record the email at each addition.

It is suggested that the mail thread be copied to *Resolve* or placed on a file when:

- you are fairly confident that the mail thread is completed
- at the end of a working day
- it may be important for other staff to access the email.

You cannot replace a prior copy of the mail thread in *Resolve* with an updated version (you will need to request that the earlier document is deleted). When you add a later version of the mail thread, you should place a note in *Resolve* indicating that the later email is an updated version of the earlier email so that someone conducting a QA knows that it is unnecessary to look at the earlier email.

DISCLOSED UNDER FOI

If you have placed a paper copy of the mail thread on a formal file, you can replace it with an updated version.

Managing your Outlook folders

The cost to the office of unmanaged emails can be significant:

- the amount of storage increases unnecessarily
- the efficient running of Outlook can be compromised
- corporate records can be lost if emails have not been appropriately filed when a staff member leaves the office.

As with any other document source. for example paper or electronic, it is the responsibility of each staff member to ensure that the records they create or receive are appropriately filed. Placing emails in a personal email folder does not reduce the IT storage requirements, although sometimes this is desirable while action relating to the email is outstanding.

Note: If you have more than 800Mb in your Inbox you will not be able to send further emails until the excess has been deleted from the Inbox.

Email security

The Australian Government Protective Security Manual (PSM) requires that information that we access or hold is appropriately protected. The PSM requires compliance with the Australian Government Information and Communications Technology Security Manual (ACSI 33) issued by the Defence Signals Directorate. The key requirements of ACSI 33 are that:

- all emails sent from the office must have a protective marking
- the protective marking must identify the maximum classification of all information in the email, including attachments.

Fedlink

The Ombudsman's office uses the Fedlink Mail system to meet these requirements. This system was designed to comply with government policy and enable agencies to safely send security-classified emails. Not all government agencies use the Fedlink system yet. Staff should be aware that there is a risk of unauthorised access when sending personal information about a complainant to an agency that is not on Fedlink. A current list of government agencies that use Fedlink can be seen at http://www.fedlink.cybertrust.com.au.

Office network security classification

The office has been classified at the non-national security X-IN-CONFIDENCE level. This means that we can only send or receive material classified at the X-IN-CONFIDENCE level or below. Therefore, we are not able to electronically send or receive any material that is classified as:

National Security Classification	Non National Security Classification
Restricted	Protected
Confidential	Cabinet-in-Confidence
Secret	Highly Protected
Top Secret	

DISCLOSED UNDER FOI

If you need to transfer information classified at one of these levels, see 'Information security requirements for classified material' on the intranet.

Choosing a protective marking

Comprehensive help information is available in Outlook. Open a new email (or select reply). Select the 'protective marking' tab on the tool bar.

It is the responsibility of the person preparing the email (or for actioning information generated outside the Australian Government) to identify and to apply an appropriate security classification. There are five choices:

Unclassified—for information that could be released to the public with no adverse affect to the office or an individual

Commercial-in-confidence—used for commercial and financial matters where release of the email might cause problems such as financial loss, result in improper gain or advantage, breach commercial confidentiality

Staff-in-confidence—where the email contains confidential information about a staff member

Security-in-confidence—for emails where release might cause distress to individuals or private entities. Also for sensitive policy issues, confidentiality issues, where release might prejudice the investigation or facilitate the commission of a crime or any other emails that might be sensitive and it is not clear which marking to choose.

Client-in-confidence—for emails that include information about agency clients or complainants. This is the classification most likely to be appropriate for complaint matters.

Please note:

- if you are forwarding an email, you can increase the security classification but you cannot reduce it
- if you select a security classification other than 'unclassified' and the receiving agency is not on Fedlink, you will be advised that the email has been blocked and you will need to send the information by other methods
- if an email is sent to the office that has protective security markings higher than the X-IN-CONFIDENCE level, the email will be blocked before you receive it — both you and the sender will be advised
- if you select a classification higher than 'unclassified', you will need to file the document on a formal file with a least the same level of security classification.
- some agencies send emails with just 'IN-CONFIDENCE' set as the security marking. While we can receive these emails you should not create or send emails marked as just 'IN-CONFIDENCE'. You should select one of the available categories, COMMERCIAL-IN-CONFIDENCE, STAFF-IN-CONFIDENCE, SECURITY-IN-CONFIDENCE, or CLIENT-IN-CONFIDENCE.

