

# Quick Reference Guide

## How to Apply Sensitivity Labels to Documents

---

**\*\*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 in 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 or Operational Records System, which provide a retention and disposal classification to the record and are a requirement for the Ministry of SaskBuilds and Procurement to be compliant according to legislation.

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

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

Sensitivity labels make it easy to identify the information classification level of documents or emails 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 documents while ensuring proper security measures, such as encryption, are in place.

---

#### QUICK REFERENCE GUIDE CONTENTS \_Toc119593022

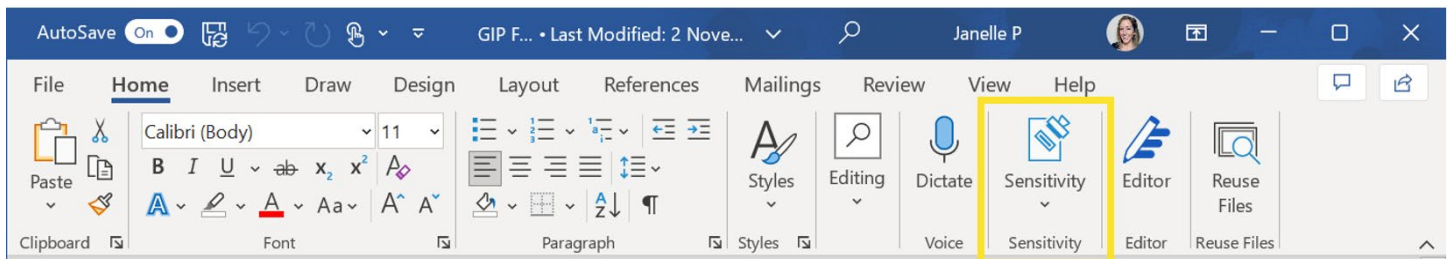
How to apply sensitivity labels to your documents .....	2
How to apply permissions to Class A & Class B documents (highly sensitive material) .....	5
How to change or audit permissions as a Class A or Class B 'Label Owner' .....	6
How to change a sensitivity label (justification required).....	8
What to expect with sensitivity labels.....	9
Support.....	10

## HOW TO APPLY SENSITIVITY LABELS TO YOUR DOCUMENTS

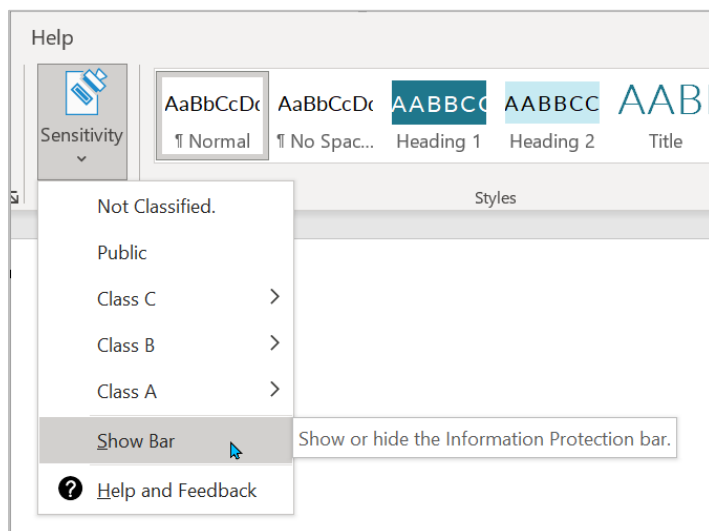
- 1) Use the **Sensitivity** labels button, found within the 'Home' ribbon of Word, Excel, and PowerPoint.



