Guidelines on developing a policy for managing email

© Crown copyright 2004

You may re-use this information (excluding logos) free of charge in any format or medium, under the terms of the Open Government Licence. To view this licence, visit nationalarchives.gov.uk/doc/open-government-licence or email psi@nationalarchives.gsi.gov.uk.

Where we have identified any third-party copyright information, you will need to obtain permission from the copyright holders concerned.

This publication is available for download at nationalarchives.gov.uk.
Guidelines on developing a policy for managing email

Contents
Summary .................................................................................................................................................. 3
Introduction ........................................................................................................................................... 3
Audience .................................................................................................................................................. 5
Benefits .................................................................................................................................................. 6
The Purpose of an Email Policy .............................................................................................................. 7
Using Email (or Sending Email Messages) ........................................................................................... 9
  When to Use Email ............................................................................................................................... 9
  Writing Business Email Messages ....................................................................................................... 13
  Dealing with Sensitive Subjects ......................................................................................................... 14
  Misuse and Personal Use .................................................................................................................... 17
Managing Email Messages .................................................................................................................... 21
  Reasons for Organising your Mailbox ................................................................................................. 21
  Making your Mailbox Manageable ..................................................................................................... 24
Management of Public and Shared Mailboxes .................................................................................... 26
  Overview of Managing Public and Shared Mailboxes ...................................................................... 26
  Public Mailbox Folders ...................................................................................................................... 28
  Shared Mailboxes ................................................................................................................................ 29
  Levels of Responsibility ...................................................................................................................... 30
Identifying and managing email records .............................................................................................. 33
  Essential Principles ............................................................................................................................. 33
  Identification and Responsibilities ....................................................................................................... 34
  Managing Email Records with Attachments .................................................................................... 36
  When and Where to Manage Email Records ..................................................................................... 37
  Encryption and Managing Email Records ........................................................................................ 39
  Titling Email Records in an Electronic Records Management System ............................................ 39
Appendix 1 - Guidelines for Writing Business Email messages .......................................................... 40
Summary

This guidance provides advice on aspects and areas that should be considered when developing an organisational policy for managing email. The guidance addresses how email can be used as a business tool for internal and external communication and how these types of email communications should be managed as records. Although there is some advice about where email records should be managed the guidance does not provide detailed technical advice on the management of email records.

The guidance argues the case for why organisations need an email policy in terms of legal and business requirements. Advice is given to people developing email policies in a way that should help them recognise the various options available when deciding how their organisation should manage and use emails. The guidance provides text that could be used in an email policy, although it is advised that organisations do not use this text without first considering the impact of the policy or consulting with members of staff throughout the organisation.

This guidance covers two major aspects that need to be addressed in an email policy, how an organisation should define appropriate use of email and how email should be managed within the organisation. These two areas are examined in detail through breaking them down into subsections to enable a policy to be produced that covers the main aspects of sending and managing email messages.

Introduction

This guidance has been developed to fill a gap in authoritative guidance on email management for organisations to use when producing their own advice on the use and management of email. It advocates that organisations giving their staff email access should develop an email policy to reduce the likelihood of essential business records being lost and help prevent the inappropriate use of email that could result in legal action.
The purpose of introducing an email policy is to present the organisation’s perception about what constitutes appropriate use and management of email in relation to the business being conducted. The way in which email messages are used and managed can either help staff organise their work effectively or cause problems in terms of missing deadlines. In addition to the immediate benefits and disadvantages staff encounter with using email there are more serious consequences if email is not used appropriately including litigation and undesirable media attention.

In developing the email policy it will be necessary to consider a variety of different areas that relate to email use and management including, legislative requirements, business requirements and the rights of an individual; the resulting policy should take into account all these areas while facilitating effective communication. The policy should be presented through clearly defined statements detailing what is expected of employees with a brief explanation to ensure that advice on procedures is given while allowing the sender to choose the most appropriate style. In areas of the policy where non-compliance may result in disciplinary action this must be clearly indicated.

In order for an email policy to be effective it is essential that the policy is developed with the agreement and support of senior management and in collaboration with representatives from various groups throughout the department. In particular it would be necessary to have representatives from the following organisational groups, Records Management, Human Resources, Information Technology and Trade Union, as well as other members of staff representing their sections. Developing the email policy in collaboration with various organisational groups should help to increase awareness and acceptance of the policy. It should be noted that an email policy should not be developed by only focusing on current use of email as is this is usually an emotive experience and will not indicate whether current use is appropriate.

Simply developing an email policy and disseminating it among employees may not be enough to ensure that email is used appropriately. To ensure that the email policy is followed, it may be necessary to consider how to promote the policy and the type of training that might need to be developed. This guidance does not give any details of the procedures that would need to be developed for the adoption and implementation of an email policy, although it is suggested that these need to be considered carefully to ensure that the policy is followed.
This guidance provides details of the areas that should be covered when developing a policy for managing and using email. The guidance provides two types of assistance with drafting an email policy: the first is an explanation of the areas that should be covered in an email policy and the second is some sample text for including in an email policy. The explanatory text is written in black and the sample text follows in a box.

For example:

It is important to consider why a policy should be introduced and who should be involved in its development. For a policy to be successfully implemented, people throughout the organisation need to approve of its content.

Sample text:

This policy applies to everyone in [ORGANISATION]. It was developed in consultation with [GIVE EACH UNIT’S NAME] and was approved by them at [DATE]. This policy will be reviewed in [x] years.

The sample text can be copied and used within an organisation’s email policy, however it is advised that the sample text is amended to suit the organisation’s own needs according to the advice provided in the guidance for each section of the email policy.

Audience

This guidance has been produced to address information and records management needs of Central Government, Local Government and other Public Authorities when developing an email policy. Other organisations may also find the guidance useful when developing their own email management policies, although it should be noted that these organisations might have different needs that are not covered within this guidance.

The guidance is aimed at people who would be producing an organisational email policy, a general assumption has been made that this will be likely to be records managers, information managers or IT personnel. It is recognised that there might be other people who have
Responsibility for developing an organisational email policy and this guidance would be applicable for this purpose, however it is advised that if you are in this position you consult with your records/information management department and your ICT department during the drafting process.

This guidance does not assume that an organisation has an electronic records management system (ERMS) and can be used to indicate best practice when developing guidance on managing email records outside of an ERMS. Although this document does cover managing emails without an ERMS it does not provide detailed specifications for how this could be done in either shared drives or public mailbox folders. Using public mailbox folders to manage email records in the absence of an ERMS will be the subject of later guidance.

Benefits

The main purpose of an email policy should be to facilitate effective communication and ensure that appropriate records of those communications are maintained. Producing an email policy will clarify an organisation’s position on how email should be treated within the organisation. This type of clarification is necessary to help ensure that email is used in a way that an organisation abides by its legislative requirements, maintains email records relating to business and encourages staff members to write email messages that do not confuse the recipient.

Organisations have a number of legislative requirements that must be adhered to in relation to the management and use of email. They have responsibilities to ensure that people are not being abusive or writing messages where the content is untrue or could be construed as being untrue. Organisations need to ensure that they can abide by information legislation that applies to email including the Data Protection Act, Freedom of Information Act and Regulation of Investigatory Privacy Act. In ensuring that they comply with legislation that affects email use, organisations must also ensure that their staff are treated with respect and that their rights are not violated.

