Parliamentary
and Health Service
Ombudsman

PARLIAMENTARY AND HEALTH SERVICE OMBUDSMAN

Email Management and Data Storage Policy

Version 1.4

Current version

Document Control

Title:	Email management and data storage policy
Reference:	
Original Author(s):	Suzanne Wright
Owner:	Suzanne Wright
Distribution:	All staff - published on Intranet
Reviewed by:	Bill Richardson, Tom Stoddart
Quality Assured by:	Bill Richardson, Records Management Project Board
File:	
Signature:	
Authority:	Approved by Executive Board

Change History

Version	Date	Status	Last update	Comment
1.0	16/12/08	Approved	16/12/08	Approved by EB at meeting of 12/08/2008
1.1	22/11/11	Draft	22/11/11	Reviewed by Suzanne Wright and updated
1.2	28/11/11	Draft	28/11/11	Reviewed by Tom Stoddart
1.3	22/12/11	Draft	22/12/11	Updated following review by Bill Richardson
1.4	09/02/12	Draft	09/02/12	Updated following Equality Impact Assessment and submitted to EB for approval

Contents

1. Purpose 4

2. Policy statement 4

3. Scope 4

4. Principles. 5

5. Objectives 5

6. Outcomes 6

7. Monitoring and compliance 6

8. Review 6

Annex 1 - Background context 7
Annex 2 - Which emails are records? 9
Annex 3 - Email management and storage 10
Annex 4 - Access to mail accounts during absences. 12

1. Purpose

1.1 The purpose of this policy is to provide a framework for the effective management of PHSO's emails in accordance with all statutory and business requirements. Compliance with this policy supports PHSO's commitment to be exemplary in its administration.

2. Policy statement

2.1 The Ombudsman recognises that effective records management is fundamental to good administration and operational effectiveness and is an enabler to the achievement of our strategic aims and objectives. The Ombudsman is therefore committed to implementing and maintaining good record keeping practices.

2.2 While PHSO is not covered by the Public Records Act 1958, nor required to adopt the Code of Practice on the Management of Records, the Ombudsman has decided to adopt an approach to records management which is consistent with the legal obligations and best practice principles embodied in them.

2.3 PHSO is subject to and will comply with the Freedom of Information Act 2000 and the Data Protection Act 1998, taking into account the statutory bar on the disclosure of information obtained in the course of investigations other than in specific circumstances.

3. Scope

3.1 This policy applies to emails that are received, created, or held in the course of PHSO's business. It should be read in conjunction with the ICT Acceptable Use policy which details email security, content and legal liability, and acceptable use.

3.2 This policy applies to all permanent, contract and temporary staff and any organisation or body acting as agents of PHSO where contractual arrangements are in place, who have access to PHSO's computer system and who use email. Everyone 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.

4. Principles

Principle 1
All business and case management data held on PHSO's IT systems (including emails and documents) belong to PHSO and not any individual or group. This data should therefore be stored in the appropriate corporate system and be available for management and operational use subject to normal access controls.

Principle 2
'My Workspace' in Meridio is available for limited personal storage. Personal emails or those containing sensitive information should be filed in My Workspace. This area must not contain emails related to PHSO's business. Staff are required to perform regular electronic housekeeping on their 'My Workspace' to ensure that data that is no longer required is deleted.

Principle 3
When an email is sent or received a decision must be made about whether it needs to be captured as a record (see Annex 2 for further information). Once an email message has been captured as a record it should be deleted from all mailboxes.

Principle 4
Emails not retained in a corporate system within a reasonable period of time (currently defined as 90 days) will be automatically deleted from the email system (Outlook).

5. Objectives

The key objectives of this policy are to:

5.1 Ensure appropriate management arrangements are in place to ensure email messages that form records of business activities are stored appropriately

5.2 Ensure all employees have a clear understanding of their personal and collective responsibilities in managing their email

5.3 Ensure email messages that form records of business activities are stored appropriately

5.4 Ensure email messages are managed in order to comply with Data Protection and Freedom of Information legislation

5.5 Help staff manage their electronic information better

5.6 Mitigate against the risks of excessive and inappropriate data storage which includes:

- important corporate information not being shared (data is held in private drives)
- inappropriate non-corporate files being stored on PHSO IT systems
- out-of-date and duplicate information using up storage capacity.

6. Outcomes

6.1 This policy will deliver the following outcomes:

- Work is conducted more efficiently as it will enable staff to locate all the information relating to specific areas of the business
- IT system performance is improved and we reduce the risks and costs of excessive email data storage
- PHSO's reputation is protected because we have systems in place to manage email so that we can comply with Freedom of Information and Data Protection legislation.

7. Monitoring and compliance

7.1 The Head of Information and Records Management is responsible for monitoring this policy to ensure it is up-to-date, relevant and continues to support strategic aims and objectives.