Email good practice

The use of email, particularly in our complaint work, carries some risks for the office. You need to be aware of potential pitfalls that can be avoided or minimised:

- the tone and language used in work emails should be the same as that used in other forms of written communication

DISCLOSED UNDER FOI

- do not exchange information that could imply a personal relationship as this could be seen as a conflict of interest
- always ensure that your emails are properly signed – please use the approved signature blocks
- content of an email can easily be changed by a recipient – if this is a significant risk, capture the email on receipt and do not use reply with history to respond
- confidentiality cannot be assured because emails can be easily forwarded, reproduced or sent to an unintended recipient
- nothing should be written in an email that cannot be comfortably said in public
- large attachments sent by email, particularly to group addresses, should be avoided where possible
- use hyperlinks rather than attachments where possible [ctrl+K]
- check the document properties of any *Word, Excel* and *PowerPoint* attachments for title, subject and author
- include clear, concise headings and the Resolve number, if appropriate
- do not let your inbox build up – move items to folders if you are unable to immediately copy them to *Resolve* or place a copy on a formal file
- use BCC (blind copy) for distribution lists where privacy should be maintained.

Group emails

Purpose

The purpose of group email addresses is:

- so that investigation officers do not have to disclose their personal email addresses when corresponding with a complainant
- to ensure that incoming emails are responded to, even when staff are absent.
- The group email address may also be useful to provide as a contact when an investigation officer is about to take time off or leave the office.

Management of group email addresses

There should be a staff member responsible for checking and allocating each group's email. In the State Offices, it is suggested that this is the person who is also responsible for incoming mail. Responsibilities include:

- clearing the group email several times each day
- identifying the approach, registering it as an incoming document and allocating it to the appropriate investigation officer
- if the email does not relate to an existing approach, registering a new approach in *Resolve* and adding it to the pool for allocation
- forwarding the email to an 'interim' folder to ensure there is a copy for the short-term
- deleting the email from the inbox after forwarding it to the 'interim' folder
- deleting the email from the 'interim' folder after five working days.

Emails should be deleted from the outbox by the person who sent them after they have been copied to *Resolve* or the formal file.

DISCLOSED UNDER FOI

The manager of the team that has the group email address is responsible for ensuring proper management of the group email address.

Subject line in emails to departmental contacts

The subject line, when pursuing a complaint with an agency, should consist of 'Your ref: xyz; Our ref: 2008-******'. Add the name of the case only if the agency is on Fedlink. Otherwise the name of the complainant/case should be in the body of the email in the first line as:

Re: Joe Bloggs Complaint

Leaving the name out of the subject line for non-Fedlink agencies increases security slightly. If the other agency's reference includes the name then that also should appear in the subject line only for Fedlink agencies, or at the start of the body of the email in other cases.

Signature blocks

Personal email addresses

The Ombudsman has approved the use of standard signature blocks:

> [*First name*] [*Family name*]
> [position title] | [*Team*]
> COMMONWEALTH OMBUDSMAN
> phone [*XXX*] | fax [*XXX*]
> email [*XXX*]
> website www.ombudsman.gov.au
>
> Assisting the Australian community by resolving complaints and fostering good government administration

This signature block should be used in all outgoing emails except where the email is being sent from a group address.

Group email addresses

The approved signature block for a group email is:

> [*First name*] [*Family name*]
> [position title] | [*Team*]
> COMMONWEALTH OMBUDSMAN
> phone 1300 362 072 | fax [*office fax*]
> email [*group email*]
> website www.ombudsman.gov.au
>
> Assisting the Australian community by resolving complaints and fostering good government administration

Out-of-office messages

If you expect to be absent for more than one day, office policy is that you should install an out-of-office message on your email. To do so, click on Actions/tools/out-of-office, enter the dates you will be absent and a message about who to contact in your absence (with their contact details) and click on enable.