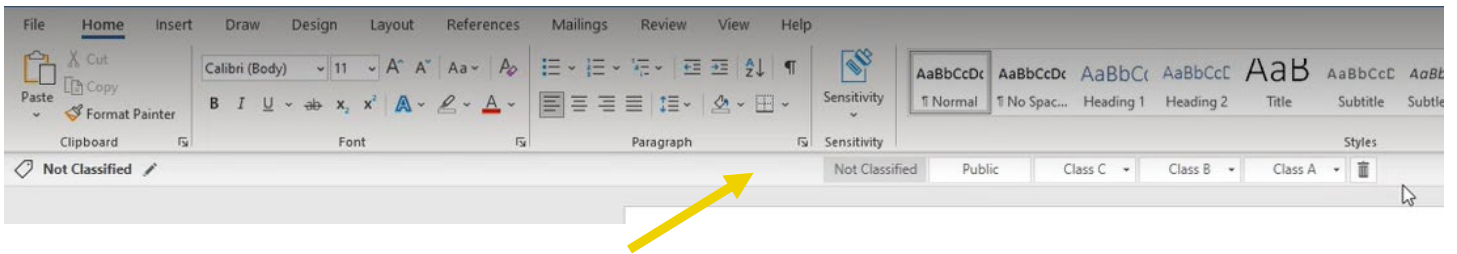
### Example: Sensitivity Labels Button in Word



- 2) Click the Sensitivity labels button, select **Show Bar** for the Information Protection toolbar to appear.



## Result: The Information Protection Toolbar



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

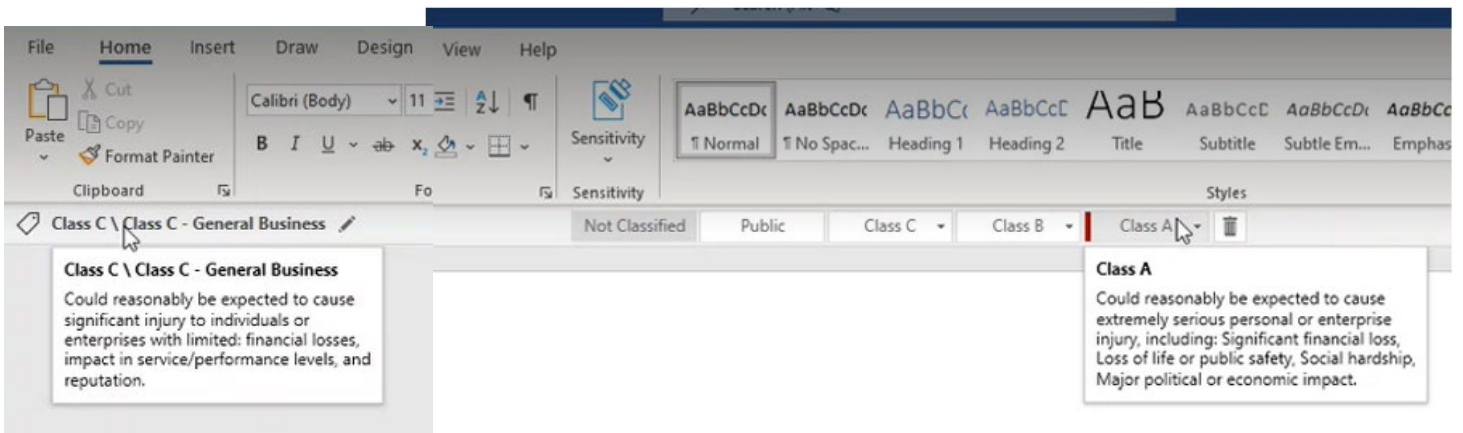
3) Select the label (the information classification level) that applies for the file.

Choose between the labels within the information protection toolbar:

- \* Public
- \* Class C – General Business
- \* Class B – Confidential
- \* Class A – Restricted
- \* Not Classified

Every document, by default, will have a label called not classified, which means the owner of the document has not officially classified the document based on its content. Not classified is not encrypted, and no restrictions are applied to the document.

**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.



**Note:** When you apply a label, you are classifying and protecting the content with pre-determined security controls. Review the **Sensitivity Labels Classification Taxonomy for Documents** to understand what security measures come standard with each label.

### Overview: Sensitivity Labels Classification Taxonomy for Documents

Sensitivity Label	Standard Protection / Permissions							
	Encrypted	Remove Encryption	Read - View only	Edit	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:

- \*When labelling a document (Word, Excel, or PowerPoint file) as Class A or Class B, a label owner can use permission controls to allow a recipient to edit, copy, or print content.
- 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.
- \*It is best practice that users do not screen share Class A or Class B emails and documents with unauthorized users.

