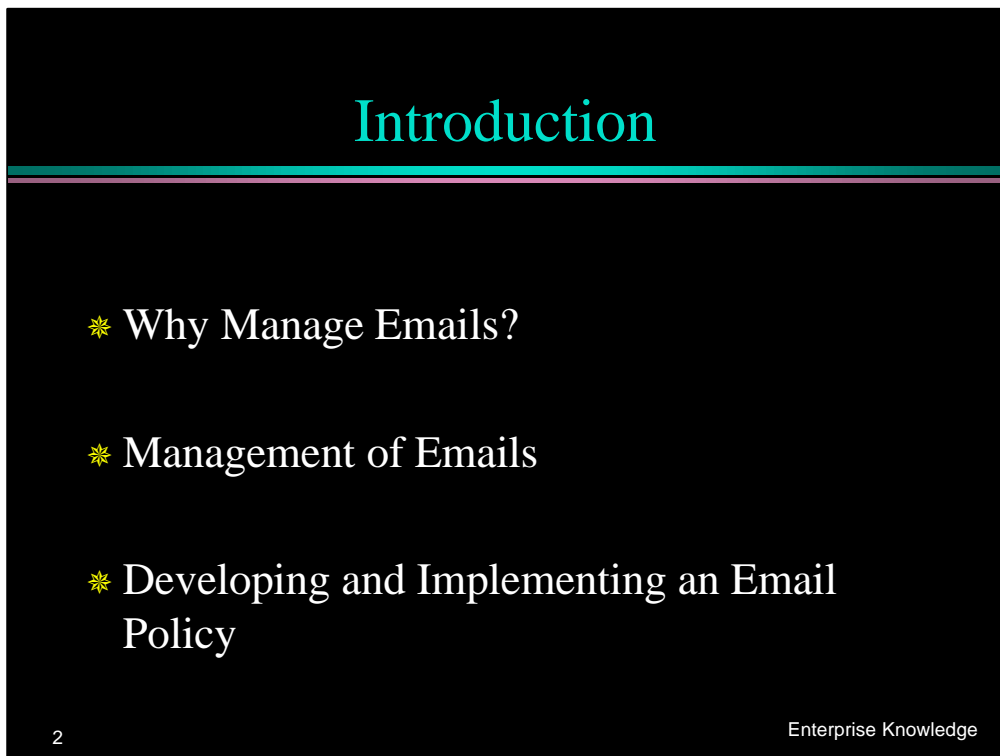


Managing Email - Effective Policies and Procedures

Jenny Robins, Senior Consultant, Enterprise Knowledge



1. after talking about the reasons for managing emails, I am going to very quickly look at:

2. some issues surrounding the management of emails:

- *Creation*
- *Capture*
- *Disposal*
- *Uses and Abuses of Email*

and then look at:

3. issues surrounding the development and implementation of a policy:

- *Roles/Responsibilities*
- *The existing Policy Framework*
- *Distribution/Communication*
- *Audit and Compliance*

Why Manage Emails?

- * Operational requirements including: finding and forwarding information
- * Minimise the risk of litigation (claims against co-workers and employers)
- * Reduce misuse
- * Reduce wastage of worktime
- * Uphold corporate value
- * Good business practice and meet accountability requirements.
- * Assist management of electronic storage space.
- * Emails are evidence!
- * To comply with legislation and standards.

3

Enterprise Knowledge

As more and more organisations - both public and private - use email systems to “do business” - there is an increasing need to apply good business practices - RM, HR, Risk etc - to ensure emails and the use of email systems are managed properly.

It is estimated that the number of electronic mailboxes will rise from 315 million in 1999 to 530 million in 2002, and the number of emails sent on a business day will increase from 5.3 billion to 14.7 billion.

Just a cursory look at the newspapers will indicate the number of email horror stories:

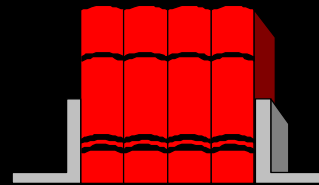
Ansett - woman successfully sued to be reinstated in her job. Ansett sacked her by saying using the email system to distribute union information was an inappropriate and disallowed use of the company’s email system. A breach of the Workplace Relations Act.

