Fact Sheet March 2026

Tips for reducing data breaches when sending emails

Who is this information for?

NSW public sector agencies and staff

Why is this information important?

This fact sheet will assist agencies to understand some of the options available to minimise the risk of inadvertent disclosure when using emails to communicate.

Email is a convenient means of communication, and it is no surprise that the vast majority of agencies rely on the use of email as an integral part of their operations. However, a significant proportion of data breaches are caused by accidental human error when using email.

Some common types of data breaches arising from the use of email include:

- emails being sent to the wrong recipient
- personally identifiable information being revealed in the 'To' or 'CC' fields of an email
- attachments containing personal information of individuals being incorrectly included in an email.

Many of these data breaches can easily be minimised using simple measures. The following tips are general in nature, and you should check whether your agency has its own email policies that may apply.

Disabling the auto-populate function in your email program

A common function available in many email programs is the auto-populate function for email recipients. This function displays a list of recipients that you have previously emailed based on the letters you type in the 'To', 'CC' and 'BCC' fields.

Using the auto-populate function can save you time by allowing you to select the recipient without the need to type out the whole email address. However, there is potential for your email to be sent to the wrong recipient, particularly where another individual has a similar email or name to the intended recipient.

To reduce the risk of these errors occurring, consider disabling the auto-populate function in your email program. If this is not possible, you should double-check the email recipients before sending, or type in the recipient's name in full.

Double checking email recipients

While it may appear simple and obvious, the main way to prevent data breaches when using email is to be careful and pay attention.

You can check the email addresses of recipients of an email by double clicking on the recipient's name as displayed in the 'To', 'CC' and 'BCC' fields before sending the email, which causes the recipient's full email address to be visible.

This will reduce the chances of sending an email to a recipient with the same or similar name.

Setting a delay rule

There may be instances where you realise that you have made an error in your email shortly after sending.

Many email programs allow you to create a rule to delay the delivery of all emails for between two and five minutes after you have clicked 'send'. The email will be held in the 'Outbox' for the specified time after you have clicked 'send'. This would allow you to go into the 'Outbox' to review, confirm, change or delete the email before it is received by the recipient.

This can be a much more effective strategy than trying to use the 'recall' function after you have already sent the email to the wrong recipient, which usually does not actually remove the email from the recipient's inbox after it has been received.

Being mindful when forwarding email chains

It is not uncommon for email chains containing multiple conversations to be forwarded as part of a communication. In doing so, there is a risk of privacy breaches occurring, whereby more information than is necessary is disclosed to the recipient.

For example, an email chain may contain personal information about an individual which is incidental to the message.

If this email is forwarded to another unrelated individual, this could be an unlawful disclosure of personal information under the *Privacy and Personal Information Protection Act 1998 (NSW)* (PPIP Act).

If an email thread is too long or contains information that the recipient does not need to know, consider alternatives.

This could be drafting a new email, manually deleting the email thread, or checking whether your agency's email program settings allow you to automatically exclude email threads when replying to, or forwarding, emails. Depending on the approach taken, agencies should ensure that their practices are consistent with its own policies, procedures and record-keeping requirements.

Sending attachments with emails

When you are sending an email and need to include additional information like an attachment, you should always consider whether the attachment can be sent using a secure platform sharing link or can be password protected. Follow any internal agency policies in place for email attachments and always review the attachment and confirm that it is intended for the email recipient. You could consider whether it is possible to have a prompt set up to check that the email is correct before sending the email.

Email management

To minimise risks of malicious access to personal information contained in emails that no longer serve a purpose, it is important to regularly empty your 'sent' and 'deleted items' folder. You should also be mindful of not using your email program for storage of emails containing personal information. Emails should be transferred to a separate records management system and then deleted from all mailboxes, consistent with any established policies, procedures and record-keeping requirements for your agency.

Being mindful when sending group emails

Where an email is sent to several recipients and you do not want each recipient's email address to be visible to all other recipients, you should insert the recipients' email addresses into the 'BCC' field, rather than the 'To' or 'CC' fields.

This is particularly important where the recipients are not known to each other, such as in the case of mailing lists or other group communications where it is unclear whether individuals have consented to the sharing of their email addresses. Although the accidental disclosure of recipients' email addresses may sound trivial, under the PPIP Act, this could be considered to be an unlawful disclosure of personal information. An email address will often consist of a person's name.

If you frequently send group emails, you may wish to consider putting certain processes in place, such as the use of distribution list management programs, checklists and policies that indicate when to use the 'BCC' and 'CC' fields and asking a colleague to review the email to confirm that everything looks correct before clicking 'send'.

If you do use a distribution list, make sure to review it regularly for accuracy and currency and that it only contains recipients who require the information.

You can also consider creating an email rule to prompt the sender where the number of recipients in the 'To' or 'CC' fields exceed a minimum number set. This will serve as an additional safeguard, as it allows the sender to confirm that there are no issues in allowing the email addresses to be visible to the recipients. Alternatively, where the email addresses should not be visible to the recipients, the prompt could serve as a reminder to use the 'BCC' field instead.

When sending an email that uses both CC and BCC, it can be helpful to send it from a "Do Not Reply" address. This prevents unintended replies — especially "Reply All" — from exposing information to the sender or to anyone copied on the email. If recipients need to respond, directing them to a separate, designated email address reduces the risk of inadvertent disclosure.

Setting up email prompts

You may also consider whether it is appropriate to set up other email prompts, which would detect potential errors while you are composing an email.

The prompt will tell you what the potential error is and provide an opportunity to fix the error before sending the email.

Some examples of email prompts include:

- if an email is being sent to an external recipient outside your organisation, a prompt could advise that it is an external recipient
- if an email contains an attachment, a prompt could suggest that the sender check that the correct attachment is attached.

Other useful resources

Other resources that may be useful on this topic include:

- Guide to managing data breaches in accordance with the PPIP Act
- Guideline – Guidelines on the assessment of data breaches under Part 6A of the PPIP Act
- Fact Sheet – Understanding your obligations - public sector staff

- Fact Sheet – NSW public sector agencies and data breaches involving tax file numbers

** The IPC acknowledges and thanks the office of the Victorian Information Commissioner in the production of this resource.*

For more information

Contact the Information and Privacy Commission NSW (IPC):

Freecall: 1800 472 679
Email: ipcinfo@ipc.nsw.gov.au
Website: www.ipc.nsw.gov.au

NOTE: The information in this Fact Sheet is to be used as a guide only. Legal advice should be sought in relation to individual circumstances.