#### 4) Save your labelled file

Ensure that the file has content within it (not blank, data is required) when applying a label, then name and save the file.

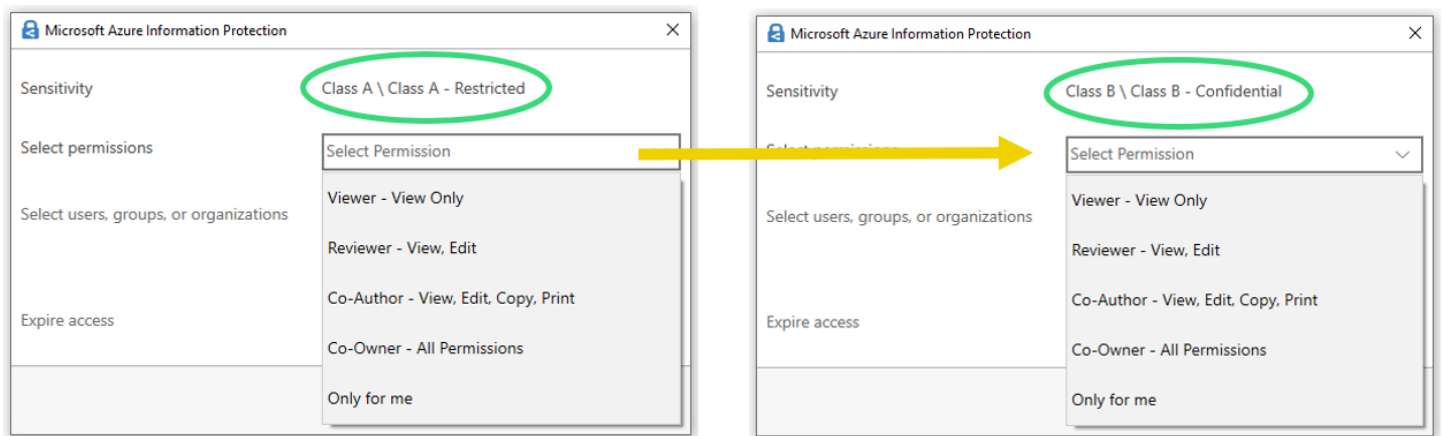
**Note:** The label on a file supersedes a sensitivity label that you might apply to an email. This means that if you label your email content as Class C but attach a file with a Class A label, the file is protected by the Class A settings.

## HOW TO APPLY PERMISSIONS TO CLASS A & CLASS B DOCUMENTS (HIGHLY SENSITIVE MATERIAL)

Class A & Class B documents contain highly sensitive and restricted information.

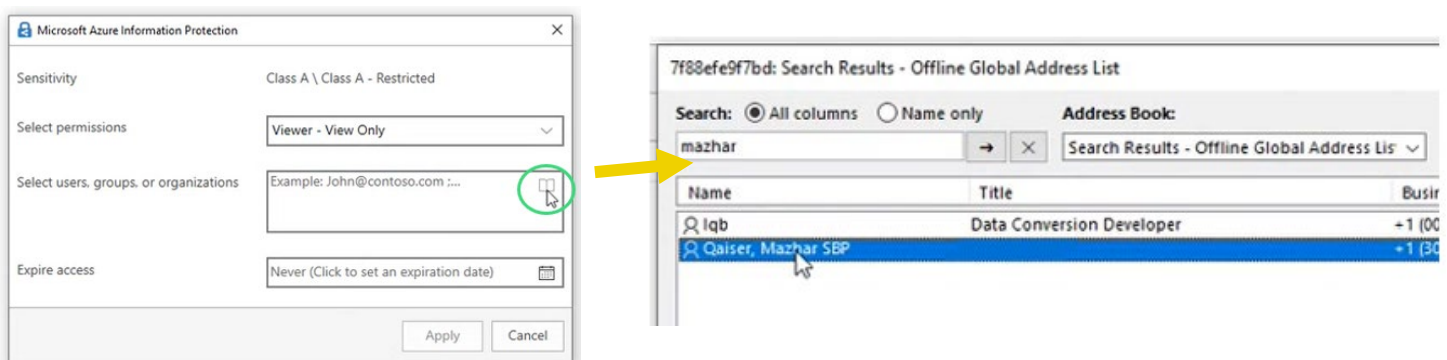
You can set access permissions accordingly and limit access capabilities to required individuals. This is completed using the Microsoft Azure Information Protection window that opens when you select a Class A or Class B label.

