Registers
of Scotland
ros.gov.uk

Security and Information Assurance

E-MAIL POLICY

Registers of Scotland
Departmental Security Group
Policies and Procedures

Department	Security and Information Assurance (SIA)
Topic	E-mail Policy
Number	SIA11
Date	25 June 2015

Introduction

Registers of Scotland (RoS) provides electronic mail (e-mail) facilities to all staff for effective and efficient business communication both internally and externally to allow staff to communicate effectively and competently with other Government Departments and Agencies and/or any Internet connected organisation or persons. This means of communication brings many benefits for RoS and staff, but also brings certain risks. Therefore, it is necessary to provide a RoS policy and procedures for the use of e-mail and remind staff that breach of this policy may result in disciplinary action being taken against them.

Access

Access to e-mail, for business use, is provided to staff on condition that they accept and comply with RoS E-mail Policy. Access to e-mail for brief personal messages in line with this policy is entirely at the discretion of RoS and should be kept to a minimum. Any such emails should be marked as “personal” using the sensitivity option under the Options tab in Outlook. Email facilities must be used in a way that does not interfere with official business or otherwise detract from the performance of official duties. The RoS e-mail system, and user’s e-mail addresses, must not be used by staff for personal commercial activities. Access to email may be withheld or withdrawn at any time without notice.

If you are aware of any illegal or inappropriate activities in connection with e-mail usage in RoS you should contact the RoS SIA Team *(IT.SecurityOfficer@ros.gov.uk)* (Ext 3333) in confidence.

Remote Access

Remote access to RoS email servers (for accessing email and files) is possible, subject to appropriate authorisation. Please discuss any needs with your team leader/manager. This policy applies equally when accessing RoS email servers remotely. Additional care and vigilance should be exercised when using remote access.

Status of e-Mail

There is no distinction between data recorded and conveyed in an e-mail and that conveyed by other means such as minutes, reports, papers or letters. All e-mails generated, or received by RoS staff, including any attachments, are public records and therefore are subject to RoS records management policies and procedures. If the sender or recipient of an e-mail, including copy addressees, decides it needs to be retained it should be treated like any other document and saved in the appropriate location, relative to the subject of the e-mail, within the shared user group structure.
E-mail and their attachments may be subject to copyright laws, intellectual property rights and other statutory or non statutory obligations and due care must be taken when publishing them, for example by making a copy available on a website. Where there is any doubt the author should first be consulted.

Types of e-mail

E-mail created or received by RoS staff can generally be divided into three types:

- *Corporate e-mail* – e-mail which relates to RoS business and which must be retained as a record e.g. policy direction. If an e-mail incorporates personal and/or transient content as well as work-related information, then the e-mail will be dealt with as a corporate record.
- *Transient e-mail* – e-mail which is used to facilitate RoS business but which does not need to be retained for business purposes e.g. correspondence arranging a meeting.
- *Personal e-mail* – e-mail which is of a personal nature and which has no relevance to RoS business e.g. ‘Let’s meet for lunch’. These e-mails should not be retained.

Retention and Disposal of e-Mail

If the message conveyed in an e-mail contributes to full understanding of a decision, results in action being taken, or forms a significant part of the 'story', it must be kept. If not, it should be deleted. Those e-mails not required 'for the record' should be deleted as soon as they have ceased to be of use. E-mails that are retained as corporate records must be deleted from inboxes or other storage areas immediately they have been successfully added to the official record. Personal, transient and other e-mails not added to the official record keeping system should also be deleted as soon as they have ceased to be of use. Individual members of staff are responsible for doing this.

Content

Email content should be kept short, polite and factual. Long messages should be conveyed by hyperlinks to the document in the RoS electronic record keeping system. In the case of external e-mail, they should be conveyed as separate documents that are attached to the e-mail.

The style, tone and content of emails have a direct effect on the way RoS is perceived by others. Personal comments and judgements should only be included where these are relevant to the issue in hand. For detailed e-mail rules and guidance see the Annex.

Security

You are responsible for protecting your email account by taking appropriate security measures, such as locking your workstation when it is unattended and shutting it down at the end of the working day.

All emails that are sent externally automatically contain the standard RoS disclaimer. You must not delete, alter or otherwise interfere with the automatic disclaimer.

Further information on security can be found in the Safeguarding RoS Information guide.

