| States of Jersey | Email Good Practice Guide |
|---|---|
| IS-GUIDE-003 | |

# Table of Contents



# 1. Purpose

This document is designed provide practical guidance on using email to communicate electronically. This is to ensure:

- Communications are effective
- Legislative requirements are met
- Evidence in legal proceedings or criminal investigations is available
- Corporate records are properly managed and available

This document can be applied to any electronic mail used for States of Jersey communications. This normally refers to government-owned or -managed email, such as @gov.je addresses. However, much of the guide is best practice and can be applied to other communications platforms.

# 2. Limitations of email

## 2.1. Delivery is not guaranteed

There is no guarantee that messages transmitted over the Internet will be delivered swiftly or reliably. Messages can get lost or delayed at any one of several places on route to their destination. Even when the States internet service is in perfect operation, we will never be in a position to guarantee delivery. When sending critical emails, please contact the recipient to ensure the email has been received.

## 2.2. Security is not guaranteed

When email has left the States network and is on the internet, it can be intercepted by anyone who is willing to try. Therefore do not send any information that can be regarded as sensitive. For further guidance on sharing sensitive information, refer to IS-POL-001 (Acceptable Use Policy) and IS-POL-002 (Information Classification Policy). It is also essential to follow any confidentiality agreements that are in place.

### 2.3. File Attachments

There are restrictions placed on the type of attachment that can be sent and received. Messages than contain executable and multimedia file types will not be delivered and you will receive an email notification of this.

There are also restrictions on emails with encrypted or password protected attachments. This is because we cannot verify the content of the email due to the encryption, and it could contain a virus or unwanted file type. Messages containing encrypted or password protected attachments will not be delivered and you will receive an email notification of this. If you have a requirement to send or receive encrypted attachments on a regular basis, please contact the IS Service Desk.

From time to time security bugs are found in certain document types – PDF, Word, and RTF being common ones. When we hear about these issues we may block the affected file type from passing through our mail gateway to protect our systems.

### 2.4. Profanities

Every email is checked for profanities by an automated process. However, some messages may slip through. Bear in mind that emails may be legally discoverable, or need to be published as part of a Freedom of Information request. Profanities can offend, cause the States embarrassment, an in extreme cases have legal consequences.

There are occasions where emails are mistakenly stopped because of business related content such as health terminology. If this causes an issue please contact the IS Service Desk who may be able to help with unblocking it.

### 2.5. Message size

To reduce email volumes, delivery problems, and duplication of records it is always better to send a link to a document rather than attach a copy. In any case messages larger than 30mb will not be delivered and you will receive an email notification of this. If you must send a large attachment then compress (zip) the attachments first to save space.

## 3. Etiquette

### 3.1. Watch your words

Email maybe a less formal method of communicating than a letter, but you are still representing your unit, area, department, or, in the case of external emails, the States of Jersey.

Emails can be forwarded to a number of other people without your knowledge. With Freedom of Information Law, you should treat each email as an unsealed letter. When responding to business related emails, do not include personal comments or anecdotes that do not relate to the topic at hand.  Never write anything that you wouldn't be happy communicating more widely.

Avoid using capitals except as necessary. They can be seen as shorthand for SHOUTING in emails and can seem AGGRESSIVE AND HOSTILE.

### 3.2. Be clear, accurate and concise

Be polite, to the point and check spelling and grammar. Give your email a clear subject header so that the person receiving it knows exactly what you're communicating with them about. If the message is to a member of the public, to a large number of individuals, to sensitive then consider having it checked by a colleague first.

### 3.3. Don’t overuse it

Email is a valuable form of communication that is degraded by overuse. Many emails are dashed off in the heat of the moment. Pause before you click the ‘reply to all’ button and question whether everyone on the address list needs to see your message. If your enquiry is insignificant or concerns just one person, it may be better to use the phone.

### 3.4. Consider your audience

Many people use email as a record of having done something, or to show that they are in the process of doing something. Consider whether this is necessary or whether you’re using email to protect yourself, rather than as a communication tool. Ask yourself:

- Is this information useful to this person?
- Is this level of detail appropriate for this person, or should I send them a summary when I have collected everyone's comments and we have come to a conclusion?
- If you are sending non-urgent information that does not need a response, put ‘FYI’ (for your information) at the beginning of your subject heading.

### 3.5. Sending to personal email accounts

You should never send States material to your personal email address, for example to work on it at home. There are several very good reasons for this:

- By using external email for States matters, you potentially bring that email account into scope for electronic discovery or Freedom of Information disclosure.
- External email, and webmail in particular, is more vulnerable to attack than our corporate email service. It is unsuitable for sensitive government material.
- Under the Acceptable Use Policy, this would be a breach of policy. You would therefore have apply for a policy exemption to forward internal emails externally

Irrespective of the above, in theory there is no need to do this. ISD provide various services that can give you secure remote access to email and other internal systems. Contact the IS Service Desk who will advise you on the options.

