{wcb Workers'
      Compensation
      Board – Alberta

Knowledge Guide

Using and Managing Email

The Workers' Compensation Board– Alberta (WCB) is subject to Alberta's *Freedom of Information and Protection of Privacy Act* (FOIP), which governs the way personal information is collected, used, disclosed, retained and destroyed. This document is designed to help you ensure that as a WCB employee, your email practices comply with FOIP, as well as with WCB's records management requirements.

Disclosure of Email

Under FOIP, anyone can request access to records of the WCB, including emails. There are limited exceptions to disclosure when the WCB must refuse to or may decide not to disclose records in response to a FOIP request.

> Keeping your personal and work-related email separate will ensure that personal emails don't get inadvertently drawn into a records search or FOIP request.

Email is a Record

Whenever an email message is sent in the course of WCB business, that email becomes an official record of the WCB. Such records can be subject to disclosure in response to a FOIP request under FOIP or subject to subpoena by the courts. So, it is important that you take care when sending emails for a business purpose.

Use Your WCB Email Account

In today's world, we all have multiple email accounts. Some are personal (such as a Gmail account), and some will be institutional (such as your WCB employee account). Always use your WCB employee email account for WCB business. If you use a non-WCB employee account to create, respond to, or store work-related information you are increasing the risk of causing an inadvertent privacy breach by using a non-authorized service provider. In addition, those emails are still subject to FOIP so you run the risk that your own personal emails will be drawn into an access to information request. For these reasons, it is imperative that you keep your personal and work-related correspondence separate.

Do	Do Not
Use your WCB employee email account for work-related correspondence.	Forward your WCB business-related emails to a personal email account (such as Gmail)
Use your personal email account for personal correspondence.	Use the alias function in a personal email account to compose messages so that they look like they are coming from your WCB address but are really created, sent, and stored using your personal account

Create Email Records with Access in Mind

Because the public (including the media) has the right to request access to the emails that you create in the course of your job, it is important that all work-related emails be composed in a professional tone, and with the basic assumption that they might be made public under a FOIP request.

Consider whether a record is necessary

Use email when you need a record of the communication. Use the phone for preliminary discussions, or when a record is not strictly necessary.

When you need a record	When you may not need a record
To officially confirm something previously discussed.	Preliminary discussions before an official decision is made.
To demonstrate due diligence.	Discussions involving opinions about others, unless an official record of those opinions is necessary.

Create professional records

Don't put anything in an email that you would be embarrassed to see on the front page of the newspaper.

Always	Avoid
Use a professional and neutral tone.	Editorializing by including unnecessary personal remarks.
Clearly distinguish between opinion and fact.	Including personal information directly in the body of your email (unless your department's procedures state otherwise).
Include only as much information as needs to be officially recorded.	Mixing personal and WCB business in a single email.
Include a clear subject line and limit messages to one topic.	Using the "Reply All" function.
Copy only those who need to know.	

Protect Personal and Confidential Information

There may be times when you may need to transmit sensitive and confidential information, including personal information. With email, there is always a risk that messages will be accidentally forwarded to an unauthorized individual or opened and saved on a mobile device that is later lost or stolen. Personal information that is lost, stolen, or disclosed to an unauthorized individual constitutes a privacy breach under FOIP.

> A privacy breach occurs when someone's personal information is disclosed to an unauthorized individual, either on purpose or by accident.

When you need to transmit personal information ask yourself first whether there is another, more secure way, to deliver the information than by email.

If you must use email to communicate personal or confidential information:

- Remove as much personal information as possible.
- Consider putting the information in an attachment and encrypting it (Adobe Acrobat Pro and Microsoft Office applications both have options to protect and encrypt files).
- Ensure a confidentiality statement is at the bottom of your email.

- Verify the email addresses of all recipients.

Keep and File Email Records Appropriately

Retain messages that are sent and received only if they relate to WCB business, all other messages can be treated as transitory and deleted (see Knowledge Guide on Transitory Records).

- When retaining a series of replies or forwards, keep only the last message as long as the thread is complete and hasn't been changed in the course of the exchange.

- Make sure to retain information in the header regarding the sender, recipients, date and time; this helps preserve the context of the message.

- The email system is not a recordkeeping system. A recordkeeping system organizes records according to a file plan, provides shared access to those who need it, and applies retention and disposition rules. Here are some options for filing email messages:

  o If you have an electronic recordkeeping system, file email (and attachments) in that system. For example, if the email is claim related, it needs to be tagged to the appropriate claim file and deleted from the mail system.

  o If you have a paper-based recordkeeping system, periodically print and file the email (and attachments) and then delete them from the email system.

  o As a temporary measure before filing in a proper recordkeeping system, create folders within the email system that reflect your department's file plan. Move email to these folders every day.

  o Save/print emails and attachments as an Adobe PDF and file in your department's shared drive or designated records repository, then delete them from the email system.

> If a file becomes the subject of a FOIP request or a legal hold, all emails associated with that file must be retained until the request is completed or the legal hold has been lifted.