Developing an email policy that explains an organisation’s requirements about how people are expected to treat email and details the organisation’s procedures for complying with information legislation will help to prevent potential litigation. However, it should be noted that simply providing an email policy might not be enough to prevent litigation if the organisation has not
attempted to ensure that staff members are aware of the policy and understand the implications of its contents.

In addition to complying with legislative requirements relating to email, organisations also need to ensure that appropriate business records are maintained for audit and accountability purposes. It is important that organisations recognise that email can be treated as a record of a business activity and that failure to capture and maintain these records could be problematic when providing evidence about how a business activity was conducted and why it was done in a particular way. To ensure that appropriate email records are maintained organisations need to provide guidance on which email messages should be maintained and where they should be maintained.

Having an email policy is beneficial for members of staff as it clarifies where their responsibilities begin. An email policy can have tangible benefits to individuals if they and other members of staff follow the policy. These benefits can be that it is easier for people to identify and locate information that is required for business, meaning that enquiries can be responded to quickly. Following the email policy can also help individual staff members use email more effectively so that email messages are clearly expressed and the recipients will be able to quickly identify the appropriate actions for each message.

The Purpose of an Email Policy

When the email policy is being developed and if you are a part of that development process it is usually fairly clear what decisions were made at particular stages, making it easy to know why certain things are more important than others and how the policy should be used. If you are not part of the development process it is not always clear why a policy was developed or how it should be made, making it harder to know why there is a need to refer to a policy and how it should be used.

The introduction to the policy should make it clear why the organisation has developed an email policy and what the benefits will be to the organisation and individuals through adopting the policy. The benefits detailed should cover both business and legislative areas. To help staff to
understand the importance of the policy content an overview should be given of what the policy will include and how the policy should be used.

In addition to giving an explanation about what the policy includes and how it should be used, there needs to be a clear statement about who needs to read and abide by the policy. This is important otherwise staff members who should be abiding by the policy might think that it is only applicable to other people and not themselves. Having a clear statement about who is covered by the policy will ensure that there is no doubt concerning to whom the policy applies.

In summary, this section of the policy should indicate the reason and need for having a policy, providing an overview about how email should be used within the organisation. There should be a clear indication of the main problems encountered when using and managing email and the potential liabilities for both individuals and the organisation that could be incurred if the policy is not adhered to.

Sample Text:

Email is increasingly becoming the primary business tool for both internal and external communication and as a result should be treated with the same level of attention given to drafting and managing formal letters and memos. Email messages should not be treated as an extension of the spoken word because their written nature means they are treated with greater authority. As well as taking care over how email messages are written it is necessary to manage email messages appropriately after they have been sent or received.

There is a common misconception that email messages constitute an ephemeral form of communication. This misconception about how email messages can be used could result in legal action being taken against [ORGANISATION] or individuals. All email messages are subject to Data Protection and Freedom of Information Legislation and can also form part of the corporate record. Staff should also be aware that email messages could be used as evidence in legal proceedings.

This email policy sets out the obligations that all members of staff have when dealing with email messages. The policy was developed in
consultation with [GROUP]. There are two main sections within the policy: the first concentrates on sending email messages and the second concentrates on managing email messages that have been sent or received. Staff should ensure that they are familiar with the content of the policy and use it as a point of reference when dealing with email messages. To ensure staff members are familiar with the content of the policy [ORGANISATION] will provide training on the policy and keep staff aware of any changes that are made.

Using Email (or Sending Email Messages)

When to Use Email

Email messages tend to be used to communicate various types of information both internally and externally. Information communicated via email ranges from a formal record of proceedings to arranging refreshments for a meeting. Although it is possible for email to be used in a variety of ways it does not follow that email is always the best way of communicating.

There are both advantages and disadvantages to communicating via email and it is often the case that the advantages of sending an email are disadvantages for the person receiving emails. For example, email allows people to send information to many people at the same but it is a frequent complaint that too many email messages are received. To maximise the advantages and minimise the disadvantages of sending messages via email the organisation needs to decide if there are any circumstances when an alternative means of communication should be used in preference to email. For example to reduce email messages being sent to everyone in the organisation it might be necessary to review the way in which the intranet is used and introduce a procedure relating to sending email messages to everyone in the organisation.

The way in which email should be used for business communication will depend on the nature of the business of the organisation and partly on the culture of the organisation. For example some organisations might consider that discussions relating to the awarding of a contract should not take place via email and that email messages should only be sent as a way of ratifying a
decision. When deciding what advice should be given on how email should be used within an organisation there needs to be a clear understanding of the type of business that is being conducted, the way in which business is conducted and who are the various stakeholders involved. When drafting this section it should be recognised that it is likely to be the case that different areas of the organisation will use email in different and possibly opposing ways.

This section of the policy is intended to encourage staff to think about whether email is the most appropriate and timely way to communicate information. It is essential that this section is not too prescriptive as the decision to send or not send an email will be dependent on a number of factors. In the sample text for this section it is suggested that there are five major factors that affect the decision to send an email, these factors could be used as a basis for considering when it is appropriate to send, or not send, an email message. If there are specific instances when email should not be used to communicate information these should be referenced in this section, with a detailed explanation in the section on Email Misuse. Due to the personal nature of email messages members of staff should be made aware that it is their decision to write an email message and that they are responsible for what they have written in an email message.

Sample Text:

**Email is not always the best way to communicate information as email messages can often be misunderstood and the volume of email messages people receive can be prohibitive to receiving a meaningful reply as a result of email overload.**

It is the responsibility of the person sending an email message to decide whether email is the most appropriate method to communicate the information. The decision to send an email should be based on a number of factors including:

- The subject of the message
- The recipient’s availability
- The speed of transmission
- The speed of response
- The number of recipients
The Subject – Email messages can be used for different types of communication and can constitute a formal record of proceedings. The types of communication which email can be used for include general business discussions, disseminating information, agreement to proceed and confirmation of decisions made. Although email can be used for these types of communication, it may be necessary to consider whether the sensitivity of the information would be more appropriately communicated in a different way. Dealing with sensitive subjects in emails is addressed in more detail in section [#]. It should also be noted that there are certain subjects that should be avoided in email messages as they could be construed as discriminatory; this is covered in more detail in the section on email misuse, section [#].

Recipient’s availability – Email messages are often sent unnecessarily due to the ease and convenience of writing an email message. There are times when email might not be the most appropriate way of communicating with people, for example if a message needs to be passed onto a person in the same office speaking to them face to face might be more productive, particularly if they receive large volumes of email. If the person to whom the message is being delivered is not located in the office it might be better to phone them, depending on the subject or nature of the communication. When a message needs to be communicated to someone who is difficult to locate, for example they work in more than more office, then an email message should be sent in preference to speaking to them either face to face or via the phone.

Speed of transmission – Email messages can be sent and delivered to the recipient quickly, which makes sending an email message a good way of transmitting information if the information is needed quickly and the recipient is expecting the information. Where information needs to be communicated as a matter of urgency it is better to use the telephone.
**Speed of Response** – Although email message can be sent and delivered quickly there is no guarantee that the message will be read or acted upon immediately. One of the perceived advantages of using email is that it can be responded to at the recipient’s convenience. If a message needs to be acted upon immediately or requires a quick decision email is probably not the best way of communicating the information. Where an immediate action or response is required it is probably better to speak to the person directly and send email confirmation if it is deemed to be necessary.