### 3.6. Forwarding messages

When forwarding messages take special care with long conversation threads. Older parts of the conversation may contain information that should not be shared with the next recipient. Only forward the part of the conversation that is relevant.

### 3.7. Dealing with sensitive subjects

Staff must ensure that all information of a sensitive nature that is sent via email is treated with care in terms of drafting and addressing. Information that is incorrect might provide a case for initiating legal proceedings against the person sending the information and/or the organisation.

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

- Information covered by a security classification higher than OFFICIAL should not be sent via standard email
- messages containing information that is not intended for general distribution should be clearly marked either in the title or at the beginning of the message
- messages containing personal information are covered by the data protection law and must be treated in line with the principles outlined in the law. The obvious areas of concern would be:

a. data subject access rights – the subject of the email has the right to request details of the content (sixth principle). Email language tends to be informal, may not be factual, and as a result disclosure may be embarrassing or even have legal consequences.
b. protection against unauthorised processing or accidental loss (seventh principle). Email can easily fall into the wrong hands, through deliberate or accidental act. There are little in the way of technical controls to prevent this.

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

### 3.8. Out of office

Whenever you are out of the office and unable to respond to email for any length of time, you should set an out of office message. Personalised out of office messages may be seen by the public. For this reason, you must not include any personal details about the reason for your absence.

### 3.9. Contact Details

You must provide contact details and your full name at the bottom of every external email you send. You can create an auto signature that is added to every email you send or reply to. Check to see if there is a standard format for your department.

### 3.10. Broadcast emails

If a message needs to be sent to a large number of internal recipients, consider using alternative means of communication such as MyStates. Discuss the your requirements first with management; they may prefer you to use the Communications Team, who are authorised and trained in sending out mass communications.

Only ever send external messages using the bcc (blind carbon copy) field, not the to: or cc: fields, otherwise recipients' email addresses will be disclosed to one another.

Where possible check the accuracy of external addresses, and be prepared to honour any requests to be removed from a mailing list.

## 4. Malicious Email

### 4.1. Viruses

Internet email poses a huge virus risk. The Melissa virus outbreak was carried around the world via email, and caused widespread system crashes within hours. Viruses can be hidden in the email, in links or attachments. Do not pass on chain letters; they are a popular hoax and will clog up the email system. Please delete the message if you suspect it to be a virus hoax.

### 4.2. Unwanted mail

If you are receiving a lot of unwanted nuisance email, please log a call with the IS Service Desk who may be able to help with blocking it. Unwanted mail or spam often results from registering for services using a particular email address. For this reason you should never use your States email account to register for personal services.

### 4.3. Phishing Attacks

Phishing is the term for fraudulent messages that trick their recipients into performing some action that either costs money or compromises the system. The sender will often forge the email so that it appears to come from a bona fide source such as a bank, eBay, Amazon, DHL

etc. The recipient is then fooled or pressured into opening an attachment, clicking a link, calling a number, entering a password and so on. The tell-tale signs of a phishing email are:

- They are unexpected
- The message contains inaccurate or inconsistent data e.g. reference number in message differs to attachment, sender email is completely different to reply-to address
- The look and feel of the message differs to that of the true sender
- They do not normally address the recipient personally, although some sophisticated attacks will use open source information to construct highly convincing targeted phishing attacks.

Suspect phishing messages should be reported to the IS Service Desk.

### 4.4. Chain mail and virus hoaxes

Never forward chain mail, virus warnings or fraud alerts however genuine or well-meaning they may seem. Some of these messages may contain malicious content; others are designed to consume system resources by clogging up the mail system. If in doubt forward the message to the IS Service Desk who will verify the message before issuing any advisory.

## 5. Managing your Email

Managing an email mailbox effectively can appear to be a difficult task, especially if the volume of email messages received is regularly of a large quantity. Here are a few approaches that might aid the management of email messages:

- Allocate sufficient time each day/week to read through and action/transfer email messages
- Look at the sender and title to gauge the importance of the message and then prioritise your email responses
- Flag where you have cc'd into email messages. These messages are often for informational purposes only and do not require immediate/any action.
- Setting rules for incoming messages so they can automatically be put into folders or highlighted in different colours
- Using folders to group email messages of a similar nature
- Deleting emails that are kept elsewhere as records

### 5.1. Requests to access another mail box

Sometimes it is necessary to gain view-only access to another person's mailbox. The reasons include:

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

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

- Gain authorisation from Head of Department
- Submit a request to the IS Service Desk
- Access to be gained in the presence of Line Manager

- A record is made of the reasons for accessing the mailbox and the names of the people who were present

The person whose mailbox was accessed is then normally informed.

