

Quick Reference Guide

How to Apply Sensitivity Labels to Emails

****IMPORTANT****

Difference between records management and Information Protection Sensitivity Labels Classification.

Information Protection Sensitivity Labels Classification is applied based on the sensitivity of the contents of a document or an email. These labels provide the ability to apply security controls based on classification labels. Records Management Classifications are applied based on the function of the record. Records Management Classifications come from an approved Administrative Records Management System (ARMS) or Operational Records System (ORS) which provide a retention and disposal classification to the record and are a requirement for SaskBuilds and Procurement (SBP) to be compliant according to legislation.

Why Use Sensitivity Labels? To Classify & Protect Organization Data.

Collaborating with people is important for business and this includes sharing data with contacts inside and outside our organization. When information roams, the chances for a security breach or content reaching unwanted or unauthorized people increases.

Sensitivity labels make it easy to identify the information classification level of emails, or documents, and protect the content with controls (permissions) that define how information is presented and what authorized users can do with the content.

The main purpose of sensitivity labels is to let people share and collaborate on classified files while ensuring proper security measures, such as encryption, are in place.

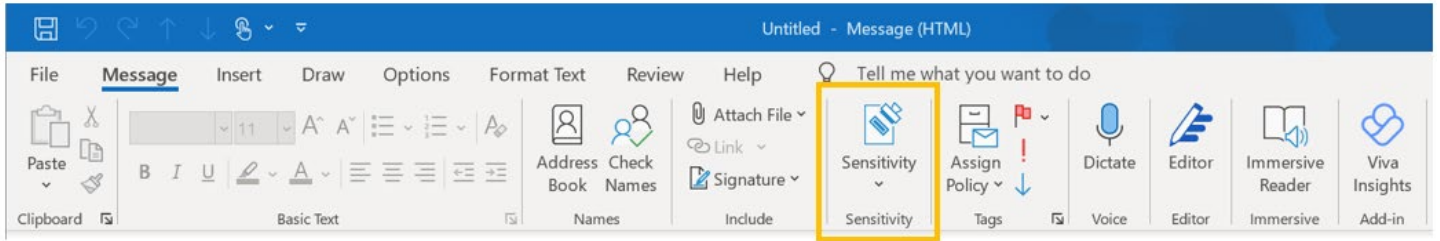
QUICK REFERENCE GUIDE CONTENTS

How to apply sensitivity labels to your email.....	1
How to edit or remove a sensitivity label on your email before sending.....	5
How to use a One-time passcode, as a recipient.....	5
What to expect with sensitivity labels.....	8
Support.....	8

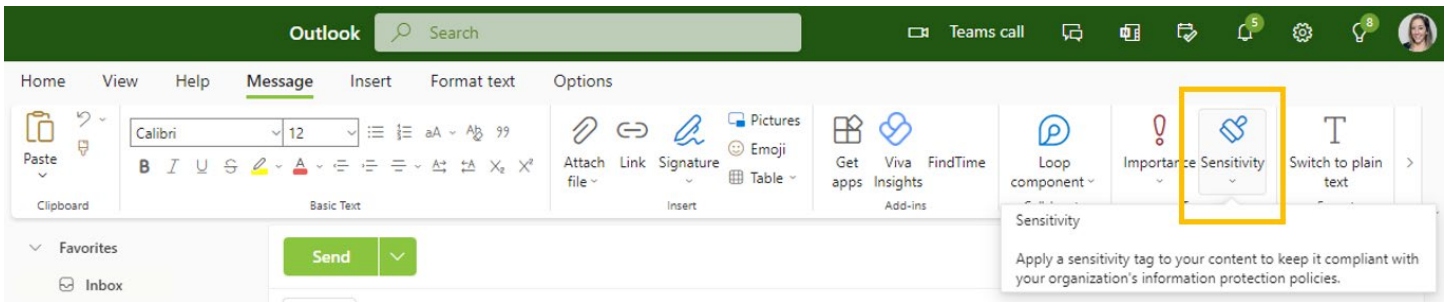
HOW TO APPLY SENSITIVITY LABELS TO YOUR EMAIL

1) Start a 'New Email'. Click the **Sensitivity** labels button, found within the 'Message' ribbon of Outlook.

