

9 Tips for ATIP-Friendly Email Management from the Office of the Information Commissioner



Information
Commissioner
of Canada

Commissaire
à l'information
du Canada

Over the years, through the investigation of ATIP related complaints, the OIC has noted that most requests for information made under the *Access to Information Act* (the Act), include information that was only ever recorded by a federal public service employee in an email. Increasingly, email is used by employees to document business decisions. In addition, email is used to share copies of reports and other records created for business purposes.

The following best practices for email management will ensure that you, as a federal public service employee, are able to respond to access requests made under the Act within legislated time frames while limiting efforts involved to produce records and ultimately respond to our investigations, if applicable. These tips should also help reduce the number of pages that will need to be processed in response to an access request by limiting duplications and/or removing personal or unrelated information.

1 The complete story

It is critical to retain emails that are records of business value to ensure that the institution's response to an access request provides the complete story. Keep in mind that keyword searches of email inboxes may not return some information in encrypted emails. The *guideline on searching encrypted emails in response to information requests* should be consulted to ensure that all responsive records are captured in the response to a request.

2 Store email in the correct repository

Emails of business value must be stored in your institution's designated corporate repository for storing information of business value, which may be an Electronic Document and Records Management System (EDRMS), such as GCdocs. File your email regularly (at least once a month). Emails of business value should be deleted once saved in the corporate repository.

3 Delete transitory emails regularly

Transitory email messages should be deleted regularly. Transitory emails cannot be deleted after an access request has been made under the Act. When deleting emails, remember to empty the Deleted Items Folder.

4 Keep personal messages separate

Avoid having personal email messages captured as part of an access to information request by ensuring they are kept separate from email messages of business value.

5 One email string = one subject

Resist the urge to request an update from your colleague on an unrelated project or file within an email string that is already started.

6 Use descriptive subject lines

Include a subject line that appropriately describes the contents of the email or the file number. This narrows the search for emails to associated records, whether electronic or paper.

7 Limit duplication

There is no need for every employee who receives an important email to save it in the records management system. The sender of the email is usually responsible for saving the message in the designated corporate repository.

8 Training and education are essential

Attend training on your institution's records management policies and procedures and ensure you understand where emails of business value are to be saved.

9 Send links instead of attachments

Whenever possible, provide links to where documents reside in the designated corporate repository instead of attaching copies of the documents to emails. Not only does this take up less space on your corporate network, enabling it to run more smoothly, it also helps ensure complete responses to access to information requests through efficient version control.