Telstra - a number of employees were disciplined (sacked) after being found to be storing and distributing pornographic material on the company system.

The silly doctor - One of my favourites: one of Australia’s leading medical experts has been forced to apologise for sending an email to 1200 drug and alcohol experts in which he made several sexist jokes about Senator Amanda Vanstone. Evidentially, he sent the email as a reply to an email he received as a subscriber to a professional discussion group - but he sent the reply to all recipients of the group, not just some “friends” who were in the group. Be careful!

Why Manage Emails?

- * Archives Legislation - Federal and State
- * Electronic Transactions Bill
- * Evidence Acts
- * Freedom of Information Acts
- * AS4390 - Australian Standard for Records Management
- * Workplace Relations Act
- * Privacy legislation
- * Criminal legislation
- * Sex, Race and Disability Discrimination Acts
- * Corporations Law



just read out this list....

as you can see it is not just legislation governing records management that applies to the use of email systems.


Management of Emails

- * Creation
- * Capture
- * Disposal
- * Uses and Abuses of Email
 - » Personal Use
 - » Privacy
 - » Netiquette



Message Creation

- * Content
 - » Accurate
 - » Authentic
- * Context
 - » What the system itself provides
 - » What people need to do



6 Enterprise Knowledge

Creation - records and documents are made - created or received- in the process of undertaking business activity by staff, regardless of the method/s or medium involved.

Content is the substance of the email. In email messages this may be in the body of the message or it may be the attachment transmitted with the message.

The content - including the metadata and the attachments should be:

Accurate - consider developing business rules and codes of conduct to ensure emails accurately reflect the transaction (especially if the email is part of your business). Examples - encourage spell checking, proof reading, adding an accurate subject line, introducing the practice of having certain types of emails checked by a superior before they are sent. (This could be done in a similar fashion to a letter being checked by a superior before it is mailed which has been and continues to be a common and regular business practice) *Anthony's example*

Authentic- it must be possible to prove that the document/record is authentic ie being able to prove that what they purport to be and that their purported creators have indeed created them. *NZ RM consultant example.*

{This example emphasises that good email management practices cannot exist in isolation from other policies and practices such as the IT policy and HR policy eg passwords on computers and staff "exit procedures"}

Security - Electronic mail systems are susceptible to unauthorised access and **electronic messages** are susceptible to manipulation. Electronic mail systems should have sufficient security provisions to ensure that only authorised users have access to the system.

Email Messages - Have you ever tried to change a message that you have received. What happens on your system?? does it allow you to save the changes? is it another message? or does the changed message become "the message"? Does the system verify that it is changed? ie does the systems indicate the message is not actually the one that was received?

Message Capture

* Methods for Capturing Messages

- » Printing to paper
- » Using the Email software
- » Using the directory tree/file manager structure
- » Using Electronic Document or Records Management Software (eg EDMS, ERMS)

7

Enterprise Knowledge

Capture is the deliberate action which result in the registration of a record/document into a recordkeeping system (also referred to as registration)

Each of these systems has advantages and disadvantages. These may be in relation to cost (upfront and ongoing), responsibilities, ability to retrieve (on-site versus offsite), ability to retrieve across the organisation, or within workgroups or only personally, how email objects are named (document naming conventions), whether or not they encourage “good” recordkeeping practices (in accordance with the Standard eg disposal/retention)

Interim measures as outlined in PROfile’s Advice to Victorian agencies on electronic recordkeeping:

- naming conventions of hardcopy filing systems applied to email folder structures as well
- print to paper.

Also consider setting up public folders where the information needs to be accessed by more than one person.

Most people already capture emails - personal “protocols” re which ones they will “file” and how they will file them

Show of hands

- print and add to hardcopy file
- setting up folders/subfolders in their email software
- EDMS/ERMS?
 - are these protocols corporate wide?
 - or are they varied and idiosyncratic?

which ever system is used -

- who is deemed responsible for “filing” the email - recipient or author?
- When is it captured? (each email, only at the end of a “dialogue”?)

Include them in your email policy!!! eg these type/s of emails will be captured using this method (remember this may change in the future!)