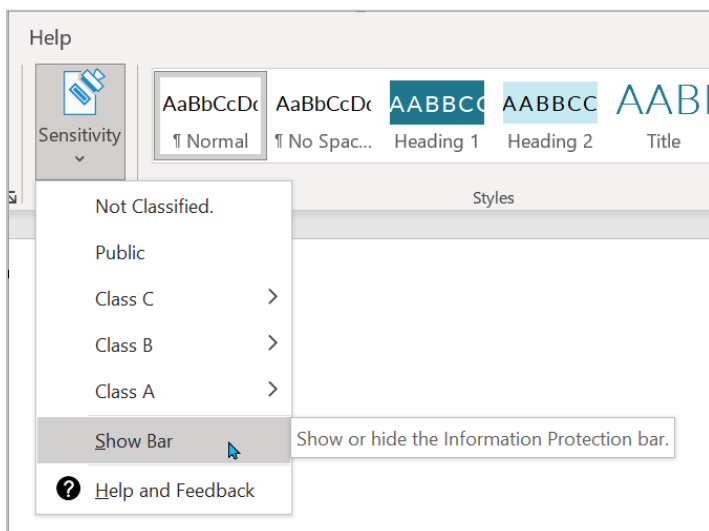
Outlook Desktop: Sensitivity Labels Button



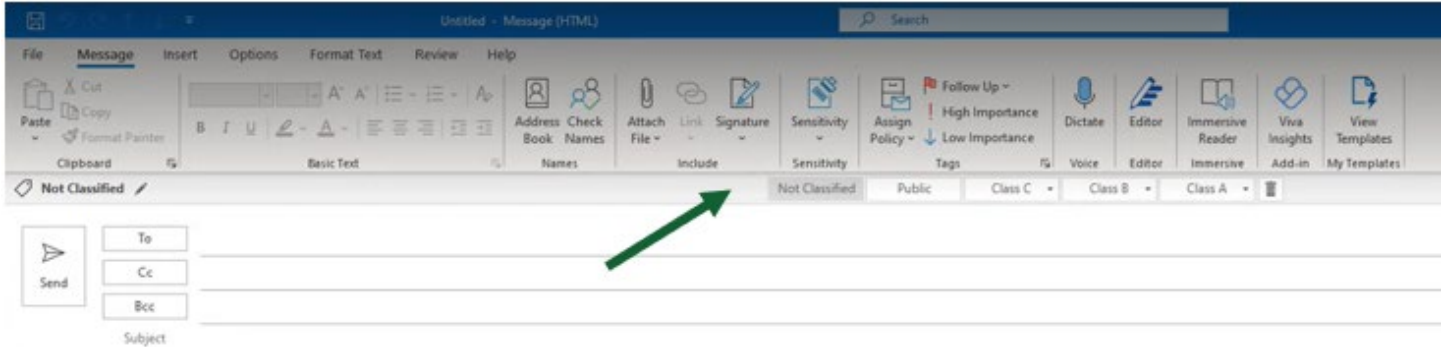
Outlook Online: Sensitivity Labels Button



2) Click the Sensitivity labels button, select **Show Bar** to have the Information Protection Toolbar appear permanently below the menu ribbon in the Outlook Desktop app.



Result: The Information Protection Toolbar in Outlook (Desktop app)



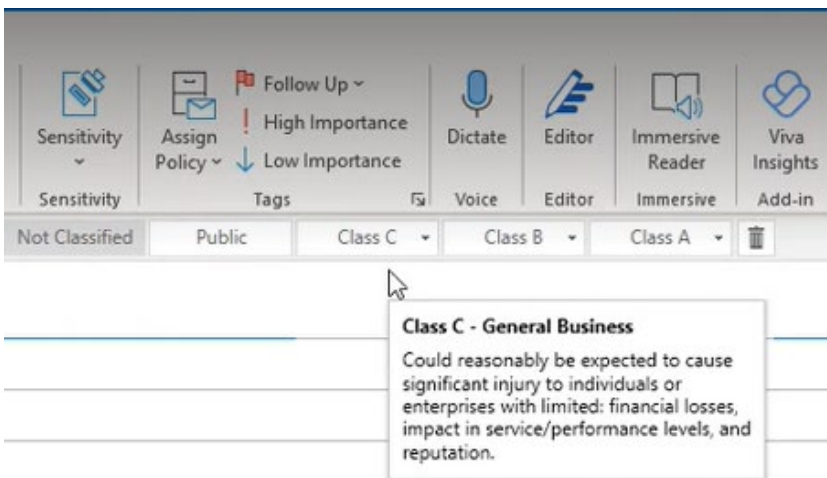
Note: A default label “Not Classified” is applied to all emails (and files). This means that the content has yet to be classified. Please consider using a Sensitivity Label to identify files according to “A Guide for Information Protection Classification.”