**Number of Recipients** – Although email is often considered to be a good way of disseminating information to large groups it should be noted that there are some restrictions. The ability to send an email to everyone in [ORGANISATION] is restricted to [NAME] and senior management. It is advised that if a message needs to be conveyed to everyone at [ORGANISATION] the message should normally be placed on the Intranet. If the message is particularly important an email should be sent to [NAME] requesting that they send an email to everyone detailing the nature of the information and providing a link to the appropriate point on the Intranet. It should be noted that only email messages that are considered to be of immediate interest to the majority of staff at [ORGANISATION] would be sent to everyone.

It should be noted that there are similar arrangements if an email needs to be sent to everyone in a particular division or department. If you need to send an email to everyone in a particular division or department please send a message to the mailbox for the division or department where a decision can be made about whether the message can be located on their part of the intranet or a oral message can be given at a departmental meeting.
Writing Business Email Messages

Email messages are often treated as a form of ephemeral communication even when they are used to communicate business decisions. One of the reasons for email messages being treated as ephemeral is because it can be difficult to distinguish between ephemeral and business communication, particularly in the case of internal email messages. It is important that the same care and attention is taken to compose an email message as a formal business letter or an internal memo otherwise there is a danger that the intended message will not be understood or acted upon in the appropriate way.

Although many members of staff will take care when sending external email messages the same level of attention is not always given to internal messages, even though the email message might provide the only evidence of an important business decision, for example agreement to proceed with a contract. It is important that staff are aware that in the electronic environment of writing email messages the rules for conducting formal communication are similar to the paper environment of sending formal business letters particular in respect to rules for grammar and spelling. There are some special conventions for email communication that staff should be made aware of in relation to both internal and external email communications, for example not writing in capitals as it can be construed as shouting.

This section should provide pointers and guidance on how to construct email messages as opposed to presenting definitive rules. The guidance should enable staff to use their own style of writing while informing them of ways to ensure that the recipient will react in the intended manner, for example using an urgent flag in the appropriate way can ensure that the message is acted upon quickly. It is suggested that the aim of this section should be to encourage staff to think about the message they are writing before it is sent. Guidelines detailing areas to consider when drafting an email message could be appended to the main policy so that they could act as a quick reference tool.

Sample Text:

```
When writing business email messages it is important that consideration is given to the way in which the message is being conveyed. This includes thinking about the title, the text and the
```
addressees. As a way of helping staff to draft emails in an appropriate fashion for business use guidelines to drafting email messages have been developed. These guidelines are intended to be a reference tool. It is up to the sender to decide to what degree to follow the guidelines, depending on their knowledge and level of familiarity with the recipient.

The guidelines are appended to the main policy.

Dealing with Sensitive Subjects

Information relating to some subjects is too sensitive to be sent via email. The precise nature of this information will vary according to the organisation concerned. There are three broad areas of sensitive information that could potentially be communicated via email, information with National Security implications, information considered as commercial in confidence and personal information. It is important that these types of information are communicated with care as if these types of information are communicated to the wrong people it could result in the organisation and or members of staff concerned being involved in legal action or undesirable media attention.

When formulating the area of the email policy associated with handling sensitive subjects it is necessary to ensure that the policy is relevant to all the main types of sensitive information an organisation holds. It should be noted that the three types of sensitive information mentioned in the guidance are illustrative, some organisations may not hold all three types of sensitive information and some organisations may hold other types of sensitive information.

Once it has been established what are the different types of sensitive information held by the organisation it will be necessary to decide the permissible ways of communicating each type of information. When considering how particular types of information should be communicated it will be necessary to consider if email is to be used whether any additional protection is required, for example connecting to the Government Secure Intranet, encryption methods and disclaimers. The decision about which type of protection is required should be made according to the nature and type of business that is conducted.
Technical methods used to protect sensitive information sent from an organisation should be considered carefully before they are implemented. For example, if it is decided that a method of encryption will be used it will be necessary to decide who will have access, the circumstances when encryption should be used and to ensure that the intended recipients have compatible systems.

Using a disclaimer is a frequent method used to protect organisations from legal action if inappropriate information is sent from an email address originating from an organisation’s server. Although it may be prudent to use disclaimers as they may provide the organisation with some protection against potential legal action there is no guarantee that this will be the case. A more effective preventative measure against legal action would be to ensure that members of staff are made sufficiently aware about the types of information that should not be transmitted via email through an email policy and training.

This section should provide a clear indication about how sensitive information should, or should not, be communicated via email. It should not be necessary to list every specific type of sensitive information, although enough information should be given about the different types of sensitive information the organisation holds so that members of staff can identify sensitive information and understand how it should probably be treated. It is important that members of staff are aware that it is their responsibility treat and communicate sensitive information appropriately, ie decide whether or not it can be sent via email.

It is particularly important that this section contains a clear message that members of staff need to be extra cautious when writing and sending email message that include personal details or where comments are made about the performance of a specific staff member or a group of staff. If there are any specific restrictions on the types of information that the organisation allows to be sent via email these should be given in detail, for example all disciplinary matters must be either dealt with either in person or on paper, email should not be used for this purpose.

Sample Text:

```
The privacy and confidentiality of the messages sent via email cannot be guaranteed. It is the responsibility of all members of staff to exercise their judgement about the appropriateness of using email when dealing with sensitive subjects. Staff are advised that all
```
external emails have a disclaimer at the footer of the email to protect [ORGANISATION] from information being disclosed to unauthorised personnel, however there is no guarantee that this will protect individual personnel from potential legal action if emails sent include unsupported allegations, sensitive or inappropriate information.

Staff must ensure that all information of a sensitive nature that is sent via email is treated with care in terms of drafting and addressing. Sensitive information sent via email that is incorrect might provide a case for initiating legal proceedings against the person sending the information and/or the [ORGANISATION]. Sensitive information can include commercial information, information about specific individuals or groups and information covered by national security classification.

When sending email messages that contain sensitive information the following aspects MUST be considered:

- Information that has a National Security Classification higher than [CLASSIFICATION LEVEL] must not be sent via email.
- If it is known that the computer system of an external email message cannot contain information of a National Security Classification higher than [CLASSIFICATION LEVEL] the information must not be sent via email. If in doubt do not send the information via email.
- Email messages containing information that is not intended for general distribution should be clearly marked either in the title or at the beginning of the message, for example an email message containing comments about the performance of a specific staff member or a group of staff. This should decrease the likelihood of the message being forwarded to unintended recipients.
- Email messages containing personal information are covered by the Data Protection Act and must be treated in line with the principles outlined in the Act. Under the Data Protection Act personal information includes opinions about an individual or the personal opinions of an individual. Email messages containing this type of information should only be used for the purpose for which the information was provided, be accurate and up to date, and must not be disclosed to third parties without the express permission of the individual concerned.
- Email messages that contain information that is not supported by fact should indicate that it is the sender's opinion that is being expressed.
The encryption of email messages is advocated in the following circumstances [LIST CIRCUMSTANCES]. The type of encryption recommended by [ORGANISATION] is [NAME], for further information on using encryption see [APPENDIX #].

Where a method of email encryption has been used this must be communicated separately to the recipient.

Misuse and Personal Use

The informal way in which email can be used can result in things being written which people would consider to be inappropriate writing in a letter or distributing to wide and unknown audience. As email is often used in an informal way to communicate information and opinions there is a misconception that it can be treated on a par with speech. However unlike speech it can be difficult to convey the precise meaning and the written nature of email means that if an opinion is expressed that might cause offence evidence can be produced to substantiate any disciplinary or legal action.