- 1) Click a Class A or Class B label from the Information Protection Toolbar and click 'Select permission' to expand options

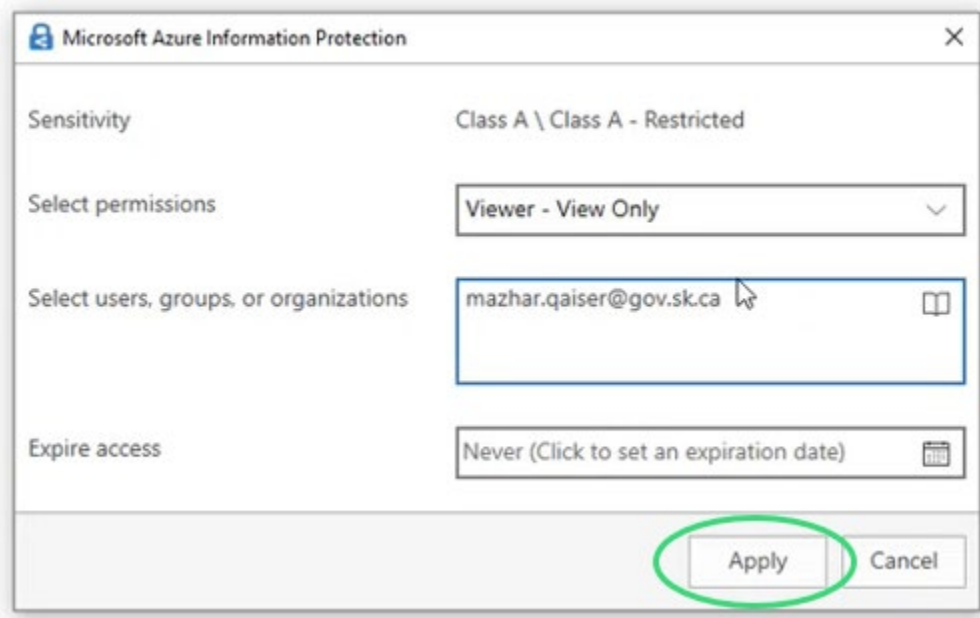


**Note:** The permission options within the dropdown for 'Select permission' are the same for Class A & Class B (as presented above).

- 2) Select required permission from the dropdown list and add a recipient to the 'Select users, groups, or organizations' field by clicking the directory icon



In this example, Mazhar now has 'View Only' permission for this Class A file. Click Apply to confirm.



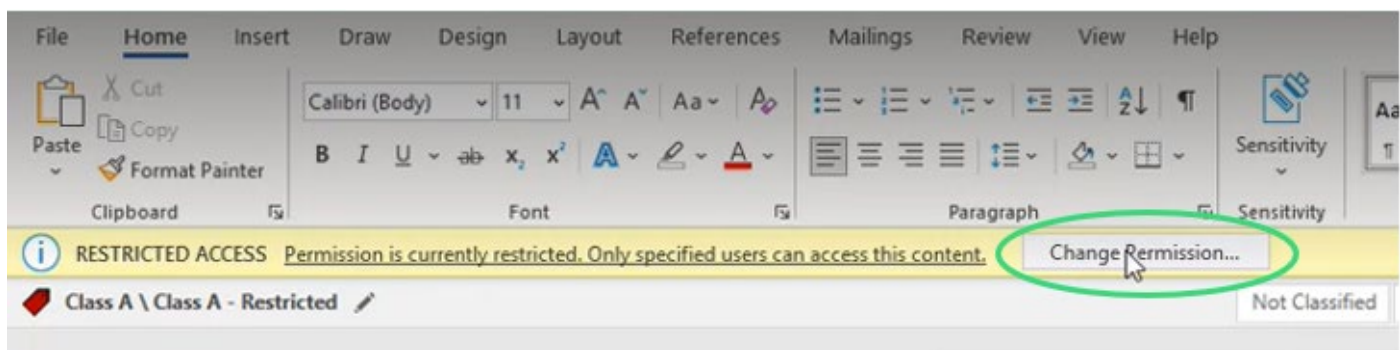
**Note:** There is no need to set an expiration date using the 'Expire access' field. Best practice is to leave this blank.