Sensitive Information

Staff are permitted to internally email sensitive information as these communications remain on RoS private secure network. External email, however, travels over the internet, which is not a secure way of transmitting information. Communications can be intercepted, modified, copied, widely distributed and disclosed to individuals other than the intended recipients. Therefore, the internet cannot be guaranteed as a safe medium for transferring protectively marked information. The Safeguarding RoS Information guide provides guidance on safe email transmission over the internet.

Disclosability

As e-mail forms part of the public record there may be a legal obligation to disclose any information held within an e-mail under Freedom of Information and Data Protection legislation. E-mails will also be disclosable to Public Inquiries and other government inquiries. Internal and external e-mails are liable to be disclosed in civil litigation and criminal proceedings, hence the reason they should not contain any information which could be offensive to any organisation or person, or any information which could be damaging or embarrassing to RoS. Internal e-mail in one department may have to be disclosed in proceedings involving another department. Incoming and outgoing e-mails are covered by the Data Protection Act so that e-mails in personal mailboxes and deleted items boxes are also potentially disclosable. If you have any questions about data protection, contact the RoS Data Protection Officer.

Emails as records

Responsibility lies with the e-mail originator for internal e-mail and the recipient for incoming external e-mail for deciding whether an e-mail is to be retained as a corporate record or whether it can be deleted immediately. Only Corporate e-mails should be retained as they constitute a record of RoS activity.

This policy applies to all members of RoS staff using e-mail, internally and externally, as part of their duties. The procedures outlined below will apply to the following uses of e-mail:

- *Internal e-mail and External e-mail sent on behalf of RoS* – the e-mail's author should save it to an appropriate location, either in a specific e-mail folder or to the appropriate folder in a shared directory.
- *Incoming External e-mail* – *e*-mail arriving in RoS can be Corporate, Transient or Personal. It is the responsibility of the recipient, or the first named recipient to decide if it is a corporate e-mail and save it accordingly.
- *E-mails sent both internally and externally* – as it is not possible to access a file hyperlink contained in an external e-mail, the practice will be to e-mail attachments externally, but hyperlinks internally.
- *Attachments* – wherever possible hyperlinks to documents or records held on the network should be used in preference to attaching the files to an e-mail. The use of hyperlinks serves two main purposes: mail traffic is minimised; and it is a more secure means of document transfer.

Any document or record attached to an e-mail or hyperlink contained in an internal e-mail should already be a corporate record and no further action need be taken. Any attachment contained in an incoming external e-mail which is considered to constitute a corporate record should be saved by the recipient, or the first named recipient, as well as saving the e-mail itself.

Monitoring e-mail

RoS monitors e-mails for security and audit purposes, including checks for offensive material, unauthorised use and to guard against viruses etc. All instances of apparent inappropriate use will be investigated. Any e-mail may be viewed at any time as part of this monitoring process, and therefore cannot be regarded as private. RoS may access e-mail messages relevant to the business on staff mail boxes whilst the member of staff is absent from work, for example on leave. If you have any queries or concerns about monitoring you should contact RoS Data Protection Officer.

Misuse

Any breach of this e-mail policy may be treated as serious misconduct and would be subject to action (up to and including dismissal) under the RoS Disciplinary Procedures

Updates

Since the technology and law in this area are subject to change, this policy will be monitored and updated as necessary.

ANNEX

Rules

Many of the rules that apply to normal correspondence also apply to e-mail. However there are some specific rules you should follow when constructing e-mails. Read the following carefully. If there is anything you do not understand, it is your responsibility to ask your team leader or manager to explain.

Restrictions

- Be careful not to commit RoS to unwanted contracts. You have no authority to commit RoS to any contractual arrangements unless approved by your manager in accordance with our standard procurement procedures.
- You must not present any views and opinions that you personally hold as views of RoS.
- Do not send e-mails containing sensitive information unless authorised to do so through the appropriate channel.
- RoS e-mail must not be (auto) forwarded to any non-RoS e-mail account.

Unauthorised Content

- Do not defame or make derogatory, rude, inflammatory or offensive remarks about another person or organisation. You should be no less careful than when writing a letter, ensuring you never make insulting, indecent, obscene, sexist or racist remarks.
- If you receive an offensive or insulting e-mail, inform your team leader/ manager immediately. Do not send or respond to this sort of e-mail. *(Dignity at Work policy).*
- Bullying and harassment can occur by email. All users must ensure that they avoid using a bullying tone or style when sending email. Remember that what is considered offensive material is determined by the effect on the recipient, not how it is regarded by the sender.
- Take care that material in e-mails does not contravene the laws of copyright and data protection.
- You must not use email to impersonate others or to forge messages or email addresses.

