

Email and Text messages

Table of Contents

Table of Contents	2
Email	3
Maintaining your email account and managing absences	3
Outbound external email	4
SEEMail	6
Retention and recovery of emails	7
Inappropriate or unsolicited emails	8
Text messages	9

Email

Email messages are evidential records, equivalent to hard copy business communications. Messages that contain a business decision and/or business transaction should be attached to the applicable operational or administrative file or otherwise retained as part of the record.

Email messages generated, sent or stored on the Police enterprise system are not private: they are public records under the Public Records Act and are the property of Police. They may be subject to scrutiny by supervisors, investigators, auditors and system administrators.

Maintaining your email account and managing absences



Maintain your account and manage absences by following these guidelines:


- Perform regular maintenance of your account, including moving key messages to the applicable system of record and deleting messages as required.
- Arrange alternatives for the management of your account when you will be absent from duty, such as using 'Out of Office' messages.
- 'Auto-forward' should be avoided. If it is necessary, use it with care to ensure that sensitive information is not forwarded. It must never be used to automatically forward Police emails outside the Police environment.
- Provide your manager with any relevant information from your email account when you are planning to be absent from duty or leaving Police.

Outbound external email

You should exercise care when sending email externally as the path or destination may not be secure. Sending emails to the wrong recipient is an unfortunately common problem. It is embarrassing at the least, but it can cause much more significant downstream problems if the content includes private or operationally sensitive information. Sending emails to non-Police addresses also increases the risk of them being intercepted or received by a third party.

Follow these steps.

<p>1. Add [SEEMail] to your signature block to avoid accidentally sending messages outside government</p>	<p>Add the term [SEEMail] (including the square brackets) as a new line in your default signature block. Any outgoing email containing the [SEEMail] string will be blocked from going to any addresses outside the SEEMail community of government agencies, e.g.,</p>  <p>For any messages that do need to go to recipients outside government, either delete the [SEEMail] line or create an alternative signature that doesn't include the [SEEMail] tag.</p> <p>To set your signature:</p> <ul style="list-style-type: none">- Outlook: Go to File -> Options -> Mail -> Signatures.- iPhone: Go to Settings -> Mail -> Signature.
<p>2. Use classification markings.</p>	<p>Add the highest classification of the message and its attachments (e.g. IN CONFIDENCE) to the subject line or the top of the message body so recipients know the protection needed. E.g.</p>  <p>Note that classification labels do not alter how the mail system processes the message. They are aimed at the human recipient.</p> <p>In some situations, you may also want to add an endorsement marking to limit distribution e.g. 'IN CONFIDENCE Police Use Only'.</p> <p>The classifications and endorsement labels Police use are described here.</p>

<p>3. Check all of the content of email messages and attachments before your send or forward.</p>	<p>Do all recipients need to get any included attachments?</p> <p>Should any of the contents or metadata be redacted before they are safe to send? Are Tracked Changes left in an attached document?</p> <p>Remember that your email, and any email chain below it, could be forwarded on indefinitely, so remove any content that isn't needed.</p>
<p>4. Apply SELF CHECK to your email communications.</p>	<p>It can be useful to pause before you hit send. Consider the Code of Conduct, SELF CHECK and Our Values. It is easy to send something you think is witty or insightful and regret it later. Don't send an email when you are angry. Be aware that all emails are discoverable under OIA request.</p>
<p>5. Password-protect sensitive attachments.</p>	<p>Use the password feature in Word, Excel 6(c) OIA to ensure an unintended recipient can't open those attachments. Get the password to the intended recipient via another channel such as by txt message.</p>
<p>6. Take care when sending or replying to distribution lists and shared mailboxes.</p>	<p>The full list of recipients might not be the same as the name of the mailbox or list suggests. Some distribution lists could have a mixture of NZP and external recipients. If in doubt, just send it to named individuals.</p>
<p>7. Take care with the address autocomplete function.</p>	<p>It is dangerously easy to send an email to the wrong person or the right person's wrong email address through inattention when using the address autocomplete feature. Double check the recipient(s) before you hit send, but these two tips can also help:</p> <ul style="list-style-type: none"> - iPhones have an optional feature to display in red any email recipient addresses that are outside NZP. Go to settings -> Mail -> Mark Addresses, and add '@police.govt.nz' plus any other domains that you want to consider as internal. - You can remove any addresses you don't want in MS Outlook's auto-complete list by clicking on the cross: 
<p>8. Add delivery delay</p>	<p>Consider adding a short delay before email messages in your outbox are sent, to provide an opportunity to cancel it if you immediately realise some aspects of the message are incorrect or inappropriate. In Manage Rules and Alerts, create a new rule ...</p> <p>Rule description (click an underlined value to edit):</p> <p>Apply this rule after I send the message defer delivery by <u>2</u> minutes</p>
<p>9. Know how to use Outlook's 'recall' function, but don't assume it will work.</p>	<p>In MS Outlook, open the message to be recalled. Go to its Message tab -> Actions -> Recall this message.</p> <p>Note that the recall function will only work on messages sent to other addresses in the same domain (e.g., another@police.govt.nz address), and only if the recipient hasn't opened the message. They will get an email to say you attempted to recall the message.</p>
<p>10. Don't auto-forward messages outside Police.</p>	<p>NZP email accounts must not be set up to auto-forward messages to an external account due to the risk of leaking sensitive personal or official information into the public domain.</p>