10/09/100

Disposal of Emails

- * Differentiating Records and Ephemera
- * Disposing of Records
- * Disposing of Ephemera

8

Enterprise Knowledge

Differentiating between records and ephemera:

Why?

Differentiate between emails that are records and emails that are ephemera because each has different requirements for retention, disposal, access etc.

Definitions

Records are recorded information in any format that provides evidence of a business transaction - **From Australian Standard 4390**

Ephemeral emails have little value after a short period of time, perhaps seconds after transmission or receipt. They may be personal or created or received in the course of business but have no continuing value. - **From: NSW State Records, Managing the Message**

Develop a list of questions that will assist all users understand how to distinguish between records and ephemera eg - is the email a business matter or personal? does the email authorise the expenditure of funds? is it formal communication between staff? is the email for information only? is it of a facilitative purpose (eg to organise a meeting).

Once agreed on, establish policies - link to the capture process and to the Disposal Schedule/Authority... **include in policy and train staff**

Uses and Abuses of Email - Personal Use and Privacy

- * Personal Use of Email
- * Privacy
 - » Privacy Commissioner's Guidelines on Workplace Email, Web Browsing and Privacy (March 2000)
<http://www.privacy.gov.au>



9 Enterprise Knowledge

Personal Use of the Email system:

similar to using the phone at work for personal matters? is it the same - not quite because the emails hang around. (remember Telstra)

SO -

- is it permitted?
- if so, what are the restrictions? are these based on types of material, OR hours when it is allowed (eg lunch time, before and after work hours etc)

Privacy:

don't have time to go through this - but wanted to inform you of these and provide you with the Web address.

“The purpose of the Guidelines is to recommend steps that organisations can take to ensure their staff understand the organisation's policy on this issue through the development of a clear policy”

Uses and Abuses of Email - Netiquette

- * Salutation
- * Signature
- * Subject Line
- * Language and Tone
- * Emoticons
- * Shorthand
- * ALL CAPITALS
- * Regular Mail Checks
- * Prompt replies
- * Resources - Time and Space
- * Subscriptions and Junk Emails

10

Enterprise Knowledge

A list of do's and don'ts

Provide a subject line, salutation and a complimentary closing (you are representing your business! and a signature file (name, title, organisation, address, telephone number, fax, Email address) **A signature is always useful if in fact your email address is gobbledygook!**

- Emails are non-verbal in their mode of communication, so be careful what you say. - an ironic response of “yeah sure” to an emailed offer of tickets to a Barry Manilow concert.
- use of ALL Capitals SHOUTING
- use of emoticons - those silly meaningless squiggles - do people at the other end understand them?
- use of email shorthand
- if you are cross, count to 10 (or 100), 1 company has its staff wait 24 hrs before sending or replying to emails - use the “draft” facility that is built into the system.

How do you improve the content of emails - consider your workplace, its culture and needs and how it uses or wants to use emails and then develop some guidelines for staff

Be courteous - check email system regularly and respond ASAP (even if it to say when you will have time to deal with the matter more fully

Use of attachments - be wary of the space they take up, avoid clogging up the server by sending email messages with large attachments if possible.

Space - think about who you are forwarding items (and attachments on to) and who needs to see your reply to a message if you have received the message that has been distributed to an entire address group

subscribing to news groups and list serves also take up space and time. Does everyone need to be a subscriber???

Developing and Implementing an Email Policy

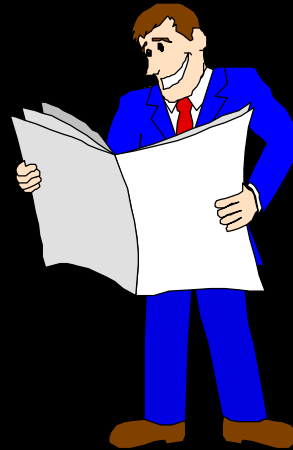
- * **Why have a policy?**
- * **Roles and Responsibilities**
- * **Existing Policy Framework**
- * **Policy Review**
- * **Documentation and Distribution of the Policy**
- * **Audit and Compliance Issues**

So you have thought about all these things and done some research and read the horror stories and you have decided on what you might want to include in your email policy...what now...

OK this is the last part... read this list out - what I want to cover

Why have a Policy?