7.2 Compliance with this email management policy will be regularly assessed and included within the internal audit programme.

7.3 Reviews will seek to:

- identify examples of good practice which can be used throughout PHSO
- highlight where non-compliance is occurring; and if appropriate, recommend remedial action to ensure exemplary records management standards are achieved and maintained.

8. Review

8.1 The policy will be reviewed every three years, unless there is a significant change in relevant legislation which requires a review before then.

Annex 1 - Background context

1.1 As an exemplary organisation all our records should be managed in line with the Lord Chancellor's Code of Practice on the management of records under Section 46 of the Freedom of Information Act 2000. This states that the principal issues for the management of electronic records are the same as those for the management of any record, including the creation of authentic records, the tracking of records, review and retention of records and disposal arrangements.

1.2 This email policy has been developed in line with The National Archives guidance on managing emails. The National Archives are widely regarded across both the public sector and private sector as leading on records management issues.

1.3 Email is increasingly becoming the primary business tool for both internal and external written communication and as a result should be treated with the same level of attention given to drafting and managing any other documents. 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.

1.4 Email messages are available until deleted by both the sender and recipient. All non-deleted email messages are subject to Data Protection and Freedom of Information Legislation and can also form part of the corporate record. They could therefore be subject to discovery action and used against PHSO.

1.5 Staff should also be aware that corporate email messages could be used as evidence in legal or employment proceedings. Members of staff are responsible for what they have written in an email message.

1.6 The consequence of all this is that after corporate/ business-related emails have been created, these are potential records and are required to be stored in the corporate file plan (i.e. not Outlook). Emails which are not records should be deleted within an appropriate time. This policy puts in place PHSO's arrangements for managing emails appropriately.

1.7 Specifically the policy ensures that PHSO has in place adequate mechanisms to:

- ensure email messages facilitate effective communication and ensure that appropriate records of those communications are maintained in accordance with the PHSO Email Management and Records Management policies;
- ensure compliance with information legislation that applies to email including Data Protection Act and, Freedom of Information Act
- ensure appropriate business records are maintained for audit and accountability purposes;
  mitigate against the risks of inappropriate and excessive data storage.

1.8 A record is defined in PHSO's Records Management policy as 'recorded information created, received and maintained by PHSO in pursuance of its legal obligations or in the transaction of business.' When deciding whether an email message constitutes a record, the context and content of the email message need to be considered. A guiding principle on identifying email records might be that as soon as the email needs to be forwarded for information purposes it should be considered a record.

1.9 The email management policy compliments the ICT Acceptable Use policy, specifically: 3.2 Email Content and Legal Liability; 4. Personal Use of the ICT system; and 5. Unacceptable use of the ICT system.

1.10 The policy applies to everyone employed by PHSO who has access to its computer system and who uses email. 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.

1.11 All employees have a clear understanding of their personal and collective responsibilities in managing their email.

Annex 2 - Which emails are records?

2.1 To help identify email records, a record is defined in PHSO's Records Management Policy as 'recorded information created, received and maintained by PHSO in pursuance of its legal obligations or in the transaction of business'. Messages that might constitute a record are likely to contain information about:

- substantive contributions to the development of legislation, policy or procedures including factual evidence and interpretative material relating to changes as well as accepted and rejected options;
- evidence of how far Office objectives have been met;
- material that relates to the main functions of the Office and its development, including major projects, special measures and initiatives;
- background material to decisions, rulings, opinions and advice issued to the public, MPs, bodies within jurisdiction, staff, etc;
- text of statements, speeches, Select Committee submissions, answers to Parliamentary Questions, etc along with briefing papers and background material;
- public or other notable events which gave rise to significant contemporary interest or controversy;
- contracts and contract changes as well as procedures used to select external suppliers;
- authorisation for payment of suppliers, contractors, staff, etc;
- measures taken to comply with legal and other obligations and regulations such as Health and Safety legislation, Data Protection Act, etc; and
- an individual's terms of employment or conditions with PHSO, collected through HR or management processes and which form a part of the worker's employment relationship with PHSO.

2.2 This list is indicative but not exhaustive and staff are advised to seek further guidance from their Local Information and Records Adviser or the Information and Records Manager if in doubt.

Annex 3 - Email management and storage

3.1 Email messages can constitute part of the formal record of a transaction. All members of staff are responsible for identifying and managing email messages that constitute a record of their work.

3.2 When an email is sent or received a decision needs to be made about whether the email needs to be captured as a record in the appropriate area of the corporate file plan. Once an email message has been captured as a record it should be deleted from your mailbox.

3.3 Emails will be treated in the same way as other corporate records in terms of retention and disposal. The information asset register sets out the retention periods for each section of the corporate file plan and these will ensure that records that are no longer required for ongoing business or historical reasons are deleted as soon as reasonably possible.