SEEMail

Secure Electronic Environment Mail (SEEMail) is an established NZ Government secure email system that uses server-based encryption between participating Government agencies.

-

 SEEMail agencies - August 2020

388.08 KB

It provides:

- protection for your message travelling over the Internet, by encrypting your message and only sending it to recipients within SEEMail-enabled agencies
- an assurance that a message came from a specific SEEMail enabled agency, preventing an outsider from sending fake messages appearing to come from a government agency or employee
- an assurance that messages will not be automatically forwarded out of a receiving SEEMail enabled agency to a non-SEEMail destination (e.g., by an out-of-office auto-forward rule).

If you want a message only to be sent via SEEMail - to confirm if it will only be sent if it can be delivered securely - place the text '[SEEMAIL]' in the subject line or at the beginning or end of the message before you send it.

Retention and recovery of emails

All emails - business and personal - sent to and from Police servers are retained in the journal archive for investigative purposes. This includes deleted emails. These emails are stored in a separate database from the production email boxes used by individuals in Microsoft Outlook.

The email archive is not a records management system, so each email user is responsible for retaining and filing email to meet Police obligations under the Public Records Act.

The production email database stores the email that users access with MS Outlook for 15-months. Any user can access email in their folder structure without needing to access and search the email archive. Email older than 15 months is purged from the production environment and a copy kept in the email archive, where it is kept for a minimum of 10-years before being destroyed.

The production email database is backed up weekly and stored for three-weeks before being overwritten. These back-ups can be used for disaster recovery purposes and to restore Microsoft Outlook email folder structures only. You can restore individual emails older than 15-months yourself using the email archive system. When a staff member leaves Police, their email files will be removed from the email production system but the messages will be retained in the archive system.

Inappropriate or unsolicited emails

Handling an email message containing material of a sexual or otherwise offensive or inappropriate nature could be a breach of the Code of Conduct. If someone sends you an email with such content, from an internal or external source, and you can identify the sender, then:

- If the material is necessary for Police work (e.g., part of a case you are involved in), manage it as for other intelligence or case material and only store or share it with others as absolutely necessary; or
- If the material is frivolous, or it is only a trivial breach of policy, delete the email and contact the sender to request they don't do it again. Don't include the original content in a Reply to advise the sender, or you might also be guilty; open a new email or let the sender know in person or by phone;

Otherwise, if the message contains objectionable material, or if it is otherwise a serious misuse, close or minimise the screen immediately and advise your manager. Note the sender and the date and time. Do not delete, print or forward such material unless you are requested to as part of the incident management process.

If you receive an unsolicited email, do not reply, as sending a response could generate more unwanted mail. Forward the email to **6(c) OIA** for follow-up.

Text messages

Text messaging and/or similar Internet or peer-to-peer communications services must not be used for communicating sensitive information.

Some text messages and telephone calls fall within the OIA and Public Records Act because they document business activities and decision-making. You need to save these into Police operational or business systems. Most work-related messages and conversations will only be of short-term value so will not need to be kept. For example, a text setting up a meeting, or a text where a separate more formal record is made. Decide whether they should be kept by:

- take a risk-based approach. Will you need to refer to it again? Will you need to produce it?
- apply the [SELF CHECK](#) to your material (Scrutiny; Ethical; Lawful; Fair).
- If Police does not have a method of capturing the message into an operational or business system, take a screenshot or capture a file note then transfer the copy to a Police system of record e.g. NIA
- ensure you record who sent the message, when it was sent (date and time) and what it was about

Personal text messages sent or received on a Police device do not need to be kept.