## HOW TO CHANGE OR AUDIT PERMISSIONS AS A CLASS A OR CLASS B 'LABEL OWNER'

When you label a file, you become the 'label owner'. Owners have full control over the label and content rights. An owner (or co-owner) can grant access and change the label with justification.

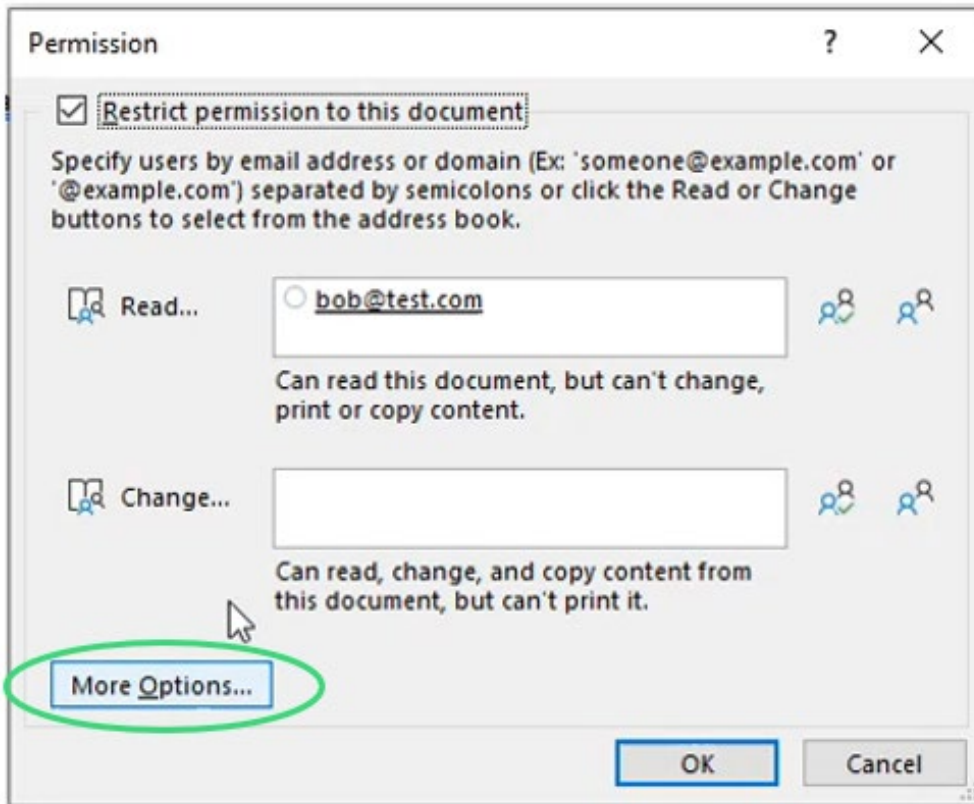
Owners can review permissions set for Class A and Class B documents to audit who has what level of access and to change permissions as necessary. To do so, start by opening the file.