The broadcasting capabilities of email and the penalties of sending abusive emails are much higher than if they were spoken. This is particularly true if defamatory comments (untrue comments made about an individual or organisation that lowers its standing in society) are made as the broadcasting nature of email means that it is likely to be treated as libel and therefore there is no requirement to prove damage¹.

Email misuse can be a problem within organisations and can also be difficult to detect. There are a variety of different types of email misuse ranging from excessive personal use of email to making discriminatory remarks. Organisations have a responsibility to ensure that all members of staff are aware about what types of comments are unacceptable in email messages. If members of staff are unaware about what constitutes email misuse an organisation could be held accountable for email messages sent by individual members of staff. It should also be noted that unless members of staff are made aware about what constitutes misuse it might not be straightforward to issue disciplinary procedures.

¹ Lloyd, Ian J (2000) Information Technology Law, Butterworths
It is important that organisations decide what types of email communication constitutes misuse within their organisation and communicates this to all members of staff. It is recommended that when an organisation develops the area of their email policy on misuse it reflects the contents of any existing policies on equal opportunities, discrimination and disciplinary matters. It is also recommended that these policies indicate they also apply in an email environment. It is advised that this section of the email policy in particular is clearly visible and accessible to everyone working within the organisation.

Organisations should consider the degree to which work email accounts can be used for personal use. There are no specific guidelines on the degree to which email should be permitted for personal use, although preventing members of staff from using work email accounts for personal use may be considered to be too strict. It is important that a sense of proportionality is maintained when restricting the level of personal use. It might be worth incorporating the limitations of personal email use in the terms and conditions of employment as a way of clarifying and enforcing what the organisation’s expectations are in relation to employees using email. If staff are allowed to use work email accounts for personal use organisations must be aware of their obligations under article 8 of the Human Rights Act that states, ‘Everyone has the right to respect for his private and family life, his home and his correspondence.’

Giving advice on what constitutes email misuse is relatively easy however, policing the misuse of email can be difficult. In order to detect instances of email misuse it might be necessary to rely on complaints. Monitoring email messages may be one method of gathering evidence of email misuse. The implications of monitoring should be fully and carefully considered before it is agreed because of the sensitivities involved.

The Information Commissioner has issued detailed guidance on what needs to be considered when monitoring employees activities in the workplace.\(^2\) In essence the guidance states that if employees activities are monitored (including email) there is a need to clearly explain to all members of staff when monitoring would take place and the procedures that will be followed. It is also necessary to ensure that when monitoring takes place the individuals, whose activities are being monitored, are aware they are being monitored and which activities are being monitored,

---

for example email use. In order to comply with Data Protection legislation it is also necessary to explain how the data collected from monitoring will be treated.

This section should give an unambiguous overview of the types of unacceptable email use. The way in which this section is referred to will depend on its links to other policies. The sample text provided gives an indication of the main types of email misuse however, there may be additional types of misuse that organisations need to mention which relate specifically to the nature of the business being conducted.

Sample Text:

There are types of email use that are expressly prohibited and could result in formal disciplinary proceedings. In addition all members of staff are advised that email messages can constitute a formal record and can be used as evidence in legal proceedings. For further information on managing email messages as records refer to section [#].

When writing email messages the following conditions must be met:

- Any behaviour or comments that are not permitted in the spoken or paper environment are also not permitted in email messages.
- Care should be taken when composing email messages to ensure they are inoffensive and cannot be construed as harassment. Downloading and forwarding material of a pornographic, sexist, racist or derogatory nature are all prohibited, refer to the [NAME OF POLICY] for further information about what exactly constitutes this type of behaviour.
- The impersonal nature of email messages can mean that it is easier to cause offence than when speaking. If you are annoyed or angry about something take time to ensure the message does not inflame the situation.
- Email messages containing inaccurate information in the form of opinion or fact about an individual or organisation, may result in legal action being taken against the person sending the email message and anyone forwarding the email message on to others.
- The forwarding of chain mail is not permitted.
- The terms and conditions of the policy on [NAME OF POLICY relating to computer use] must be abided by.
- It is not permitted to conduct any business other than that of [ORGANISATION] via email.
- Only authorised personnel should access email accounts.

A restricted level of personal use of the work email account is permitted provided the following conditions are met:

- The sending of email messages does not interfere with work commitments.
- The email messages do not constitute misuse of email, as detailed above.

To protect the email network email messages are routinely scanned to ensure they do not contain viruses. Email messages that are suspected of containing viruses will be retained by [NAME]. An email will be sent to the intended recipient asking them if they are expecting an attachment. The email message and the attachment will only be forwarded if an affirmative reply is received. The email message and the attachment will be retained by [NAME] for [# WEEKS] before being deleted.

Members of staff are advised that the content of email messages will be monitored if they are suspected of misusing email or excessive personal use. However, the content of email messages is not routinely monitored. Any member of staff who has the content of their email messages monitored will be informed before the monitoring takes place. If no further action is to be taken as a result of monitoring the content of email messages then all the data collected as a result of the monitoring will be destroyed immediately. If further action is taken as a result of monitoring the content of email messages the data will be stored for [X] years.
Managing Email Messages

Reasons for Organising your Mailbox

As email messages are used for a variety of purposes it is likely that the mailbox of any individual will contain a range of email messages, for example informative emails, discussions and agreements to proceed. It is often the case that the nature of the information that is contained within an email is difficult to determine without reading the email. As email messages are not always clearly identifiable without reading the message and there can be a large number of email messages in a mailbox, it can be hard to locate email messages that contain specific information. Email messages containing specific types of information will be easier to locate if the email messages that are records are identified, removed from the personal mailbox and retained with other records and if the mailbox is organised so that like types of information are contained within the same folder.

If mailboxes are not organised there is a possibility that some types of information will not be found, meaning that the information is effectively lost. The loss of information can mean that it takes longer to conduct business or make it difficult to comply with requests for information under the Data Protection Act and the Freedom of Information Act. Requests for personal information under the Data Protection Act or other types of information under the Freedom of Information Act are likely to be contained in the content of the email and are not always going to be obvious from just the address details (sender and recipients) or the subject matter. Difficulties in not being able to identify specific information in email can be avoided by encouraging members of staff to organise their mailbox.³

To make it easier to locate information that is held in mailboxes it is important that a clear message is given to all members of staff explaining why it is necessary to organise and manage their mailbox. Members of staff need to be aware of both the legislative and business reasons for organising their mailboxes. The message about organising mailboxes needs to be communicated

³ If further information is required on identifying information covered by and answering information requests under the Data Protection Act or Freedom of Information Act refer to the guidance produced by the Office of the Information Commissioner.
in a way where members of staff will be able to identify personally with the reasons, for example referring to the business needs of staff.

Effective email management will benefit members of staff and the organisation as a whole. To ensure that members of staff recognise the need to manage email messages it is important that they take responsibility for managing their own mailboxes, which means that members of staff are responsible for locating any information that is held in their mailbox. There should be an explicit message that members of staff are responsible for managing their own mailbox and that they need to allocate time for this purpose. To help members of staff to organise their mailbox they should be given an explanation about what is meant by organising a mailbox, for example identifying records of business activities, creating folders to contain similar email messages and deleting email messages no longer required in a timely fashion.