3.4 All important documents and emails that demonstrate action or contribute to policy or decision making must be stored in Visualfiles (where it is related to a specific case) or in the appropriate place in the corporate file plan for longer term retention and review.

3.5 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 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 not be apparent when the conversation has finished.

3.6 Email messages relating to casework must be filed in Visualfiles.

3.7 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 messages;
- For messages sent externally, the sender of the message;
- For external messages received by one person, the recipient; and
- For external messages received by more than one person, the person responsible for the work relating to the message. If this is not clear it may be necessary to clarify who this is with the other people who have received the message.

3.8 Where an email 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. In most instances 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. Where further work is required on an attachment, the initial email message and attachment will be one record, and the copy attachment used for further work will become a completely separate record.

3.9 The subject line of an email message does not always reflect the reason for capturing an email as a record and therefore might not be the most appropriate name for the email when it is transferred to Meridio or Visualfiles. This can be avoided by following the naming convention guidelines (available on Ombudsnet) for naming emails at the point they are created. Re-naming emails is particularly important when they represent different parts of an email string as it helps to identify the relevant aspects of the conversation.

3.10 During the 90 days after the creation of the email, a decision needs to be made as to whether the email is a record. If it is it should be transferred to an appropriate place either in Visualfiles (for casework) or in the appropriate place in the corporate file plan. Any emails still in Outlook after 90 days will automatically be deleted.

3.12 A further option is storage on an individual's 'My Workspace'. However, this is only to be used for personal or sensitive, non-business emails. Any records held there must be transferred to the corporate file plan or Visualfiles as soon as possible.

Annex 4 - Access to mail accounts during absences

4.1 In the case of planned absences (eg holidays) staff should use the 'Out of Office Assistant'. The auto-reply message should ideally give an alternative contact and state when a full reply can be expected. Emails should be forwarded to another member of staff during a prolonged absence. Alternatively, where this can be done securely, access to a mailbox should be delegated to another member of a team to ensure urgent messages are dealt with.

4.2 Shared mailboxes can be created where there are a group of people responsible for the same area of work (eg an investigation team, a working group, project team or a section in Corporate Resources). This will help to ensure that queries are answered if members of the team are away from the office. One person should be identified as the 'owner' of a shared mailbox or public folder. The owner is responsible for the overall management of that mailbox or folder.

4.3 In the case of unplanned absences and/or where the member of staff has not made arrangements for access (eg sickness) the manager should arrange redirection of email; authorisation should be requested from the Head of HR Operations and Head of ICT. Access should be in the presence of the line manager. On return, the staff member should be told when and why their mailbox was accessed.

4.4 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. Authorisation should be requested from the Head of HR Operations and Head of ICT. Access should be in the presence of the line manager. On return, the staff member should be told when and why their mailbox was accessed. 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; and
- Evidence in support of disciplinary action.

4.5 Staff should ensure that any personal or sensitive emails are filed in My Workspace. This area would not be subject to the review outlined in 4.3 above.

Parliamentary
and Health Service
Ombudsman

PARLIAMENTARY AND HEALTH SERVICE OMBUDSMAN

Knowledge and Information Management Programme

Email Management and Data Storage Policy

Version 1.0

Document Control

Title:	Email management and data storage policy
Reference:	
Original Author(s):	Noelle Brelsford
Owner:	Noelle Brelsford
Distribution:	All staff - published on Intranet
Reviewed by:	Noelle Brelsford
Quality Assured by:	The National Archives (v0.5), Leadership Group, Philip Aylett
File:	G:\PIC\KIM\Email Management
Signature:	
Authority:	Approved by Executive Board

Change History

Version	Date	Status	Last update	Comment
1.0	16/12/08	Approved	16/12/08	Approved by EB at meeting of 12/08/2008

Contents

1 Purpose and Scope 4
2 Objectives 5
3 Principles 5
4 Outcomes 6
5 Monitoring and review 6
Annex 1 Background context 7
Annex 2 - Which emails are records? 9
Annex 3 - Email management and storage 10
Annex 4 - Daily email management (framework) 12
Annex 5 - Access to mail accounts during absences 13
Annex 6 - Naming conventions 14

1 Purpose and Scope

1.1 The purpose of the email management and data storage policy (the policy) is to ensure that the Office of the Parliamentary and Health Service Ombudsman (PHSO) has in place adequate mechanisms to:

- ensure email messages that form records of business activities are managed appropriately;
- ensure compliance with Data Protection and Freedom of Information and Regulation of Investigative Privacy legislation; and
- mitigate against the risks of inappropriate and excessive data storage.

1.2 This policy deals with email management, disposal and storage issues, it should be read in conjunction with the ICT acceptable usage policy which details email security, content and legal liability, and acceptable use.

1.3 This policy applies to everyone employed by PHSO who has access to its computer system and who uses email. 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.