- 1) Click the **Change Permission** button within the yellow RESTRICTED ACCESS notification banner, to open the Permission controls window



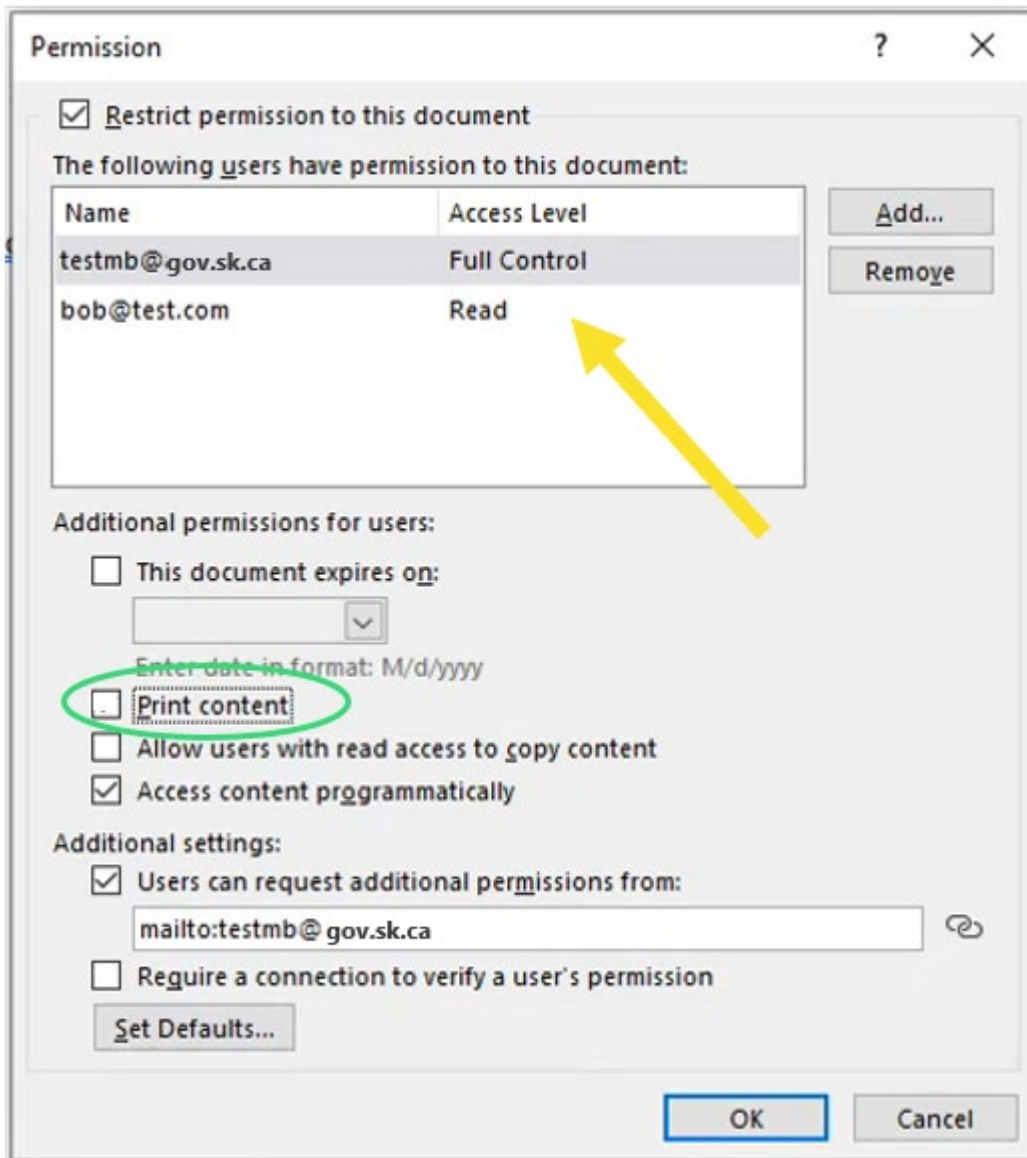
**Tip:** If you do not see the RESTRICTED ACCESS banner, close out of the document (ensure it is saved) and re-open it for the **Change Permission** button to appear.

2) Delete or Add contacts to the 'Read' (Viewer) or 'Change' (Co-Author) fields as required, and click **More Options** to see all permissions for all users



3) Review and adjust permissions as necessary, click **OK** to apply changes

Within the 'More Options' Permission window, you can easily see and manage who has access to the file. In this example, testmb@gov.sk.ca is the label owner with 'Full Control' and bob@test.com has 'Read' only access.