3) Select the label (the information classification level) that applies to the email content.

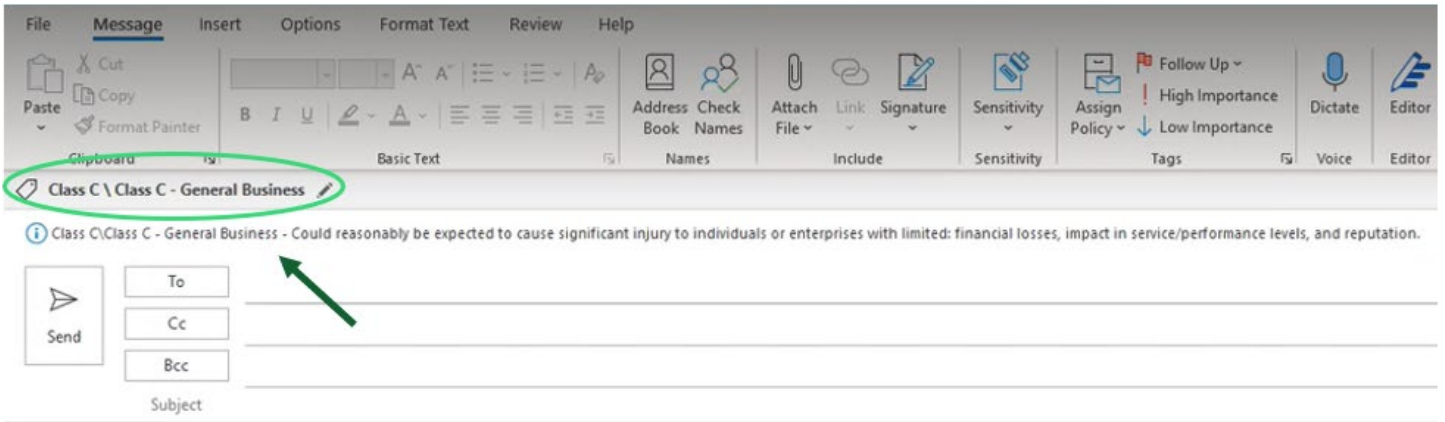
Choose between the labels within the information protection toolbar:

- Public
- Class C – General Business
- Class B – Confidential
- Class A – Restricted

Tip: Not sure what a label means? Hover over the label with your cursor to see the description assigned to it according to Government Information Protection (GIP).



4) Once a label is selected, the tag name in the Information Protection Toolbar changes accordingly and a description is shown above the “To” field.



When you apply a label, you are classifying and protecting the content with pre-determined security controls. Review the [Sensitivity Labels Classification Taxonomy](#) to understand what security measures come standard with each label.

Overview: Sensitivity Labels Classification Taxonomy for Emails

Sensitivity Label	Standard Protection / Permissions							
	Encrypted	Remove Encryption	Reply / Reply All	Forward	Copy & Extract	Print	Save Content	Send Externally
Class A Restricted	Yes	No	Yes	No	No	No	Yes Encrypted	Yes With Audit
Class B Confidential	Yes	No	Yes	No	No	No	Yes Encrypted	Yes With Audit
Class C General Business	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes
Public	No	N/A	Yes	Yes	Yes	Yes	Yes	Yes
Not Classified	No	N/A	Yes	Yes	Yes	Yes	Yes	Yes

Notes:

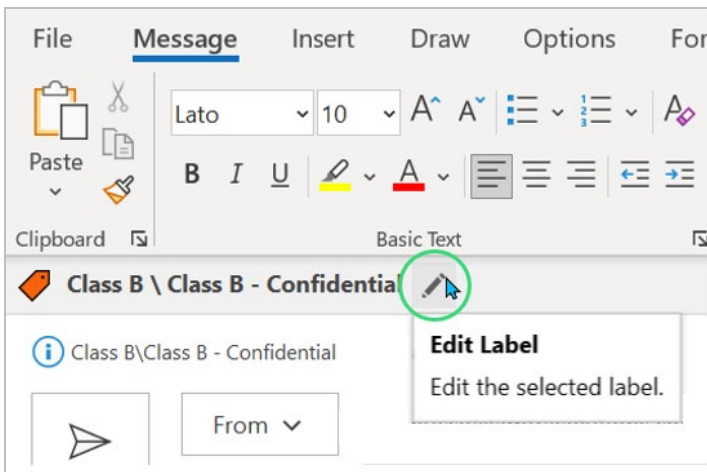
- Saving content is possible; however, for Class A and Class B, “Yes, Encrypted” means that the file is saved in an encrypted format. Only authorized people are provided with the ability to view encrypted content in a readable format.
- The ability to ‘Share Externally’ is set to ‘Yes – with Audit’. This means that an alert is sent to users when an email or attached document labelled as Class A or Class B leaves the organization. The

alert reminds the user that this action is against government Standards and Guidelines.

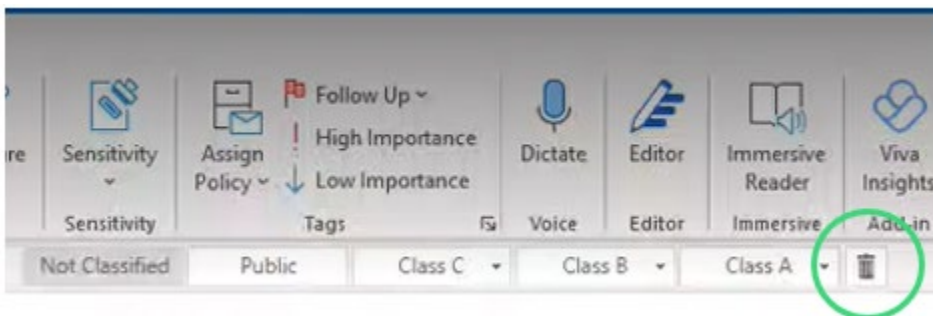
- Email and document labels are typically independent to one other. An email label will only add protection to an attachment if the document is not encrypted (i.e., labelled as Public or Not Classified).
- It is best practice that users do not screen share Class A or Class B emails and documents.

HOW TO EDIT OR REMOVE A SENSITIVITY LABEL ON AN EMAIL BEFORE SENDING

1) With the new email open, click the Edit pen icon within the Information Protection toolbar and select the appropriate label.



Tip: When the sensitivity labels are listed in the Information Protection Toolbar, a trashcan icon is present that allows you to delete the label you applied and return your email back to 'Not Classified'.



HOW TO USE A ONE-TIME PASSCODE, AS A RECIPIENT

If a recipient has a domain that is not recognized by Information Technology Division, for example a Gmail account, the recipient can gain access using a one-time passcode.

1) Follow the prompts as presented to access a protected message using a **One-time passcode**.

The image shows two side-by-side screenshots from an email client. The left screenshot shows an email from Janelle P (janpemail@gov.sk.ca) with a subject line 'Class A'. The email content indicates a protected message and includes a blue button labeled 'Read the message'. A yellow box with the text 'Opens a web page, Click **One-Time passcode** option.' has a yellow arrow pointing from the 'Read the message' button to the right screenshot. The right screenshot is titled 'Encrypted Message' and shows a notification from 'janpemail@gov.sk.ca' with a lock icon. It contains the text 'Sign in to view the message' and two buttons: 'Sign in with Google' and 'Sign in with a One-time passcode'. The 'Sign in with a One-time passcode' button is circled in green. Below these buttons are links for 'Need Help?' and 'Privacy Statement'.

We sent a one-time passcode to [redacted]@gmail.com.

Please check your email, enter the one-time passcode and click continue. The one-time passcode will expire in 15 minutes.


One-time passcode

This is a private computer. Keep me signed in for 12 hours.