1.4 Guidelines for writing business email messages and managing emails will be provided, and introduced as part of the PHSO induction process.

2 Objectives

2.1 Appropriate management arrangements are in place to ensure email messages that form records of business activities are stored appropriately.

2.2 All employees have a clear understanding of their personal and collective responsibilities in managing their email.

2.3 Ensure email messages that form records of business activities are stored appropriately.

2.4 To ensure email messages are managed in order to comply with Data Protection and Freedom of Information legislation.

2.5 To help staff manage their electronic information better.

2.6 To mitigate against the risks of excessive and inappropriate data storage which includes:

- important corporate information not being shared (data is held in private drives);
- inappropriate non-working files being stored on PHSO IT systems;
- out of date and duplicate information unnecessarily using up storage capacity.

2.7 To ensure that the least information is kept for the least time i.e. to minimise the amount of time information is kept for.

3 Principles

3.1 All business and case management data held on PHSO's IT systems (including emails and documents) belong to PHSO and not any individual or group. It should therefore be stored in an appropriately accessible place and not held in personal drives or folders.

3.2 P:drive will be available as limited personal storage areas in line with the ICT acceptable usage policy.

3.3 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 all mailboxes.

3.4 Email quotas will be used to contain data storage and to mitigate against the risks of excessive data storage.

3.5 Email will be automatically deleted when 90 days old.

3.6 Staff will be required to perform regular electronic housekeeping on P and shared drives to ensure that data that is no longer required for ongoing business, historical or legal reasons is moved to a corporate information source or deleted.

4 Outcomes

4.1 Managing email messages appropriately will mean that work can be conducted more efficiently as it will enable staff to locate all the information relating to specific areas of the business.

4.2 IT system performance will be improved and we reduce the risks and costs of excessive email data storage.

4.3 PHSO's reputation is protected because we have systems in place to manage email so that we can comply with Freedom of Information and Data Protection legislation.

5 Monitoring and review

5.1 Compliance with the policy will be monitored to help us:

- identify examples of good practice which can be used throughout PHSO;
- highlight where non-conformance to the policy is occurring; and if appropriate, recommend a tightening of controls and make recommendations as to how compliance can be achieved more effectively.

5.2 The policy will be reviewed on an annual basis, unless there is a significant change in relevant legislation which requires a review before then.

Annex 1 - Background context

1.1 Following a Records Management Review in PHSO, in 2007, the Executive Board made a decision to implement the recommendations of the review within the Knowledge and Information Management Programme. As an exemplary organisation all our records should be managed in line with the Lord Chancellor's Code of Practice on the management of records under Section 46 of the Freedom of Information Act 2000. This states that the principal issues for the management of electronic records are the same as those for the management of any record, including the creation of authentic records, the tracking of records, review and retention of records and disposal arrangements.

1.2 This email policy has been developed in line with The National Archives guidance on managing email. The National Archives are widely regarded across both the public sector and private sector as leading on records management issues.

1.3 Email is increasingly becoming the primary business tool for both internal and external written communication and as a result should be treated with the same level of attention given to drafting and managing non-electronic 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.

1.4 There is a common misconception that email messages constitute an ephemeral form of communication. In fact they are available until deleted by both the sender and recipient. All non-deleted email messages are subject to Data Protection and Freedom of Information Legislation and can also form part of the corporate record. They could therefore be subject to discovery action and used against PHSO.

1.5 Staff should also be aware that email messages could be used as evidence in legal or employment proceedings. Members of staff are responsible for what they have written in an email message.

1.6 The consequences of all this is that after emails have been created; these are potential records and are required to be stored in the corporate file store (i.e. not Outlook). Emails which are not records should be deleted within an appropriate time. This policy puts in place PHSO's arrangements for managing emails appropriately.

1.7 Specifically the policy to ensure that PHSO has in place adequate mechanisms to:

- ensure email messages facilitate effective communication and ensure that appropriate records of those communications are maintained in accordance with the PHSO records management policy;
- ensure compliance with information legislation that applies to email including Data Protection Act, Freedom of Information Act and Regulation of Investigatory Privacy Act;
- ensure appropriate business records are maintained for audit and accountability purposes;
- mitigate against the risks of inappropriate and excessive data storage.

1.8 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 pursuance of business'. 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 needs to be forwarded for information purposes it should be considered as a record.

1.9 The email management policy compliments the ICT acceptable usage policy, specifically 3.2 Email Content and Legal Liability, 4. Personal Use of the ICT system, 5. Unacceptable use of the ICT system.

1.10 The policy applies to everyone employed by PHSO who has access to its computer system and who uses email. 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.

1.11 All employees have a clear understanding of their personal and collective responsibilities in managing their email.

Annex 2 - Which emails are records?