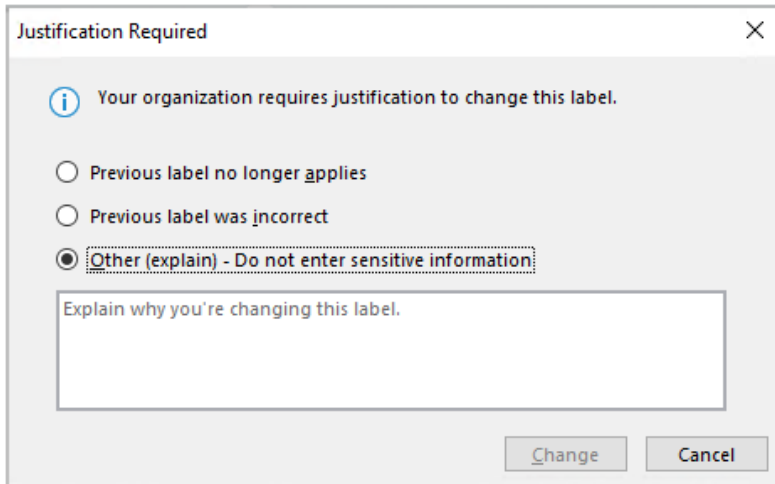
**Tip:** Use the 'Change Permission' button to periodically audit access to highly sensitive information and to select specific capabilities for specific user. For example, you can allow bob@test.com to print content while having Read (View Only) access.

## HOW TO CHANGE A SENSITIVITY LABEL - JUSTIFICATION REQUIRED

1) With the file open, click the preferred label for classifying the file using the Information Protection toolbar

The Justification Required window appears. Provide your reasoning for changing the label and click **Change**.





Justification Required

**i** Your organization requires justification to change this label.

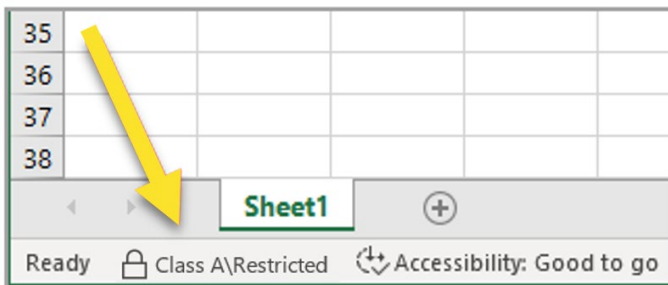
Previous label no longer applies  
 Previous label was incorrect  
 Other (explain) - Do not enter sensitive information

Explain why you're changing this label.

Change Cancel

**Note:** This is not an approvals process. The change justification information is stored for record keeping and the update to the file label takes place immediately, along with the pre-set security controls.

**Tip:** If the Information Protection Toolbar is not showing, you can identify what label is currently applied to a file by looking at the status bar at the bottom of the window.



## WHAT TO EXPECT WITH SENSITIVITY LABELS

Sensitivity Labels allow you to classify content with the appropriate information classification level and set protection measures to a file with a single click.

### Key Take-Aways:

- All users and groups which are part of “gov.sk.ca” 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).
- Use permission controls to allow authorized recipients of Class A or Class B documents to view, edit, copy, or print accordingly.
- Justification is required by a label owner to change a label.

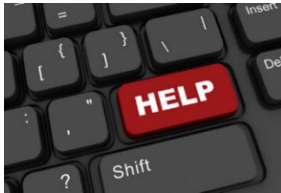
- When a recipient attempts to open a document they do not have permission for, they receive a pop-up notification informing them that access is denied. The email of the label owner is made available in the notification. It is the recipient's responsibility to contact the label owner to inquire about access.
- It is best practice to not screen share Class A or Class B emails and documents with unauthorized users.

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

- [Sensitivity Labels Classification Taxonomy for Documents](#)
- [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