Although it is important to encourage members of staff to organise their mailboxes it can be difficult to see if this is happening. There are ways of motivating staff to manage their email messages, for example introducing auto-deletion and restricting mailbox size, but these should only be introduced after careful consultation and preparation to ensure staff are capable of managing their mailboxes. The type of preparation required includes:

- ensuring there are appropriate backups
- ensuring that the retention periods for email inside the mailbox are understood
- ensuring that staff are able to identify email business records and have somewhere secure to manage these

This type of preparation is important to ensure that valuable information will not be lost through staff not managing their email messages appropriately. Note that imposing these measures on the mailboxes of everyone in an organisation cannot be used instead of providing guidelines about organising mailboxes.

In addition to members of staff organising their mailbox to help locate email messages in their mailbox relating to different types of information, it might be necessary to locate email messages in the mailboxes of members of staff who are absent. It is likely that all mailboxes will contain some personal email messages which means there need to be clearly stated procedures and reasons for granting access to the mailbox of an absent member of staff. Failure to develop and publish procedures on granting access to the mailbox of another member of staff could result in an accusation of non-compliance with section 8 of the Human Rights Act or the Regulation of
Investigatory Privacy Act. It should be noted that drafting these procedures requires a thorough consultation within the organisation.

This section of the email policy should be used to explain why it is important for mailboxes to be organised. The need for organising mailboxes should be explained in a way that members of staff will relate to themselves, impressing upon them that it is their responsibility to organise their mailbox. If the organisation takes any measures to encourage staff to organise their mailbox, for example auto-deletion after a number of months, this must be stated. There should also be a clear statement on the procedures that should be followed if the mailbox of an absent member of staff needs to be accessed.

Sample Text:

It is the responsibility of all members of staff to manage their email messages appropriately. It is important that email messages are managed in order to comply with Data Protection and Freedom of Information legislation. Managing email messages appropriately will also mean that work can be conducted more effectively as it will help towards locating all the information relating to specific areas of business.

To manage email messages appropriately members of staff need to identify email messages that are records of their business activities and ephemeral email messages. It is important that email messages that are records are moved from personal mailboxes and managed with, and in the same way as other records (see section [#]).

Ephemeral email messages should be managed within the mailbox and kept only for as long as required before being deleted.

Staff are advised that email messages are automatically deleted from the mailbox after (number of weeks/months) and that to prevent loss of information email messages must be acted upon and moved to an

---

4 Personal mailbox includes the inbox, where you receive emails which are addressed to yourself, folders created under the inbox, where emails from your inbox might be moved to, and the sent box, where email addressed from you are sent to other people.
appropriate location as quickly as possible.

There may be occasions when it is necessary to access email messages from an individual’s mailbox when a person is away from the office for an extended period, for example holiday.

The reasons for accessing an individual’s mailbox are to action:

- Subject access request under the Data Protection Act
- Freedom of Information request
- Evidence in legal proceedings
- Evidence in a criminal investigation
- Line of business enquiry
- Evidence in support of disciplinary action

Where it is not possible to ask the permission from the member of staff whose mailbox needs to be accessed, the procedure for gaining access their mailbox is:

- Gain authorisation from [NAME, maybe Head of Department]
- Submit a request to [NAME, maybe IT personnel]
- Access is gained in the presence of [NAME and NAME, could be Line Manager rather than a named person]
- A record is made of the reasons for accessing the mailbox together with the names of the people who were present.
- Inform the person whose mailbox was accessed.

It is less likely that this procedure will need to be followed if email records are managed appropriately or mailbox access has been delegated to a trusted third party.

**Making your Mailbox Manageable**

Encouraging members of staff to organise and manage their email messages should be accompanied with some practical advice about how email messages could be managed. This type of advice is essential because it is likely that there will be some members of staff who will find managing their mailbox a difficult and onerous task, particularly if they receive large volumes of email messages.
There are a number of facilities that email clients can provide to help people to organise their mailboxes making them manageable. Familiarity with the features for organising email messages could help people to identify particular messages, for example MS Outlook has a feature that can give different colours to received emails depending on whether a person’s name is in the ‘cc’ field and ‘to’ field. Members of staff who receive excessive quantities might require additional support to organise their mailbox, for example advising on the creation of appropriate folders to group messages together or using an automatic filter to file email messages.

There is no right way to organise a mailbox and it is important that people find the best way to organise their own messages. However, it is likely that many members of staff are uncertain about how to being organising their mailbox and will need some guidance on how to begin. This section should be used to provide some practical advice about how to organise and prioritise email messages. The prepared text below is intended as generic advice on the type of information that could be given to members of staff and does not necessarily reflect the capabilities of every email client. It is advised that the people producing the guidance are familiar with some of the advanced functionality of the email client used by their organisation so that they can customise the guidance to reflect the capabilities of the email client used.

Sample Text:

<table>
<thead>
<tr>
<th>Managing an email mailbox effectively can appear to be a difficult task, especially if the volume of email messages received is regularly of a large quantity. Managing an email mailbox should not be about following rigid classification guidelines; it is about following a methodology that works best for you.</th>
</tr>
</thead>
<tbody>
<tr>
<td>There are a number of approaches that might aid the management of email messages. These approaches that might be worth further consideration are:</td>
</tr>
<tr>
<td>Allocating sufficient time each day or week to read through and action email messages</td>
</tr>
<tr>
<td>Prioritising which email messages need to be dealt with first</td>
</tr>
<tr>
<td>Looking at the sender and the title to gauge the importance of the message</td>
</tr>
<tr>
<td>Flagging where you have been ‘cc’d’ into email messages. These messages are often only for informational purposes and do not require immediate/any action</td>
</tr>
</tbody>
</table>

Last updated March 2004
Management of Public and Shared Mailboxes

Overview of Managing Public and Shared Mailboxes

Public and shared mailboxes can be potentially difficult to manage because they rely on everyone who is using them to work collaboratively. As the use of public and shared mailboxes is a complex issue it will need to be explored in more depth in subsequent guidelines. The points made in this section are intended to reflect the main issues that should be considered when drafting a policy on the use of public and shared mailboxes rather than definitive guidelines.

For the purpose of this guidance the issues relating to public and shared mailboxes have been grouped together as there are a number of similarities in the way they can be managed. When organisations are drafting their own email policy it might be felt to be more prudent to separate these into two separate areas to reflect their different uses. This guidance has assumed that a public mailbox is open to everyone in an organisation, that it is split into folders and that the folders are used for discussing discrete areas of work, while a shared mailbox is used for sending queries or information relating to a particular area of work conducted by an organisation. It is recognised that this is not the potential only use of a public mailbox as they could be used for managing email records, however it is advised that public mailboxes should be used for only one purpose.
Sample Text:

Managing shared mailboxes and public folders – In the case of shared mailboxes management is likely to be shared between everyone who has access. In the case of public mailbox folders management the folder owner should be responsible. The purpose of managing email messages, whether they are in shared mailboxes or in public folders is to identify emails that should be retained as a record of an activity and delete ephemeral messages.

When managing shared email mailboxes, the sections of this email policy relating to, ‘reasons for organising your mailbox’, ‘making your mailbox manageable’ and ‘identifying and managing email records’ should be adhered to. There will also need to be some additional rules relating to when to delete an email message from the mailbox, how to identify an email message as having been answered and the types of email messages that should be treated as records. While it is the responsibility of the owner to ensure that there are specific rules relating to the management of shared mailboxes it is the responsibility of all staff members with access to shared mailboxes to abide by those rules.

When managing public mailbox folders the owner of the folder should provide some clear rules as to how the mailbox will be managed, this should include:

- The purpose of the folder
- How long messages will remain in the mailbox before being removed
- An indication of the length of time the folder will exist, where possible

The owner of the folder must ensure that the messages remain in the folder no longer than the pre-agreed time period. After this time they should either be deleted or managed as records of the discussion. It is also the responsibility of the folder owner to delete the folder once it is no longer required and ensure that all email messages that all non-
ephemeral email messages are captured as records of the discussion.