→

Didn't receive the one-time passcode? Check your spam folder or [get another one-time passcode.](#)

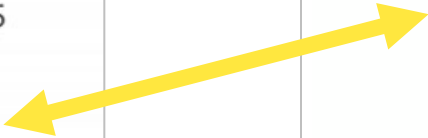
Your one-time passcode to view the message Inbox

 Microsoft Office 365 Message Encryption Nov 17
to me

Here is your one-time passcode
33631048 → Example

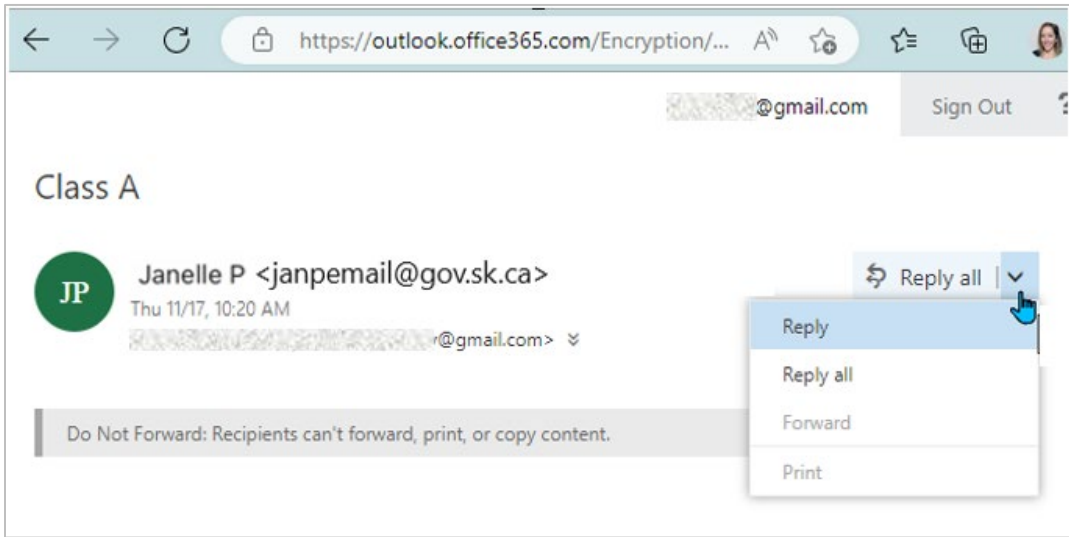
To view your message, enter the code in the web page where you requested it.





NOTE: This one-time passcode expires 15 minutes after it was requested.



Enter **One-Time passcode** (sent to inbox) into the passcode field on the web page, click continue.


2) View the email from a secure Microsoft web page



← → ↻ <https://outlook.office365.com/Encryption/...> A    

[redacted]@gmail.com Sign Out

Class A

 Janelle P <janpemail@gov.sk.ca>
Thu 11/17, 10:20 AM
[redacted]@gmail.com

Do Not Forward: Recipients can't forward, print, or copy content.

- ↻ Reply all
- Reply
- Reply all
- Forward
- Print

Note: The sensitivity label protection is noted in the email for easy awareness. In this example, of an email labeled Class A, the recipient is notified that they cannot forward, print or copy content. The only features available to them are to reply (all) to the sender(s). This complies with the [Sensitivity Labels Classification Taxonomy for Emails](#).

WHAT TO EXPECT WITH SENSITIVITY LABELS

Sensitivity Labels allow you to classify content with the appropriate information classification level and protect emails with a single click.

Key Take-Aways:

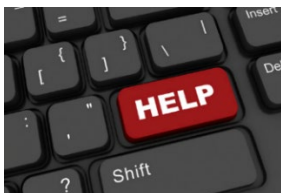
- All users and groups recognized by the Information Technology Division at the Government of Saskatchewan can see and use sensitivity labels.
- The default label "Not Classified" is applied to emails and documents, always consider classifying content appropriately (i.e., Public, Class C, Class B, or Class A).
- Recipients outside of the organization can access a protected message using a One-Time passcode.
- Email and document labels are independent of one other. Email and document labels operate independently. An email label will only add protection to an attachment if the document is not encrypted (i.e., labelled as Public or Not Classified).
- It is best practice to not mix sensitivity labels when emailing out – use one file type per email for simplicity.

It is important that all users understand what sensitivity labels can do and utilize them well. Further resources include:

- [Sensitivity Labels Classification Taxonomy Chart](#) for emails
- [A Guide for Information Protection Classification](#)

Know that the sensitivity labels at the Government of Saskatchewan have been well planned with great intention behind them and have undergone rigorous testing.

SUPPORT



IT Service Desk

For questions or issues, call the IT Service Desk.

Phone: 306-787-5000