2.1 To help identify email records – a record is 'information created, received, and maintained as evidence and information by an organisation or person, in pursuance of legal obligations or in the transaction of business'. Messages that might constitute a record are likely to contain information about:

- substantive contributions to the development of legislation, policy or procedures including factual evidence and interpretative material relating to changes as well as accepted and rejected options;
- evidence of how far Office objectives have been met;
- material that relates to the main functions of the Office and its development, including major projects, special measures and initiatives;
- background material to decisions, rulings, opinions and advice issued to the public, MPs, bodies within jurisdiction, staff, etc;
- text of statements, speeches, Select Committee submissions, answers to Parliamentary Questions, etc along with briefing papers and background material;
- public or other notable events which gave rise to significant contemporary interest or controversy;
- contracts and contract changes as well as procedures used to select external suppliers;
- authorisation for payment of suppliers, contractors, staff, etc;
- measures taken to comply with legal and other obligations and regulations such as Health and Safety legislation, Data Protection Act, etc; and
- individuals terms of employment or conditions with PHSO, collected through HR or management processes and which form a part of the workers employment relationship with PHSO.

2.2 This list is indicative but not exhaustive and staff are advised to seek further guidance from their Records Advisers if in doubt.

Annex 3 - Email management and storage

3.1 Email messages can constitute part of the formal record of a transaction (Annex 2) for more guidance on what to put on record. All members of staff are responsible for identifying and managing email messages that constitute a record of their work.

3.2 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 your mailbox.

3.3 Email that is no longer required for ongoing business or historical reasons must be deleted as soon as reasonably possible. This is because over-retention can lead to:

- risk of contravening Freedom of Information and Data Protection legislation;
- difficulties in finding the information you are looking for if information remains unstructured; and
- ongoing server capacity issues.

3.4 All important documents and emails that demonstrate action or contribute to policy or decision making must be stored in Visualfiles (where it is related to a specific case) or on the G:drive for longer term retention and review.

3.5 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 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 not be apparent when the conversation has finished.

3.6 Email messages relating to complaint investigation casework must be filed in Visualfiles.

3.7 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 messages;
- For messages sent externally, the sender of the message;
- For external messages received by one person, the recipient; and
- For external messages received by more than one person, the person responsible for the work relating to the message. If this is not clear it may be necessary to clarify who this is with the other people who have received the message.

3.8 Where an email 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. In most instances 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. Where further work is required on an attachment, the initial email message and attachment will be one record, and the copy attachment used for further work will become a completely separate record.

3.9 The title of an email message does not always reflect the reason for capturing an email as a record. This can be avoided by following the guidelines for titling emails at the point they are created. If the email title 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 in the record system (Annex 6). Re-titling emails are particularly important when they represent different parts of an email string as it helps to identify the relevant aspects of the conversation.

3.10 During 90 days after creation, a decision needs to be made as to whether email is a record. If it is it should be transferred to an appropriate place either in visual files (for casework) or the G:drive. Any emails still in Outlook for 90 days will automatically be deleted on a daily basis.

3.12 A further option is storage on an individuals P:drive. However, this is only to be used for personal, non-business emails as when working off-line prior to connecting on-line. The size of P:drives will normally be limited to 50mb to restrict the amount of storage in this folder. Any records held there must be transferred to the G:drive as soon as possible.

Annex 4 - Daily email management (framework)

4.1 As defined in the Lord Chancellor's Code of Practice and BS ISO 15489 - 1:2001 a record is Information created, received and maintained as evidence and information by an organisation or person, in pursuance of legal obligations or in the transaction of business.

4.2 Emails that are a record or part of a record should be moved using the 'drag and drop' process into Visual Files if they relate to casework, or the appropriate folder in the g:drive.

4.3 To 'drag and drop' open Outlook Inbox and minimise window by double clicking on the name bar, and do the same with the g;drive, then move the chosen email(s) by dragging using the mouse, from the Inbox into the chosen folder within the g;drive.

4.4 Before moving the email it is important to ensure that the title of the email reflects the reason for capturing it as a record and should be re-titled if necessary (Annex 3):

- Ensure that FW and RE are taken out of any email titles;
- Where the email also has an attachment, in most cases both should be captured as the record as the email could provide the context within which the attachment is used (Annex 3);
- G:drives will be reconfigured with additional folders to reflect the Corporate Taxonomy;
- To ensure appropriate confidentiality, accessibility to g:drive folders will be locked down by functional area and subject matter to specified users;
- Emails that are not a corporate record need to be deleted and this will be enforced through daily deletions of emails over 90 days old;
- Once an email is destroyed the information will not be recoverable;
- It is the responsibility of the 'Sender' to ensure email records are captured whether they are sent internally or externally (Annex 3) and the responsibility of the 'Recipient' of External messages to ensure email records are captured (Annex 3).