It is important to remember that any email that made a significant contribution to the discussion of the business being conducted should be captured as a record and not just the final conclusions. The discussions that take place in the mailbox folder will represent the context within which the final decision was made and must be maintained as a record of the proceedings.

Public Mailbox Folders

When a public mailbox folder is created there should be a clear idea about why it has been created, how it should be used and who will be using the folder. For example a folder could be created to discuss issues relating to a particular project, with the intention that people who are taking part in the project use the folder. Having an awareness of the purpose of the folder can help keep the focus of the discussion and enables the owner to take action where the discussion is associate with the intended purpose of the folder.

There needs to be some guidance on how long the discussions in the public mailbox folder will be accessible in the folder before they are removed, together with their new location. This might be partly influenced by the length of time it is anticipated the folder will be required for discussion purposes. It is advised that if the public mailbox folders are used for these types of discussion they are not used for managing the records of the discussion, which means they will either need to be printed to paper, managed within an ERMS or managed in a different and distinct public mailbox. Public mailbox folders that are used for discussion purposes should not be used for long-term management of email messages.

An important point to remember when producing guidelines on the management of public mailbox folders is that all of the email messages should be evaluated to determine which email messages should be retained as record of the discussion and not just the conclusions at the end of the discussion. It is necessary to decide which parts of the discussion should be retained as records as there may be a need to justify the final decision.
Sample Text:

The public mailbox is accessible by everyone in [ORGANISATION] and is organised into folders. The public mailbox should be used for people across [ORGANISATION] who want to discuss and share ideas relating to a particular area of work. Different folders should be used for discussing different topics. The public mailbox system works by staff members placing email messages into the relevant folder and other members of staff replying to the email messages that already exist. Access to folders in the public mailbox is open to everyone, unless the member of staff who is responsible for managing the folder makes a specific request to the contrary.

Shared Mailboxes

When shared mailboxes are created there should be a clear idea about the purpose of the mailbox, who will have access to the contents of the mailbox and who is likely to send email messages to the mailbox. For example, a mailbox might be required to answer IT related queries; the people who would require access would need to be work on the IT helpdesk and the people who are likely to use it are anyone within the organisation who has access to a computer. Although it might be difficult to know precisely who will send email messages to a shared mailbox, but this may help influence how many people will need access to the mailbox.

The owner of the shared mailbox needs to decide and communicate to the other users how to treat the email messages that will be received in the mailbox. The owners of the mailbox should consider the following aspects:

- Who should answer which email messages
- How can it be determined that someone has responded to an email message
- If someone has replied to an email should the received email or the reply remain in the mailbox
- Who has the responsibility to capture records of the email messages
- Where will the email records messages received and replied to be maintained
The issues relating to who should respond to which email messages will depend on who has access to the mailbox and the type of emails that are received and will need to be determined by the owner. The issues relating to capturing records of the email messages received in the shared mailbox will be similar to those relating to personal mailboxes. Although, with personal mailboxes the line manager would provide some guidance about what needs to be captured as a record and where to file a record, in a shared mailbox the owner should provide this guidance.

Sample Text:

Shared mailboxes should be used where there are a group of people responsible for the same area of work. Where there are a group of people responsible for the same work using a shared mailbox can be a way of ensuring that queries are answered quickly when members of the team are away from the office. Access to a shared mailbox is initially given by [UNIT] and can be granted by the person who owns the mailbox.

Levels of Responsibility

The management of public mailboxes and shared mailboxes has two main levels. The first level is the unit/department in the organisation who has responsibility for controlling access to the mailboxes. The second level is the owner of public folder or shared mailbox that has responsibility for overseeing the daily management of the folder or mailbox. These two levels have specific responsibilities that when combined should ensure that people using either public mailbox folders or shared mailboxes are aware of how the contained email messages should be treated.

It is advised that general guidelines should be given on how to manage public mailbox folders and shared mailboxes. These guidelines should be supplemented by more specific rules developed by the owner of the mailbox or folder reflecting the way in which the shared mailbox or public folder will be used. The general guidelines should be developed in collaboration with the whole of the organisation but overseen by the unit/department, which controls access to mailboxes. The guidelines on managing public mailbox folders and shared mailboxes should
include usage guidelines (these could be similar to those required for email) for everyone in the organisation and instructions to the public folder/shared mailbox owner on their responsibilities.

All folders within a public mailbox and all shared mailboxes should have an owner. It should be the responsibility of the unit/department controlling access to public folders/shared mailboxes to ensure that these all have an owner allocated. It should also be the responsibility of the unit/department controlling access to public folders/shared mailboxes to ensure that all owners are aware of their own responsibilities.

The owners of public mailbox folders/shared mailboxes need to develop some specific rules relating to the management of the public mailbox folders/shared mailboxes. To enable the owners of public mailbox folders/shared mailboxes to develop appropriate rules they will need to be given some instructions on the areas this should cover. The instructions for developing rules for managing public mailbox folders and shared mailboxes will be different.

Sample Text:

Although the purpose of shared mailboxes and public mailbox folders is different there are some similarities in the way in which they should be organised. If a shared mailbox or a folder in the public mailbox is going to be used the following areas must be addressed so that the email messages contained do not become unmanageable and appropriate records are identified:

- Identifying an owner
- The purpose
- Access
- Managing the contents of shared mailboxes and public folders

**Identifying an owner** – When a public folder or a shared mailbox is created one person must be identified who can take ownership of the folder or mailbox. For public mailboxes this person should be responsible for ensuring that the topics being discussed do not change too radically from the purpose for which the folder was created. In shared folders the owner should be responsible for developing rules governing how email messages are responded to and how this is
communicated to other people using the shared mailbox.

It should be noted that [UNIT] has overall responsibility for maintaining shared mailboxes and public folder. If the owner has any specific problems with managing the shared mailbox or public folder these should be discussed with [UNIT].

**The purpose** – The creation of a public folder or a shared mailbox should be done with a specific purpose, for example a public folder might be created to discuss a particular policy area and a shared mailbox might be created to answer queries on a particular subject. It is the responsibility of the owner of the shared mailbox or the public folder to ensure that the mailbox or public folder is used for the specified purpose. If the shared mailbox or public folder is not being used for the specified purpose the owner should take appropriate action. In the case of a shared mailbox this might be suggesting the sender a more appropriate place to send their enquery. In the case of public folders the owner should act as a kind of virtual chairperson of the discussion and act as a mediator if the discussion is drifting from the original purpose.

**Access** – The level of access granted for shared mailboxes and public is likely to be different. For shared mailboxes access should only be granted to people who are able to answer the email enquiries that will be received. In shared mailboxes it might also be necessary for the owner to delegate some responsibility to other people who are granted access in terms of managing the emails and ensuring the mailbox is used for its specified purpose.

In terms of people sending messages to the mailbox it will be necessary to ensure that a message is given to people who might want to send enquiries giving the email address and the purpose of the mailbox, this can be done on a website.

The default access to all public mailbox folders is that everyone in the organisation can view the contents of all the folders. When the folder is
created everyone who might be interested in contributing to the discussion should be informed of the existence of the folder. As everyone in [ORGANISATION] has access to the folder the owner of the folder needs to ensure that the email messages posted are relevant, where the email messages are irrelevant the owner can delete the messages, having informed the sender why they are taking this action.

