National Records of Scotland

Managing Email Policy

July 2016

1. Introduction and Purpose

1.1 National Records of Scotland (NRS) is committed to improving the way in which electronic documents are managed and used throughout the organisation. A framework of guidelines to support colleagues has been developed in cooperation with all staff. This Managing Email Policy is one element of the framework and must be followed by all staff when managing emails.

1.2 Email need to be managed effectively in order to enable the efficient storage and retrieval of information; support compliance with all relevant legislation, including the Data Protection Act 1998, Freedom of Information (Scotland) Act 2002 and Public Records (Scotland) Act 2011; and reduce costs and pressures on server storage space.

2. Sensitive Information

2.1 It is the responsibility of all staff to ensure that personal and sensitive data is kept secure and is protected at all times. The privacy and confidentiality of information sent outside of a secure email network cannot be guaranteed, therefore, care must be taken when using email to communicate such data.

2.2 Staff in our Edinburgh buildings have access to the SCOTS network which has been accredited for the Government Secure Intranet (GSi). Staff in the NHSCR at Cairnsmore House work predominantly on the NHS network and use NHSmail which is connected to the Gsi service.[1] This allows all of our staff to send documents with Government Security Classifications markings[2] of OFFICIAL and OFFICIAL-SENSITIVE to each other and also to other government departments who also have access to GSi. Care is required when sending protectively marked documents outside of the GSi and staff should follow guidelines in the *NRS Data Handling and Management Policy* and/or consult the Information Security team for guidance. There is no requirement to mark emails containing routine OFFICIAL information, but emails containing sensitive information should be marked OFFICIAL-SENSITIVE in their subject header and body. This should be followed by additional handling instructions detailing distribution and access requirements for the sensitive information.

2.3 Emails containing information that is not intended for general distribution should be clearly marked either in the title or at the beginning of the message. Furthermore, when sending emails of a sensitive or confidential nature, you should mark this clearly in the subject heading of the email.

2.4 Colleagues should ensure that care is taken when sending or forwarding emails in order to ensure that sensitive and/or confidential information is not being passed on without the appropriate permissions. In particular, colleagues should check the intended recipient's address carefully before sending an email, as the auto-complete function within Outlook can result in an incorrect address being substituted for the intended recipient.

[1] When procured NHSmail2 will also be interconnected to support co-existence.
[2] For more information on the Government Security Classification Policy see Saltire: http://intranet/InExec/SEAndMe/Secure/NGSCP/Intro.

2.5 Emails containing personal information are covered by the Data Protection Act 1998 and must be treated in line with the principles outlined in the Act. Under the Act, personal information includes opinions about an individual or the personal opinions of an individual. Emails containing this type of information should only be used for the purpose for which the information was provided/collected, be accurate and up-to-date, and must not be disclosed to anyone outwith NRS without the express permission of the individual concerned.

3. Responsibilities for Managing Email

3.1 It is the responsibility of all staff to manage their emails appropriately. Colleagues should identify emails that are records of their business activities and transactions, move them from personal mailboxes and manage them alongside other records.

3.2 It is the responsibility of the sender of an email or the initiator of a dialogue to decide if the email and/or attachment(s) constitute an official record. If the email or its attachment(s) contain key decisions and/or actions taken, it should be considered a record, renamed, if appropriate, in accordance with the '*Document Naming Guidelines*' and saved in the most appropriate place.[3]

3.3 If you are the sole recipient of an external email or, if there are several recipients, and you are responsible for the most relevant work area, it is your responsibility to decide if the message forms part of an official record or not and take responsibility for its management.

3.4 When managing emails in a shared mailbox, colleagues must be clear as to who is responsible for the retention, naming, capture and disposal of emails within the mailbox. Without the identification of these clear responsibilities, emails may be lost or duplicated. It is recommended that the folder owner is the designated person with responsibility for a shared mailbox.

3.5 The limited use of email for personal use is permitted within NRS, but you must conform to the rules concerning appropriate usage and be aware of your responsibilities for the content and management of such communications. This is set out in the Scottish Government *IT Code of Conduct*.

3.6 Emails that contain information that is not supported by fact should indicate that it is the sender's opinion that is being expressed.

3.7 Occasionally it may be necessary to access an individual's mailbox. For example, to action:

- Subject access requests under the Data Protection Act;
- Freedom of Information requests;
- Evidence in legal proceedings;
- Evidence in a criminal investigation;

[3] This may be in Quickr, in a branch/divisional shared drive, or in a paper file to be stored, after it has been closed, in the Records Management Unit. Colleagues should ensure that the email is available to all staff who require access to it, bearing in mind any security and/or access implications. Moving forward, these records are to be stored within a corporate electronic records management system.

- An urgent business enquiry;
- Evidence in support of disciplinary action.

In these circumstances, the first action must be to seek authorisation from the individual and obtain delegated rights of access (if this has not already been established)[4]. Where it is not possible to ask for an individual's permission, the procedure for gaining access to their mailbox is:

- Gain authorisation from your Head of Branch, the individual's Head of Branch and Human Resources, in writing;
- Submit a request to the IT Helpdesk, stating how long you require access to the mailbox;
- Access is gained in the presence of your Head of Branch;
- 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.