Annex 5 - Access to mail accounts during absences

5.1 In the case of planned absences (eg holidays) staff should use the 'Out of Office Assistant'. The auto-reply message should ideally give an alternative contact and state when a full reply can be expected. Emails should be forwarded to another member of staff during a prolonged absence. Alternatively, where this can be done securely, access to a mailbox should be delegated to another member of a team to ensure urgent messages are dealt with.

5.2 Shared mailboxes can be created where there are a group of people responsible for the same area of work (eg an investigation team, a working group, project team or a section in Corporate Resources). This will help to ensure that queries are answered if members of the team are away from the office. One person should be identified as the 'owner' of a shared mailbox or public folder. The owner is responsible for the overall management of that mailbox or folder.

5.3 In the case of unplanned absences and/or where the member of staff has not made arrangements for access (eg sickness) the manager should arrange redirection of email; authorisation should be requested from the Head of HR Operations and ICT Manager. Access should be in the presence of the line manager. On return, the staff member should be told when and why their mailbox was accessed.

5.4 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. 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; and
- Evidence in support of disciplinary action.

Annex 6 - Naming conventions

6.1 Following an agreed naming convention creates a consistent way of working that makes information retrieval more effective.

6.2 When creating content in any form the following principles must be observed:

- Keep file names short, but meaningful;
- Avoid unnecessary repetition and redundancy in file names and file paths;
- Use capital letters to delimit words, not spaces or underscores;
- When including a number in a file name always give it as a two-digit number, i.e. 01-99, unless it is a year or another number with more than two digits;
- If using a date in the file name always state the date 'back to front', and use four digit years, two digit months and two digit days: YYYYMMDD or YYYYMM or YYYY or YYYY-YYYY;
- When including a personal name in a file name give the family name first followed by the initials;
- Avoid using common words such as 'draft' or 'letter' at the start of file names, unless doing so will make it easier to retrieve the record;
- Order the elements in a file name in the most appropriate way to retrieve the record;
- The file names of records relating to recurring events must include the date and a description of the event, except where the inclusion of any of either of these elements would be incompatible with rule 2;
- The file names of correspondence must include the name of the correspondent, an indication of the subject, except where the inclusion of any of these elements would be incompatible with rule 2;
- The file name of an email attachment must include the name of the correspondent, an indication of the subject, except where the inclusion of any of these elements would be incompatible with rule 2.
- The version number of a record must be indicated in its file name by the inclusion of 'V' followed by the version number and, where applicable, 'Draft'.
- Avoid using non-alphanumeric characters in file names.

6.3 Emails or documents received that do not conform to naming conventions must be re titled: For example:

Before - document from P Smith is received entitled 'complaint'
After - Smith P Complaint on Services

6.4 Remember that subject relevance can diminish over the time or loose context if the document is moved out of its original folder so using words like ‘update’, ‘progress report’, ‘draft’ or ‘letter’ on their own without qualification must be avoided.

6.5 Similarly, the use of current acronyms and abbreviations must be avoided as knowledge of their meaning may be lost over time and/or become ambiguous.

Parliamentary
and Health Service
Ombudsman

PARLIAMENTARY AND HEALTH SERVICE OMBUDSMAN

Knowledge and Information Management Programme

Email Management and Data Storage Annexes

Version 1.0

Document Control

Title:	Email management and data storage annexes
Reference:	
Original Author(s):	Noelle Brelsford
Owner:	Noelle Brelsford
Distribution:	All staff - published on Intranet
Reviewed by:	Noelle Brelsford
Quality Assured by:	The National Archives (v0.5), Leadership Group, Philip Aylett
File:	G:\PIC\KIM\Email Management
Signature:	
Authority:	Approved by Executive Board

Change History

Version	Date	Status	Last update	Comment
1.0	30/12/08	Approved	30/12/08	Approved by EB at meeting of 12/08/2008

Contents

Annex 1 - Background context 4
Annex 2 - Which emails are records? 6
Annex 3 - Email management and storage 7
Annex 4 - Daily email management (framework) 9
Annex 5 - Access to mail accounts during absences 10
Annex 6 - Naming conventions 11

Annex 1 - Background context

1.1 Following a Records Management Review in PHSO, in 2007, the Executive Board made a decision to implement the recommendations of the review within the Knowledge and Information Management Programme. As an exemplary organisation all our records should be managed in line with the Lord Chancellor's Code of Practice on the management of records under Section 46 of the Freedom of Information Act 2000. This states that the principal issues for the management of electronic records are the same as those for the management of any record, including the creation of authentic records, the tracking of records, review and retention of records and disposal arrangements.

1.2 This email policy has been developed in line with The National Archives guidance on managing email. The National Archives are widely regarded across both the public sector and private sector as leading on records management issues.