Unsolicited email

- Do not send, respond to or forward “chain letter”/pyramid e-mails. You should report such e-mails to the SIA team (Ext. 3333).
- Treat all e-mails with attachments and hyperlinks with care. If the subject matter of the e-mail looks suspicious, even if the e-mail has come from a trusted source (e.g. another member of staff) do not open the e-mail. Attachments and embedded links in emails are a potential source of virus infections. RoS has anti-virus software in place but, as this can only detect known viruses, there is a risk that new viruses can be spread before effective protection is possible. Please seek the advice of the SIA team (Ext. 3333) if you are not sure if an email is genuine.
- If you receive an email containing some warning message encouraging you to forward the email on to others, do not forward it on but contact the SIA team (Ext 3333). These are usually hoax messages.

Rules (cont.)

Out of Office Assistant

You must switch on the "Out of Office Assistant" before leaving the office if you know you will not be in the office and/or will be unable to pick up your emails for periods of one working day or more.

You should ensure that your Out of Office message includes the following details:

- Date on which you are absent or will return to the office [or be able to pick up emails];
- Contact details for someone to whom urgent queries can be directed in your absence;
- A statement that you will respond to any enquiries on your return.

e.g. "I am out of the office until Wednesday 5 April. If your enquiry is urgent, please contact xxxx xxxxx on [Telephone Number & Extension] or via email xxxxxxxxx@ros.gov.uk in my absence. Otherwise, I will respond to your enquiry on my return."

Please ensure that the person to whom you are re-directing enquiries is aware of this arrangement.

Because you do not know to whom an Out of Office message might be sent, for security reasons it is best to avoid including details of where you will be during your absence.

Remember that email is a business tool and you should be careful when composing your Out of Office message to ensure it is accurate and contains only business information.

In cases where team members go on a period of sick leave lasting three or more days, team leaders should compose an appropriate message and forward this to the IT Service Desk requesting that the Out Of Office function be activated.

When a member of staff leaves RoS, their email account will be disabled and for a set period an automated Out of Office message will be sent to all incoming emails to request that enquiries be redirected. After the set period ends, senders will thereafter receive a non delivery message.

Guidance

Etiquette

- Consider if there is a need to reply to an e-mail which you have been copied ("cc'd") to.
- Don't use e-mail for supervisory functions such as feedback on job performance and disciplinary matters, these type of issues are best dealt with on a confidential face to face basis.
- As the sender, you have no control over the future use of data conveyed in an e-mail and so must exercise care in deciding how widely to distribute the message.
- Prioritise e-mail; e-mail lets you mark any important messages as "High Importance" Use this function with care and only when your messages are

genuinely important. If you are unsure whether to mark a message as "High Importance" ask yourself if the message is so important the recipient would wish to put other tasks aside to read your mail.

Housekeeping

- Regularly delete old and out of date e-mails from your inbox and Sent Items. Keep your inbox tidy, possibly by setting up topic folders.
- Outlook has feature to automatically empty the Deleted Items folder on exiting the programme, this should be used unless there is a valid business reason not to.

Group emails

- Do not send unsolicited, trivial e-mails to groups of e-mail users.
- Use the blind copy function to email groups of users.
- Do not "mass mail" all users. In the event of requiring to send e-mail to very large numbers of staff, requests should be directed through Internal Communications Section who have the procedures in place to carry this out.

Attachments

- Avoid sending attachments wherever possible – send plain text e-mails or send hyperlinks to files saved on the network using the e-mail hyperlink function.
- Treat attachments from unsolicited e-mails with suspicion.

Email Signatures

Email signatures are automatically added to outgoing emails where the function is being used. They can be set up in Outlook. Email signatures as a minimum should include your name, job title and phone number.

Sensitive Information

When sending sensitive information, the "importance" and "sensitivity" settings in Outlook should be considered and the guidance in the Safeguarding RoS Information booklet must be followed.

Disclaimer

The following disclaimer appears at the end of emails sent externally:

"This e-mail and any files transmitted with it are confidential and intended solely for the use of the individual or entity to which they are addressed. If you have received this e-mail in error please notify the sender immediately and destroy all copies. Registers of Scotland does not accept any liability or responsibility for any damage caused by any virus transmitted by this e-mail or for changes made to this e-mail after it was sent.

For information on Registers of Scotland and the products and services we supply, visit our website at https://www.ros.gov.uk/.