- * to remove doubt
- * to minimise the risk of vicarious liability
- * protect IT system (eg from viruses)
- * maintain productivity/efficiency
- * protect reputation



A policy is a statement of the organisation's expectations on any matter. It acts as a guide to telling how staff should behave, including minimum standards, do's and don'ts and how to do things ...

The advantages of having a policy are here on the overhead...

Roles and Responsibilities

- * Information Technology/Services
- * Human Resources/Personnel
- * Legal and Risk Departments
- * Management
- * Process Owners
- * Others in your organisation?



13 Enterprise Knowledge

Development and implementation of an email policy cannot be done in isolation - a group effort - here are some - think of others in your organisation eg do you have a policy writing team?

Who will do what, and when will they do it??

eg write the policy , approve the policy, disseminate the policy, audit the policy, train existing staff, train new staff etc etc etc...

Existing Policy Framework

- * **Human Resources Policies**
 - * Codes of Conduct
 - * Induction and Exit
- * **IT Policies**
 - * Passwords
 - * Security
 - * Use of System
- * **Records Management Policies**
 - * Disposal
- * **Others?**

eg the Privacy Commissioner specifically mentions the Australian Public Service Code of Conduct which states that Commonwealth employees must use Commonwealth resources in a proper manner and behave in a way that upholds APS values and integrity and the good reputation of the APS.

Review of Policy

- * Review and Reissue your policy whenever a significant change is made (especially given the accelerating development of Information Technology and the Internet)



- Stay in touch with stakeholders - things change. Documentation should not be seen as anything but dynamic. Business needs change frequently, legislative requirements tend to change every now and then as well and IT may have plans that will impact so Stay in Touch! Update the documentation when required and reissue it - making sure staff know that it has changed and when they need to change what they do.

Distribution of Policy

* How?

- » hardcopy
- » intranet
- » reminder messages on computer

Documentation is only worth having if it is seen by the users.

No matter how well it is written it won't be followed if people can't find it or don't know about it.

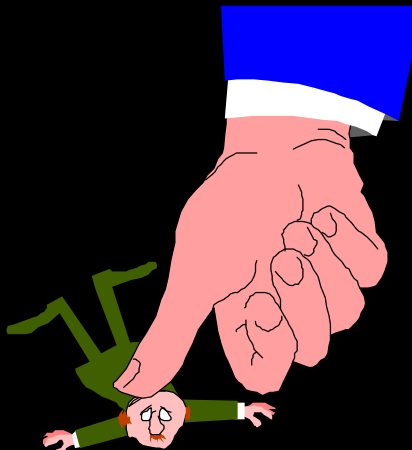
So:

- Have documentation readily available. Consider making it available electronically if that suits your workplace environment.

- Conduct training and awareness workshops and make sure new starters get trained as part of their induction. Link it to other records management or IT training if you have it.

Compliance and Audit

- * Who is going to audit the policy?
 - » Management
 - » IT
 - » Records Management
 - » Human Resources
- * What are the penalties (if any)?
- * Document these in the Policy.



The illustration shows a large, pink hand with a blue sleeve cuff, holding a small, green-suited person upside down by their collar. The person has a distressed expression. This visual metaphor likely represents the power imbalance or disciplinary action associated with compliance audits.

17 Enterprise Knowledge

To ensure that instructions and policy are complied with introduce a compliance audit. But do it in a careful and supportive manner.

Remember if you make the policy too strict you will have to discipline a lot of people.

I think the Privacy Commissioner made an excellent point when he said...

“Balancing the legitimate interests of organisations and staff may be difficult and this balance may vary in different organisations. Policy or practice which leads staff to believe that their privacy in the workplace is not respected may be regarded as intrusive and oppressive and have a negative impact on morale and productivity”

I think the same can apply if the policy demands that staff are made to do a lot of things they did not do before (eg filing), or cannot see the purpose or value of. So this may come down to broader training (eg legislation, RM practices etc) that can result in the successful implementation of your organisations email policy.

Jenny Robins
Senior Consultant
Enterprise Knowledge
Suite 1, 1014 Doncaster Road
Doncaster Vic 3109
Ph: (03) 9842 0999

email:jennyr@archivalsystems.com.au