1.3 Email is increasingly becoming the primary business tool for both internal and external written communication and as a result should be treated with the same level of attention given to drafting and managing non-electronic 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.

1.4 There is a common misconception that email messages constitute an ephemeral form of communication. In fact they are available until deleted by both the sender and recipient. All non-deleted email messages are subject to Data Protection and Freedom of Information Legislation and can also form part of the corporate record. They could therefore be subject to discovery action and used against PHSO.

1.5 Staff should also be aware that email messages could be used as evidence in legal or employment proceedings. Members of staff are responsible for what they have written in an email message.

1.6 The consequences of all this is that after emails have been created; these are potential records and are required to be stored in the corporate file store (i.e. not Outlook). Emails which are not records should be deleted within an appropriate time. This policy puts in place PHSO's arrangements for managing emails appropriately.

1.7 Specifically the policy to ensure that PHSO has in place adequate mechanisms to:

- ensure email messages facilitate effective communication and ensure that appropriate records of those communications are maintained in accordance with the PHSO records management policy;

- ensure compliance with information legislation that applies to email including Data Protection Act, Freedom of Information Act and Regulation of Investigatory Privacy Act;

- ensure appropriate business records are maintained for audit and accountability purposes;

- mitigate against the risks of inappropriate and excessive data storage.

1.8 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 pursuance of business'. 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 needs to be forwarded for information purposes it should be considered as a record.

1.9 The email management policy compliments the ICT acceptable usage policy, specifically 3.2 Email Content and Legal Liability, 4. Personal Use of the ICT system, 5. Unacceptable use of the ICT system.

1.10 The policy applies to everyone employed by PHSO who has access to its computer system and who uses email. 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.

1.11 All employees have a clear understanding of their personal and collective responsibilities in managing their email.

Annex 2 - Which emails are records?

2.1 To help identify email records – a record is ‘information created, received, and maintained as evidence and information by an organisation or person, in pursuance of legal obligations or in the transaction of business’. Messages that might constitute a record are likely to contain information about:

- substantive contributions to the development of legislation, policy or procedures including factual evidence and interpretative material relating to changes as well as accepted and rejected options;

- evidence of how far Office objectives have been met;

- material that relates to the main functions of the Office and its development, including major projects, special measures and initiatives;

- background material to decisions, rulings, opinions and advice issued to the public, MPs, bodies within jurisdiction, staff, etc;

- text of statements, speeches, Select Committee submissions, answers to Parliamentary Questions, etc along with briefing papers and background material;

- public or other notable events which gave rise to significant contemporary interest or controversy;

- contracts and contract changes as well as procedures used to select external suppliers;

- authorisation for payment of suppliers, contractors, staff, etc;

- measures taken to comply with legal and other obligations and regulations such as Health and Safety legislation, Data Protection Act, etc; and

- individuals terms of employment or conditions with PHSO, collected through HR or management processes and which form a part of the workers employment relationship with PHSO.

2.2 This list is indicative but not exhaustive and staff are advised to seek further guidance from their Records Advisers if in doubt.

Annex 3 - Email management and storage

3.1 Email messages can constitute part of the formal record of a transaction (Annex 2) for more guidance on what to put on record. All members of staff are responsible for identifying and managing email messages that constitute a record of their work.

3.2 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 your mailbox.

3.3 Email that is no longer required for ongoing business or historical reasons must be deleted as soon as reasonably possible. This is because over-retention can lead to:

- risk of contravening Freedom of Information and Data Protection legislation;
- difficulties in finding the information you are looking for if information remains unstructured; and
- ongoing server capacity issues.

3.4 All important documents and emails that demonstrate action or contribute to policy or decision making must be stored in Visualfiles (where it is related to a specific case) or on the G:drive for longer term retention and review.

3.5 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 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 not be apparent when the conversation has finished.

3.6 Email messages relating to complaint investigation casework must be filed in Visualfiles.

3.7 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 messages;
- For messages sent externally, the sender of the message;
- For external messages received by one person, the recipient; and
- For external messages received by more than one person, the person responsible for the work relating to the message. If this is not clear it may be necessary to clarify who this is with the other people who have received the message.

3.8 Where an email 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. In most instances 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. Where further work is required on an attachment, the initial email message and attachment will be one record, and the copy attachment used for further work will become a completely separate record.

3.9 The title of an email message does not always reflect the reason for capturing an email as a record. This can be avoided by following the guidelines for titling emails at the point they are created. If the email title 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 in the record system (Annex 6). Re-titling emails are particularly important when they represent different parts of an email string as it helps to identify the relevant aspects of the conversation.

3.10 During 90 days after creation, a decision needs to be made as to whether email is a record. If it is it should be transferred to an appropriate place either in visual files (for casework) or the G:drive. Any emails still in Outlook for 90 days will automatically be deleted on a daily basis.

