



Records Management

Guidance for the management of emails

2010

Evidence additional element – appendix 47

Document Control Sheet

Name of Document:	Guidelines for the Management of Emails as Records 2010
Author:	Eleanor Rowe, Records Manager
Consultees	ICT Bridget Mustard, Chief Executive's Office Records Management Liaison Group
Description of Content:	The management of emails to ensure appropriate preservation of important information.
Distribution:	Council wide upon approval
Status:	Version 1.0

Evidence additional element – appendix 47

Guidelines for the Management of Emails as Records

Contents:

[Introduction](#)

1. **[The benefits of Email Management](#)**
2. **[Data Protection and Freedom of Information legislation](#)**
3. **[Copyright](#)**
4. **[Managing Emails](#)**
 - 4.1 [Organising your Mailbox](#)
 - 4.2 [Deleting Emails](#)
 - 4.3 [Saving Emails](#)
 - 4.4 [Records Retention and Archiving](#)
 - 4.5 [Access to another persons' emails](#)
 - 4.6 [Making your mailbox manageable](#)
5. **[Identifying and Managing Emails as Records](#)**
 - 5.1 [Essential principles](#)
 - 5.2 [Identifying Emails as Records](#)
 - 5.3 [Who is responsible?](#)
 - 5.4 [Managing Emails with Attachments](#)
 - 5.5 [Managing an Email conversation, string or thread](#)
6. **[Security](#)**
7. **[Legal Admissibility and Liability](#)**
8. **[References & Consultations](#)**

Any enquiries about this policy please contact:-

Eleanor Rowe
Records Manager
Elgin Library
Elgin
Tel 01343 562633
Email : Records@moray.gov.uk

For advice on ICT and Security issues please contact

Mike Alexander
ICT Security Officer
HQ Elgin
Tel 01343
Email

January 2010

Evidence additional element – appendix 47

Introduction

The email has largely replaced written documents, faxes and often even the telephone as the favoured method of communication both internally and externally, as a result large numbers are received and created every day.

Email is a Corporate Information Asset and should be appropriately managed and stored. Emails need to be captured quickly so that they can be retrieved and accessed for their information content, and managed according to the Council's retention schedule so that they are reviewed, destroyed or permanently archived. Emails need to be managed so that the information they contain can be shared by the whole organisation.

The Council should avoid the use of personal email addresses, especially on the website and on customer contact information. Email addresses on Moray Council web pages must be generic addresses rather than personal ones, for example: info@moray.gov.uk for all Freedom of Information (Scotland) enquiries.

Without effective management of emails the following could happen:-

- Risk to the IT network if storage space becomes full.
- Rising costs and efforts associated with trying to store emails, retrieve information or deal with a backlog of emails in individual's in-boxes
- Loss of critical records and information
- Corporate information is inaccessible if emails are held in individual's in-boxes
- Non compliance with access to information legislation such as Freedom of Information and Data Protection

For guidance on the composition of an email please see the **Customer Care Guidelines** on the intranet or on the council website http://www.moray.gov.uk/moray_standard/table_45779.html

For further advice on sending and using emails please see the **Computer Use Policy** on the intranet. <http://www.moray.gov.uk/internal/corpserv/policy/policy.pdf>

1. The Benefits of Email Management

The benefits of managing emails, including reviewing and saving appropriately, is to create a store of readily accessible, relevant and usable information which can be used e.g. to deal with enquiries received under access to information legislation; to track the progress of a contract; follow the decision process and project research etc. It will also ensure that emails are accessible to appropriate staff, during staff absence and after a member of staff leaves. It will also help with server space as emails will not be kept for longer than necessary by referring to the records retention policy. This will also ensure compliance with the Data Protection Act (1998) and Freedom of Information (Scotland) Act 2002.

2. Data Protection and Freedom of Information legislation

The Data Protection Act (1998) and the Freedom of Information (Scotland) Act (2002) apply to all emails sent and received by the Council.

Treat emails in the same way as you would any electronic or paper records.

The Data Protection Act (DPA) allows individuals to seek information about themselves including emails. Staff should therefore be able to find the information easily.

Evidence additional element – appendix 47

DPA also requires that information about identifiable individuals is kept for no longer than is necessary, that the information is accurate and up to date. You should deal with email records as you would any electronic or paper record – reviewing, deleting or archiving according to the Record Retention Schedules on the intranet.

http://intranet.moray.gov.uk/documents/RetentionSchedulesVersion14-5_2011.pdf

Emails containing personal, confidential or sensitive information should also be saved in a secure location just as you would lock paper records in a filing cabinet or save a confidential word document in a password or rights protected area of your computer system.