### 5.2. Dealing with messages sent in error

If you send the wrong message to the wrong people there can be serious legal or reputational implications. You may simply need to explain your mistake to the recipients and reissue the message. In more serious cases a formal apology may be warranted, or a breach notification may need to be made to the Data Commissioner. In stressful situations like these the best course of action may be difficult decide on. Discuss the matter immediately with your line manager, or if it has a more public impact, discuss with the Communications team so that a carefully considered response can be agreed. Do not attempt to rely on Outlook's recall feature as this only works on internal mail that has not yet been opened.

## 6. Records Management

### 6.1. Introduction to managing email records

The main points to consider when managing email records are:

- Identification of information that is a business record
- Responsibility for capturing records
- What to capture
- When to capture records
- Where to capture records
- Retention
- Naming conventions

Each of these topics is covered in detail below.

### 6.2. When is email a "record"?

Emails often can constitute part of the formal record of a transaction. Under the Public Records (Jersey) Law 2002, a record is defined as information that is –

*created or received in the conduct of a corporate, institutional or individual activity; and has such content, context and structure as to provide evidence of the activity.*

Any communications that fall under this definition must be considered as records and captured accordingly, for example:

- Contractual negotiations
- Tender processes
- Board meetings
- Recruitment and performance assessment
- Interactions with customers

### 6.3. Transient messages

Not all messages are classed as official records. These messages are characterised by being of a temporary or transient nature, and lose all significance with time or after a related event has occurred, e.g.

- Communications made to arrange a meeting
- Covering notes where the link or attachment is the record and not the email

Typically transient messages are retained until the event occurs or the request is fulfilled. The retention period is subject-dependent.

### 6.4. How much data should be captured?

At the most basic level the message subject, content and contextual information such as sender, recipients, and timestamp must be captured. This often includes the conversation history; any correspondence that made a significant contribution to a business discussion should be captured and not just the final conclusions.

Ideally the entire message should be captured, as this will include metadata that may have evidential value. For example: IP address, domain name, system information, and digital signatures. Some of this information may be lost when saving, depending on what method is used to capture the information.

### 6.5. Responsibility

As communications can be sent to multiple recipients there are specific guidelines to indicate who is responsible for capturing them as records. Under normal circumstances these are:

- For internal messages, the sender of the message, or initiator of a dialogue that forms a string of messages
- For messages sent from the States to a third party, the sender
- For in-bound messages received by one person, the recipient
- For in-bound messages received by more than one person, the person responsible for the area of work relating to the message

### 6.6. What to Capture

Where a message has an attachment a decision needs to be made as to whether the message, the attachment or both should be kept as a record. It is likely that in most circumstances both should be captured, since the message will provide the context within which the attachment was used.

### 6.7. When to Capture Emails

Email messages that can be considered as records should be captured as soon as possible. However, many messages will form part of an on-going conversation thread. Where a thread has formed part of a discussion it is not necessary to capture each new part of the conversation individually. Instead, threads should be captured as records at significant points during the conversation.

### 6.8. Where to Capture Emails

Email messages that constitute records must be captured using one of the following methods (in order of preference):

- An electronic records management system (e.g. SharePoint or LiveLink)
- A CRM or case management system such as Nessie or Prescient
- Saved on shared drives in .msg format at the appropriate place in the organisational filing system
- Printed to paper and placed in the organisational filing system

The email system itself should not be used for the long-term storage of records. This is because records stored in mailboxes (or PST files) are generally only accessible to their owner, and therefore not easily searchable. This could be a problem in the event of a legal discovery order or a Freedom of Information request.

### 6.9. Retention of Emails

Email records that have been transferred to paper or electronic filing systems should be retained in line with the retention policies in place for that set of records/files. There is no set general maximum retention period for the contents of emails – the length of retention depends on the content.

However, the email system is supported by a forensic email archiving system. This system is primarily to support dispute resolution and legal discovery, and stores all in- and outbound messages (except spam) for up to two years. Messages in the archive may only be accessed under exceptional circumstances, and therefore the system must not be relied on for day to day record keeping purposes.

### 6.10. Managing Shared Mailboxes

Any shared resources must be assigned an owner. The owner is responsible for documenting and communicating:

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

### 6.11. Naming Conventions

When saving an email care needs to be taken to preserve its metadata. Where possible follow the same convention as for other electronic records. This should be detailed enough for someone else to determine the relevance of the content themselves without necessarily opening the document. Examples include:

- Remove any re: or fw: prefixes
- Use the full name of the organisation or department
- If possible refer to a person's role rather than their name
- Date of message
- Subject or project

## 7. Exemptions

In rare circumstances policy exemption may be requested. This is done through a formal approval process via the Service Desk. Requestors will be expected to make a business case for the exemption, and demonstrate that appropriate compensating controls have been established.

## 8. Further Assistance

For assistance sending or receiving email please call the ISD Service Desk on 440440.

## 9. Related Documents

IS-POL-001 Acceptable Use Policy

IS-POL-002 Information Classification Policy

IS-POL-017 Email Records Management Policy

END