Identifying and managing email records

Essential Principles

The written and permanent nature of email messages means that they should be treated as records of business activities. As email can be used for a variety of purposes, email messages are not always treated as records of business activities leading to important records being lost potentially leading to difficulties in accounting for decisions and actions taken. To ensure that there is a full record for evidential and accountability purposes it is important that everyone in an organisation who uses email for business purposes is aware that email messages might need to be retained with the formal business records and how these email messages should be treated.

In composing this section of the email policy it will not be possible to give advice that defines precisely when an email should be managed with the other business records, but it should be possible to give enough information so that members of staff should be able to take responsibility for managing their own records.

Sample Text:

Email messages can constitute part of the formal record of a transaction. All members of staff are responsible for identifying and managing emails messages that constitute a record of their work. When an email is sent or received a decision needs to be made about whether the email needs to be captured as a record. Once an email message has been captured as a record it should be deleted from the
email client. The main points to consider when managing email records are:

- Identifying email records
- Who is responsible for capturing email records
- Email messages with attachments
- When to capture email records
- Where to capture email records
- Treatment of encrypted email records
- Titling email records

Identification and Responsibilities

Email messages can be used as records of business activity. The types of emails that might need to be managed as a record include discussions, information distributed to groups of people, agreement to proceed and other exchanges relating to the discharging of business. Email messages can provide evidence about why a particular course of action was followed which means that it is necessary not just to capture the email relating to the final decision but discussions that might indicate why one decision was made as opposed to another.

All members of staff must be able to identify which email messages should be captured as a record in relation to their work. In this context capturing a record of work means locating the relevant email message with other records that relate to the same business activities, whether this be in an ERMS or on a paper file. As the types of records produced by an organisation can be diverse it will be necessary to work closely with line managers to provide more specific guidance in different work areas about which email messages will constitute records.

As email messages can easily be sent to many people in an organisation. Staff members need to be given an indication about who is responsible for identifying and managing email messages as records. The message that is conveyed will need to be consistent with the records management policy. It is not necessarily possible to give definitive guidance about managing email messages as records because email messages can be sent to many people and can form one or many long strings, which makes it difficult to know when an email message should be captured with the other business records. However, it is advised that rules are created regarding who is responsible for capturing email messages according to whether the messages are internal or...
external together with some consideration for who is responsible for the area of work. There should also be some advice about when to capture a record of an email exchange that has formed a string and how previous iterations of the email string should be treated.

Sample Text:

**Identifying Email Records** A record is 'information created, received, and maintained as evidence and information by an organization or person, in pursuance of legal obligations or in the transaction of business.'\(^5\) When deciding whether an email message constitutes a record, the context and content of the email message needs to be considered. A guiding principle on identifying email records might be that as soon as the email message needs to be forwarded for information purposes it should be considered as a record.

Email messages that might constitute a record are likely to contain information relating to business transactions that have or are going to take place, decisions taken in relation to the business transaction or any discussion that took place in relation to the transaction. For example, during the decision to put out a tender document for a particular service, background discussion about what this should and should not include might take place via email and should be captured as a record.

**Who is Responsible** As email messages can be sent to multiple recipients there are specific guidelines to indicate who is responsible for capturing an email as a record:

- For internal email messages, the sender of an email message, or initiator of an email dialogue that forms a string of email messages
- For messages sent externally, the sender of the email message
- For external messages received by one person, the recipient
- For external messages received by more than one person, the person responsible for the area of work relating to the message.

Managing Email Records with Attachments

The organisation should consider how to treat email messages with attachments as records. There are likely to be cases where either, the email message only, the attachment only or the email and attachment should be treated as a record, depending on the circumstances within which the email and attachment were sent. Whatever advice is given it should be remembered that the email itself provides a certain context to the attachment in terms of who sent it and when it was received. As a general rule it is advised that the email and any attachments should be managed together as a single entity although there might be reasons for capturing an additional separate record for the attachment, for example if further work was required on the attachment. This is a fairly straightforward exercise where an ERMS is used by an organisation as many ERMS provide this functionality, however it will require further consideration if an ERMS is not used.

Where an ERMS is not used the management of email messages together with their attachments might influence the way in which it is decided to manage email messages. There are potential problems, for example in the paper environment the email message and the attachment can easily be separated, which means that part of the context will be lost. If it were decided to manage email messages on a shared drive it is important that the email can be retained as a compound object, this means avoiding text based formats, for example .txt, which would not provide a relationship between the message and the attachment. It should be noted that some email clients might have difficulty storing email messages as a compound object on a shared drive, which means that alternative arrangements would need to be made.

Sample Text:

**Email messages with attachments** Where an email message has an attachment a decision needs to be made as to whether the email message, the attachment or both should be kept as a record. The decision on whether an email and/or its attachment constitute a
record depends on the context within which they were received. It is likely that in most circumstances the attachment should be captured as a record with the email message as the email message will provide the context within which the attachment was used.

There are instances where the email attachment might require further work, in which case it would be acceptable to capture the email message and the attachment together as a record and keep a copy of the attachment in another location to be worked on. In these circumstances the copy attachment that was used for further work will become a completely separate record.

When and Where to Manage Email Records

When an email message has been identified as a record of a business transaction it is important that the message is retained with other records relating to that particular business activity. This will mean moving the email from an individual’s personal inbox and pointing it in the appointed records management system, this might be on an ERMS or on a paper file. The point at which a record is put into the appointed records management system is sometimes referred to as the point at which the record is captured. It is important to ensure that records are captured within the appointed records management system as this is where members of staff will refer to when they want to know when, why and what decisions were made about any given business activity.

As the records management system presents the corporate view of any given business activity the timing of when a record is captured within this system is important. Email messages can pose particular problems in terms of when they should be captured within the records management system, as they often tend to form a string of conversation that not only continues for a lengthy period but also changes its subject over time. It is necessary to provide advice about how email strings should be captured as records as there is a tendency to either wait until the end of the conversation, even though this might never be apparent, or to capture all iterations of the email conversation string. It is advised that a balance should be made between these two extremes and that members of staff should be encouraged to capture an email message when a particular point has been made about a business transaction or activity.
It is important that email messages that will be captured as records must be distinguished from those email messages that do not need to be managed as records. This means that email messages that need to be captured as records should be removed from an individual’s personal inbox and managed with other records that are about that particular business activity. The actual advice given about the treatment of email records will depend on whether or not the organisation manages their records using an ERMS or on paper files.

If the organisation uses an ERMS it should be relatively easy to persuade people to capture their email records into the ERMS where they can be managed together with the other electronic records associated with the business activity. If the organisation is not using an ERMS it is likely that there will be a need for the organisation to consider how and where email records should be managed. It will be necessary to strike a balance between printing out all email messages to paper and the individual’s desire to refer to email messages quickly in electronic form.

If the organisation wants to keep an electronic version of email records, but does not have an ERMS, this could be done through using shared public email folders or saving email messages in .msg format on shared drives (this second option will not be available with some email clients). It will be necessary to explore the feasibility of these options before opting for one of them in terms of the protection available to the email records, for example how easily could the records be changed and can access to groups of email records be restricted. Whichever option is chosen, whether it is strictly print to paper, shared public email folders or shared drives, it is important that there is consistency throughout the organisation in how and where the email records are managed. It should be noted that even if the organisation does not have an ERMS it is not advisable for email records to be stored in individuals’ personal mailboxes.