You should also think before sending an email containing personal information – is this the most secure way of communicating, are you using a secure system for sending the email? For advice on this please contact the ICT security officer.

If you print out emails remember also to destroy them appropriately if they contain personal, confidential or sensitive information – this includes names, addresses, contact details and the email address itself (work email addresses available in the public domain are not confidential). Please see guidance on the Identification and Destruction of confidential, Personal, Sensitive or commercially sensitive records.

The Freedom of Information (Scotland) Act gives anyone the right of access to recorded information held by the Council, including emails. Remember that a third party may request to see your emails so be professional about what you write.

The tight deadlines for answering these enquiries means that information must be readily and easily accessible to save time and frustration in dealing with these requests. Remember - 20 working days for FOI(S)A and up to 40 calendar days for a Data Protection request.

Please see the **Freedom of Information guidelines** and the **Data Protection guidelines** on the intranet and the internet under Information Rights for further information about the legislation:-

http://www.moray.gov.uk/moray_standard/page_41220.html

3. Copyright

An email message to a single person is like a letter as far as copyright is concerned. Copyright remains with the author or the employer if the email was created as part of your job. An email to a single recipient does not imply a license to publish the message nor, unless stated or permission sought, can the message be forwarded to someone else. Email messages to a discussion list are like letters to a newspaper and permission to publish and share the contents is implicit. To keep an email message personal or confidential a note to that effect should be included with the message.

4. Managing Emails

4.1 Organising your Mailbox

It is the responsibility of all members of staff to manage their email messages appropriately. To achieve this staff need to identify email messages that are

- a record of their business activities
- ephemeral email messages which will not make significant contribution to the business of the Council.

Emails identified as records (in the same way as a conventional letter or paper document or an electronic document) should be moved from an individual's mailbox (individual mailbox includes

Evidence additional element – appendix 47

the in-box and folders created under the in-box, and the sent box) and managed with, and in the same way, as other records.

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

4.2 Deleting emails

Emails should be regularly deleted if they are not saved as Records of actions and decisions taken. Remember deleting an email from your in-box doesn't mean that it is automatically deleted from the system – empty the deleted items folder and contact the ICT Security Officer if you need advice. Even when they are deleted from this folder they will remain backed up on the ICT servers until such time as these are 'emptied'; the time taken to erase the backups varies depending upon the server being used.

The Retention and Disposal Schedule says review email inboxes every 3 months and destroy records no longer required. Review regularly after another 3 months or retain permanently as record on shared system

Emails and attachments saved as records should be kept according to the retention schedule appropriate to the content.

4.3 Saving Emails

Electronic Document Records Management Systems

Emails should be saved to the Council's electronic document and records management system. File according to the Council file plan according to the subject matter of the email.

Once the email has been saved as a record it should be treated the same as other records and dealt with according to the Retention Schedules available on the intranet

http://www.moray.gov.uk/documents/council_retention_schedules.pdf

The content of the email will decide the type and category of record and its fate.

Attachments

These should be saved separately according to the Council file plan and naming conventions. Often the attachment is the document which contains the information required. The email is merely the messenger! Make sure that you save the correct version and try to ensure that different people are not all saving the same attachment.

4.4 Records Retention

Emails which have been identified as Records will be treated like other records of the same subject and dealt with according to the Retention Schedules available on the intranet

http://www.moray.gov.uk/documents/council_retention_schedules.pdf

4.5 Access to another person's emails

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, e.g. During annual leave or extended sick leave. The reasons for accessing an individual's mailbox are for business purposes and business continuity, which may include requests for information under Freedom of Information or Data Protection legislation.

Evidence additional element – appendix 47

Where it is not possible to ask the permission from the member of staff whose mailbox needs to be accessed there is an authorisation procedure in place – please contact ICT for help. Remember to keep a record of the reasons for accessing the mailbox together with the names of the people who were present and 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 and mailbox access is delegated to a colleague.

There are guidelines on the intranet on how to forward new, incoming emails to a colleague and an out of office message if you are away from your desk for more than 2 days.

4.6 Making your Mailbox Manageable

Managing an email mailbox effectively can appear to be a difficult task, especially if the number of email messages received is large. Managing an email mailbox should not be about following rigid classification guidelines; it is about following a methodology that works best for you. There are a number of approaches that might aid the management of email messages including:

- Allocating sufficient time each day or week to read through and action email messages – deleting or saving as appropriate to content
- Prioritising the order in which email messages need to be dealt with
- Looking at the sender and the title to gauge the importance of the message
- 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.
- Using folders to group email messages of a similar nature or subject together so they can be dealt with consecutively and retrieved easily
- Identifying email messages that are records or need to be brought to other people's attention
- Keeping email messages in individual's folders only for short-term information. Emails that are required for longer purpose should be managed as **records** [see section 5 below].
- Deleting email messages that are no longer required from the inbox, deleted items box and sent items.