Emails which have been archived in the Enterprise Vault can be searched organisation wide by system administrators, but the same procedures for authorisation of access must be followed.

4. Retention and Disposal of Emails

4.1 An email's value is based on its content, so the retention or disposal of emails should be based on the information they contain or the purpose they serve. The content of emails may vary considerably, so no single retention period applies to all email. Please see the table below for further guidance.

Type of Message	**Examples**	**Value**	**Retention**
Transactions that provide evidence of your business activities.	Emails recording policy decisions, evidence of business transactions with stakeholders (including attachments).	Records required for ongoing business.	To be retained in accordance with the Retention and Disposal Schedule.
Information messages with a business context but not part of a business transaction.	Notifications of meetings, general circulars to staff, travel arrangements, discussions in which you were involved but another member of staff has responsibility for documenting and recording.	Records of short-lived value.	Destroy when administrative use is concluded.
Personal emails.	Any personal or social emails or junk mail.	None	Destroy when no longer required.

[4] Colleagues are advised to identify delegates who may access their mailbox and view content in their absence. Delegates, and their associated permissions, can be set up in the Options field in Outlook.

5. Capturing Emails and Attachments

5.1 In order to prevent loss of information, emails must be acted upon and moved to an appropriate location as quickly as possible.

5.2 It is not necessary to capture every email in an email conversation string, separately. Instead, emails should be captured at key points during the conversation, when key decisions are made and transactions are processed.

5.3 Email attachments should be saved as part of a record, in order to provide context to an email. However, there will be occasions when it won’t be necessary to capture both the email and its attachment. For example, if an attachment has been sent for reference purposes only and you know it has been captured elsewhere.

5.4 When capturing emails, the Outlook Message Format (.msg) should be used in order to ensure that the saved email is a true representation of the email as a record and retains the characteristics of the original email.[5]

5.5 If the title of an email does not accurately reflect the content of the message then it should be re-titled at the point it is captured. 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. Please refer to the *Document Naming Guidelines* for further information.

6. Email Archiving and .pst

6.1 Email services operate on SCOTS V using Exchange 2010 and archiving software, Enterprise Vault 10. Emails will remain in your Outlook mailbox for 60 days and will then be automatically archived in Enterprise Vault for 1 year before deletion. If you want to retain emails for a longer period you can move them to the #Archive folder from where they will be archived overnight to Enterprise Vault and retained for 3 years before deletion. You cannot extend the retention period of emails which have already been automatically archived so if you want to keep emails for a longer period you will have to move them across to the #Archive folder within the first 60 days. As stated above emails with corporate value should be separately saved as a corporate record alongside other related records.

6.2 ISIS no longer permit users to either create Personal Storage Table (.pst) files to store and retain emails or to add emails to existing .pst.[6] This configuration is known to cause performance issues for the end user and is not supported by Microsoft. The content of existing .pst files on personal or shared network drives should either be transferred over the #Archive folder or deleted. Be aware that any .pst file which has been stored on the C drive of your PC will not be secure. Any other user who logs into your PC to hot desk will be able to access the contents of your .pst file. This security issue should be an added incentive to empty the content of any .pst files you retain as soon as possible.

[5] To save, click File-> Save As then select Outlook Message Format from the ‘Save as type’ drop-down menu.

[6] Saltire explains in more detail why the use of .pst is being discontinued on SCOTS V: http://intranet/InExec/SEAndMe/IT/SCOTSVhome/Guidance/pstsinscotsv

7. Some Final Tips[7]

- ✓ Set aside time on a daily/weekly basis to regularly clean up your mailbox.
- ✓ Where possible, use shortcuts or links to documents rather than sending attachments; in particular when emailing a group of recipients or large attachments
- ✓ Try to limit email messages to one subject per message
- ✗ Do not allow others to read personal information by leaving your screen in view and unattended
- ✗ Do not use .pst file formats to capture emails outside of Outlook
- ✗ Do not forward chain emails

7. Legislative Framework

7.1 There is a wide range of legislation available to tackle the potential criminal and civil liability issues that may arise from employees' misuse of communication facilities while at work. Some of the key statutes are listed below:

- Equality Act 2010
- Communications Act 2003
- Freedom of Information (Scotland) Act 2002
- Data Protection Act 1998
- Protection from Harassment Act 1997
- Computer Misuse Act 1990
- Civic Government (Scotland) Act 1982

8. Relationship to other NRS Policies

8.1 This policy forms part of NRS's overall framework but specifically relates to the following policies and procedures:

- Data Protection Policy
- Retention and Disposal Schedule
- Document Naming Guidelines
- Data Handling and Management Policy

[7] For further guidance on *Email Management and Best Practice* is available on Saltire: http://intranet/InExec/SEAndMe/IT/Guidance/SCOTSGuidanceNew/email/emailMagtBestPract/IntroBestPractice