Sample Text

| When to capture | Email messages that can be considered to be records should be captured as soon as possible. Most email messages will form part of an email conversation string. Where an email string has formed as part of a discussion it is not necessary to capture each new part of the conversation, ie every reply, separately. There is no need to wait until the end of the conversation before capturing the email string as several subjects might have been covered. Email strings should be captured as records at significant points during the conversation, rather than waiting to the end of the conversation because it might |

Last updated March 2004
not be apparent when the conversation has finished.

Where to capture  Email messages that constitute records must be [printed to paper, saved on shared drives in .msg format, put into public folders or captured within the ERMS]. Email messages captured as records should be located with other records relating to the same business activity. Personal mailboxes should not be used for long-term storage of email messages. Personal mailboxes should be used for personal information or short-term reference purposes, when these emails are no longer required they should be deleted.

Encryption and Managing Email Records

The management of encrypted emails over time is likely to be problematic. There is a danger that encrypted emails might become inaccessible over time as the method of encryption becomes obsolete. If an organisation does send or receive encrypted emails there is a need to consider how encrypted email records will continue to be accessed over time, for example de-encrypting email messages before they are captured as email records either in an ERMS, on shared drives or public email folders.

Sample Text

Encrypted email records  Where is it known that an email has been encrypted it is important that it is unencrypted prior to capturing it as a record. If an email record is captured without being unencrypted it is highly likely that there will be problems with accessing the record over a period of time.

Titling Email Records in an Electronic Records Management System

When records are managed in an ERMS the title of records is the main way in which records will be retrieved and identified. In many ERMS the title of the email record captured will default to
the title of the email, however email messages will not usually have a title that accurately reflects
the reason for capturing the email as a record. As the title of the email is unlikely to reflect the
reason it would be captured as a record members of staff should be given advice on how to title
email records when they are captured within the ERMS. It is important that the title of the email
itself is not changed, which means that email messages stored within an email client should not
be re-titled. Titling an email record that is being captured into an ERMS will not change the title
of the email itself, as this is the equivalent of attaching label to the email.

Sample Text:

**Titling email records** The title of an email message does not always
reflect the reason for capturing an email message as a record. The
problem of email titles not reflecting the reason for capturing the
message as a record can, to some extent, be avoid through people
following the guidelines for titling emails at the point they are created.
If the title of an email does not accurately reflect the reason why it is
being captured as a record then it should not be re-titled within the
email client but at the point it is captured within the ERMS, i.e. the
record entry form. Re-titling email records is particularly important
when they represent different points in an email string as it will help to
identify the relevant aspects of the conversation.

Appendix 1 - Guidelines for Writing Business Email messages

To encourage the use of this section as a quick reference tool it is advised that it is split into
sections reflecting the main areas to be considered when drafting email messages. The sample
text is indicative of the most frequent types of advice that is given in guidance on the appropriate
use of email. The wording in this section should be written in a way that provokes thought about
which email features could be used and how to draft an email message.

The sample text is not a definitive list of everything that should be considered when composing
an email, nor is it intended to be. The sample text is intended to reflect the major points that
should be considered when drafting email messages however there might be additional areas
that organisations would like to add depending on the nature of the business conducted or to reflect particular email problems that are encountered within an organisation.

Sample Text:

Subject Line

- Ensure the subject line gives a clear indication of the content of the message
- Indicate if the subject matter is sensitive
- Use flags to indicate whether the message is of high or low importance and the speed with which an action is required
- Indicate whether an action is required or whether the email is for information only

Subject and Tone

- Greet people by name at the beginning of an email message
- Identify yourself at the beginning of the message when contacting someone for the first time
- Ensure that the purpose and content of the email message is clearly explained
- Include a signature with your own contact details
- Ensure your signature is not unnecessarily long
- Ensure that the email is polite and courteous
- Tone of an email message should match the intended outcome
- Make a clear distinction between fact and opinion
- Proof read messages before they are sent to check for errors
- Try to limit email messages to one subject per message
- Include the original email message when sending a reply to provide a context
- Where the subject of a string of email messages has significantly changed start new email message, copying relevant sections from the previous string of email messages
- Ensure email messages are not unnecessarily long
- Ensure that attachments are not longer versions of emails
- Summarise the content of attachments in the main body of the email message

Structure and Grammar

- Try to use plain English
- Check the spelling within the email message before sending
- Use paragraphs to structure information
- Put important information at the beginning of the email message
- Avoid using abbreviations
- Avoid using CAPITALS
- Try not to over-use of bold text
- Do not use emoticons

**Addressing**

- Distribute email message only to the people who need to know the information
- Using ‘reply all’ will send the reply to everyone included in the original email. Think carefully before using ‘reply all’ as it is unlikely that everyone included will need to know your reply.
- Use the ‘To’ field for people who are required to take further action and the ‘cc’ field for people who are included for information only.
- Think carefully about who should be included in the ‘cc’ field
- Ensure the email message is correctly addressed

**General**

- Be aware that different computer systems will affect the layout of an email message
- Avoid sending email messages in HTML format as if an email recipient is using an email system that does not allow HTML the layout will be affected
- Be aware that some computer systems might have difficulties with attachments
- Observe the restrictions on attachment size [give the attachment size restriction]
- Restrict the number of addressees to [#; the number will vary depending on the network]
- Try not to forward message unnecessarily. Put the email into the [ERMS, shared drive or public folder] and provide a shortcut link
- Internal emails should use pointers to attachments and not be included in the body of the text [this point can only really apply if an ERMS is being used]

**Appendix 2 - Naming Conventions**

When email messages are stored electronically as records the title provides the easiest way of retrieving the required message. Advice should be given to staff about how they should title email messages when they capture email messages as records because the title used in the subject
line of an email message does not always indicate the reason why it is being captured as a record.

Naming conventions should be used for either email messages captured as records into an ERMS or saved onto a shared drive in .MSG format. An amended form of the naming conventions could also be used to provide advice on how staff should write the subject line of an email before it is sent. If email messages are being kept as records inside shared public mailboxes it is advised that staff are discouraged from renaming the message within the mailbox this will change the subject line of the email and affect the integrity of the record.

Sample Text:

The purpose of a record title is to identify one record from other records that may be in the same or a different folder. The principles detailed below apply to email records but may be applicable to other electronic records.

- Change the title of the e-mail when saving it in [the shared drive or ERMS] if it does not accurately reflect the content of the message. For example, titles such as “A few points” will soon become meaningless when it forgotten what the points relate to
- Ensure the title contains sufficient information to enable any member of the department to identify the relevance of the content to themselves
- All instances of ‘FW’ and ‘RE’ should be removed from the title as they do not provide any information about the content of the message
- Do not include the date of an email, and the fact that it is an email. The date will be automatically captured and the fact it is an email will be obvious
- Do not include nonsense terms, for example ‘letter1’
- Do not use ‘MSDOS’ style 8-letter titles, for example ‘maylet03’
- Use natural language and spell words in full
- Use abbreviations and acronyms with caution, as they may become obsolete over a period of time and can have more than one meaning
- Write the names of organisations in full and include the appropriate abbreviation. If there is not enough space ensure the information is captured elsewhere, for example in the notes field.

- Wherever possible, always use the role title rather than the name of the person. For example, “Comments on .... by Head of Department”

- Always identify people by their full name rather than by their initials. Initials can easily be forgotten or confused with people with similar initials.

References

Data Protection Act (1998)


Human Rights Act (1998)


Regulation of Investigatory P