3.12 A further option is storage on an individuals P:drive. However, this is only to be used for personal, non-business emails as when working off-line prior to connecting on-line. The size of P:drives will normally be limited to 50mb to restrict the amount of storage in this folder. Any records held there must be transferred to the G:drive as soon as possible.

Annex 4 - Daily email management (framework)

4.1 As defined in the Lord Chancellor's Code of Practice and BS ISO 15489 - 1:2001 a record is Information created, received and maintained as evidence and information by an organisation or person, in pursuance of legal obligations or in the transaction of business.

4.2 Emails that are a record or part of a record should be moved using the 'drag and drop' process into Visual Files if they relate to casework, or the appropriate folder in the g:drive.

4.3 To 'drag and drop' open Outlook Inbox and minimise window by double clicking on the name bar, and do the same with the g;drive, then move the chosen email(s) by dragging using the mouse, from the Inbox into the chosen folder within the g;drive.

4.4 Before moving the email it is important to ensure that the title of the email reflects the reason for capturing it as a record and should be re-titled if necessary (Annex 3):

- Ensure that FW and RE are taken out of any email titles;
- Where the email also has an attachment, in most cases both should be captured as the record as the email could provide the context within which the attachment is used (Annex 3);
- G:drives will be reconfigured with additional folders to reflect the Corporate Taxonomy;
- To ensure appropriate confidentiality, accessibility to g:drive folders will be locked down by functional area and subject matter to specified users;
- Emails that are not a corporate record need to be deleted and this will be enforced through daily deletions of emails over 90 days old;
- Once an email is destroyed the information will not be recoverable;
- It is the responsibility of the 'Sender' to ensure email records are captured whether they are sent internally or externally (Annex 3) and the responsibility of the 'Recipient' of External messages to ensure email records are captured (Annex 3).

Annex 5 - Access to mail accounts during absences

5.1 In the case of planned absences (eg holidays) staff should use the 'Out of Office Assistant'. The auto-reply message should ideally give an alternative contact and state when a full reply can be expected. Emails should be forwarded to another member of staff during a prolonged absence. Alternatively, where this can be done securely, access to a mailbox should be delegated to another member of a team to ensure urgent messages are dealt with.

5.2 Shared mailboxes can be created where there are a group of people responsible for the same area of work (eg an investigation team, a working group, project team or a section in Corporate Resources). This will help to ensure that queries are answered if members of the team are away from the office. One person should be identified as the 'owner' of a shared mailbox or public folder. The owner is responsible for the overall management of that mailbox or folder.

5.3 In the case of unplanned absences and/or where the member of staff has not made arrangements for access (eg sickness) the manager should arrange redirection of email; authorisation should be requested from the Head of HR Operations and ICT Manager. Access should be in the presence of the line manager. On return, the staff member should be told when and why their mailbox was accessed.

5.4 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. 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; and
- Evidence in support of disciplinary action.

Annex 6 - Naming conventions

6.1 Following an agreed naming convention creates a consistent way of working that makes information retrieval more effective.

6.2 When creating content in any form the following principles must be observed:

- Keep file names short, but meaningful;
- Avoid unnecessary repetition and redundancy in file names and file paths;
- Use capital letters to delimit words, not spaces or underscores;
- When including a number in a file name always give it as a two-digit number, i.e. 01-99, unless it is a year or another number with more than two digits;
- If using a date in the file name always state the date 'back to front', and use four digit years, two digit months and two digit days: YYYYMMDD or YYYYMM or YYYY or YYYY-YYYY;
- When including a personal name in a file name give the family name first followed by the initials;
- Avoid using common words such as 'draft' or 'letter' at the start of file names, unless doing so will make it easier to retrieve the record;
- Order the elements in a file name in the most appropriate way to retrieve the record;
- The file names of records relating to recurring events must include the date and a description of the event, except where the inclusion of any of either of these elements would be incompatible with rule 2;
- The file names of correspondence must include the name of the correspondent, an indication of the subject, except where the inclusion of any of these elements would be incompatible with rule 2;
- The file name of an email attachment must include the name of the correspondent, an indication of the subject, except where the inclusion of any of these elements would be incompatible with rule 2.
- The version number of a record must be indicated in its file name by the inclusion of 'V' followed by the version number and, where applicable, 'Draft'.
- Avoid using non-alphanumeric characters in file names.

6.3 Emails or documents received that do not conform to naming conventions must be re titled: For example:

Before - document from P Smith is received entitled 'complaint'
After - Smith P Complaint on Services

6.4 Remember that subject relevance can diminish over the time or loose context if the document is moved out of its original folder so using words like ‘update’, ‘progress report’, ‘draft’ or ‘letter’ on their own without qualification must be avoided.

6.5 Similarly, the use of current acronyms and abbreviations must be avoided as knowledge of their meaning may be lost over time and/or become ambiguous.