5 Identifying and managing Emails as Records

An email as such is not a record - the subject matter is what makes it a record. This means that filing the email and the retention period for the email depends on the content. Every email should be treated exactly as an electronic or paper document of the same subject would be treated.

5.1 Essential Principles

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. Remember to use a meaningful name which complies with your Council file plans. Electronic document management systems can be used to capture emails classed as records. Once an email message has been captured as a record it should be deleted from the email client.

5.2 Identifying Emails as Records

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

Evidence additional element – appendix 47

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.

They will contain information which will provide evidence of why decisions were reached, actions taken, decisions made, background information and research undertaken. They may be seen as vital to the continuity of the service and to the provision of an audit trail about actions and decisions made.

5.3 Who is Responsible?

As email messages can be sent to multiple recipients there need to be specific guidelines on who is responsible for capturing and saving 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. If this is not clear it may be necessary to clarify who this is with the other people who have received the message.

5.4 Managing Emails with Attachment

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. It is most likely that the attachment will be saved as a record along with the email message which provides the context for the attachment.

There are times when 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.

5.5 Managing an email conversation, string or thread

Most email messages will form part of an email conversation, string or thread of discussion on a particular topic. It is not necessary to keep each new part of the conversation, i.e. every reply, separately. It may be sufficient to keep the one email which captures most of the thread of the discussion with an appropriate subject heading to enable it to be retrieved.

Email strings should be captured as records at significant points during the conversation, rather than waiting to the end of the discussion because it might not be apparent when the conversation has finished.

6. Security

Please see the ICT Security Policy

Always use the correct email address.

Always use a work email address for work.

If you are unsure about sending personal data, (which includes name, address, telephone number, email address, identifiable photograph, membership details) or sensitive personal data, (which includes information about political opinion, racial and ethnic background, religious beliefs, mental

Evidence additional element – appendix 47

or medical condition, trade union membership, sexual life, offences or criminal proceedings and financial information) please check with the ICT Security Officer.

7. Legal Admissibility and Liability

Email content is admissible in court in the same way as verbal and written expressions and statements are.

Emails may contain information which will hold the Council liable by assuming that the author and creator of the email was acting on the behalf of the Council. All emails sent from the Council system will bear a statement concerning liability.

8. References

Data Protection Act (1998)

Freedom of Information (Scotland) Act (2002)

Human Rights Act (1998)

Customer Care Policy –The Moray Council

http://www.moray.gov.uk/moray_standard/table_45779.html

Computer Use Policy – The Moray Council

<http://146.116.190.100/internal/corpserv/policy/policy.pdf>

Security of Information Policy – The Moray Council

Review of Mail Dispatching Procedures, (2007). The Moray Council, intranet May 2007

http://146.116.190.100/documents/Chief_Executive/review_of_mail_dispatching_procedures.pdf

Record Retention Schedules, The Moray Council intranet

http://146.116.190.100/documents/council_retention_schedules.pdf

Craine, K (March 2007) *The Strategic importance of email archive management*, Records Management Society Bulletin March 2007

Russell, E (2004) *Guidelines on developing a policy for managing email*, The National Archives

Information Commissioner (2003), *The Employment Practices Data Protection Code: Part 3: Monitoring at Work: Supplementary Guidance*,

<http://www.dataprotection.gov.uk/dpr/dpdoc.nsf>

International Standards Organisation ISO 15489 *Information and documentation: Records Management, Part 1* 2001

BS ISO/IEC 17799:2000, BS 7799-1:2000 Information technology. Code of practice for information security management

BS ISO/IEC 27002:2005, BS 7799-1:2005, BS ISO/IEC 17799:2005 Information technology. Security techniques. Code of practice for information security management

Copyright, Designs and Patents Act, 1998

Padfield, Tim (2004) *Copyright for Archivists and users of archives*, Facet Publishing

Evidence additional element – appendix 47

Norman, Sandy (2004), *Practical Copyright for information professionals, The CILIP Handbook*, Facet Publishing

Consultations

Mike Alexander, Information Security Officer, ICT

Phil MacDonald, ICT Project Manager

Bridget Mustard, Corporate Services Manager, Chief Executive

Nichola Smith, Quality Assurance Officer, Environmental Services – development

Workflow and Document Management Team, DBS project

Revision - This document will be revised regularly in liaison with ICT