

# Microsoft Information Protection (MIP) User Guide

Prepared By  
ITSC

Version: 6.0

*[Initial version: Nov 2017]*

*[Last update: Oct 2025]*

## Table of Contents

<b>1. About MIP</b>	<b>4</b>
<b>2. Client Installation</b>	<b>4</b>
2.1. Supported Environment	4
2.2. Download MIP Client Installation File	5
2.3. MIP Client Installation	5
<b>3. MIP Policy, Classification/Sensitivity Labeling and Protection</b>	<b>7</b>
3.1. Pre-defined Sensitivity Labels and Permission Controls	7
<b>4. File Protection in Windows</b>	<b>8</b>
4.1. Create a MIP-Protected File with Sensitivity Label	8
4.2. Open a MIP-Protected file and View Permission	13
<b>5. File Protection in Mac OS</b>	<b>16</b>
5.1. Create a MIP-Protected File with Sensitivity Label	16
5.2. Open a MIP-Protected file and View Permission	16
<b>6. File Protection in Mobile Devices</b>	<b>17</b>
6.1. Create a MIP-Protected File with Sensitivity Label	17
6.2. Open a MIP-Protected file and View Permission	21
6.3. Change or Remove Sensitivity Label of MIP-protected file	23
<b>7. Email Protection for O365 Email</b>	<b>26</b>
7.1. Send MIP-Protected Email with Sensitivity label in MS Outlook	26
7.2. Send MIP-Protected Email with Sensitivity label in Outlook Web Access (OWA)	28
7.3. Send MIP-Protected Email with Subject Tag	30
7.4. Read MIP-Protected Email	32
<b>8. File Protection in SharePoint Online &amp; OneDrive</b>	<b>34</b>
8.1. Create a MIP-Protected document in SharePoint Online & OneDrive	34
8.2. Open a MIP-Protected document in SharePoint Online & OneDrive	34

<b>Document History</b>		
<b>Version</b>	<b>Update Date</b>	<b>Changes</b>
1.0	Nov 2017	Initial version
2.0	Dec 2017	Updated supported iOS and Android OS version in Section 2.1 Added the remarks about central deployment Section 2.2
3.0	Oct 2019	Updated the wordings and screens for MS Outlook in Section 5.1.1
4.0	Feb 2020	Updated supported Windows OS, Office, iOS and Android OS versions in Section 2.1
5.0	Jan 2021	Updated all steps and screens from AIP client to MIP Unified Labeling client
6.0	Oct 2025	Updated all steps and screens from MIP Unified Labeling client to Microsoft Purview Information Protection client






## 1. About MIP

**Microsoft Purview Information Protection (MIP)** helps you to classify, label and protect your data at the time of creation based on the sensitivity of data. Labels, and protection are persistent, traveling with the data throughout its lifecycle, so that it's detectable and controlled at all times – regardless of where it's stored or with whom it's shared – internally or externally.

## 2. Client Installation

### 2.1. Supported Environment

The following table shows the required applications and supporting environment to protect and/or access the files and emails:

Supported OS	Supported Office	Required applications	Operations can be done
Windows 11 or above	Microsoft 365	<ul style="list-style-type: none"> <li>- Microsoft Purview Information Protection client (v3.1.x)</li> <li>- Foxit PDF Editor</li> </ul>	<ul style="list-style-type: none"> <li>- <b>Protect</b> MS Office files with <b>Sensitivity</b> button in MS Office applications</li> <li>- <b>Protect</b> PDF files with <b>Foxit PDF Editor</b></li> <li>- <b>Protect</b> non-MS Office files with <b>MIP client</b></li> <li>- <b>Access</b> all MIP-protected MS Office files with MS Office application</li> <li>- <b>Access</b> all MIP-protected PDF files with Foxit PDF editor</li> <li>- <b>Access</b> all MIP protected non-MS Office files with MIP client</li> </ul>
Mac OS 14 or above	Microsoft 365	<ul style="list-style-type: none"> <li>- RMS Sharing app </li> <li>- Foxit PDF Editor app </li> </ul>	<ul style="list-style-type: none"> <li>- <b>Protect</b> MS Office files with <b>Sensitivity</b> button in MS Office apps</li> <li>- <b>Protect</b> PDF files with <b>Foxit PDF Editor</b></li> <li>- <b>Access</b> all MIP-protected MS Office files with <b>MS Office apps</b></li> <li>- <b>Access</b> all MIP-protected PDF files with <b>Foxit PDF editor</b></li> <li>- <b>Access</b> all other MIP-protected non-MS Office files with <b>RMS Sharing app</b></li> </ul>
iOS 18.0 or above	Latest Microsoft Office apps 	<ul style="list-style-type: none"> <li>- Azure Information Protection viewer app (v2.x) </li> </ul>	<ul style="list-style-type: none"> <li>- <b>Protect</b> MS Office files with <b>Sensitivity</b> button in MS Office apps</li> <li>- <b>Protect</b> PDF files with <b>Foxit PDF Editor</b></li> </ul>
Android OS 13 or above		<ul style="list-style-type: none"> <li>- Foxit PDF Editor app </li> </ul>	<ul style="list-style-type: none"> <li>- <b>Access</b> all protected MS Office files with <b>MS Office apps</b></li> <li>- <b>Access</b> all protected PDF files with <b>Foxit PDF editor app</b></li> <li>- <b>Access</b> all protected non-MS Office files with <b>AIP viewer app</b></li> </ul>

## 2.2. Download MIP Client Installation File

### 2.2.1. For Windows:

For standalone installation, you may download and extract the installation file “**PurviewInfoProtection.exe**” at <https://www.microsoft.com/en-us/download/details.aspx?id=53018>.

For central deployment, you may download and extract the MSI file “**PurviewInfoProtection.msi**” at <https://www.microsoft.com/en-us/download/details.aspx?id=53018>.

### 2.2.2. For Mac OS:

Download “**RMS Sharing**” app from App Store.

### 2.2.3. For iOS and Android OS:

Download “**Azure Information Protection**” app from Apple Store (iOS) and Google Play (Android OS).

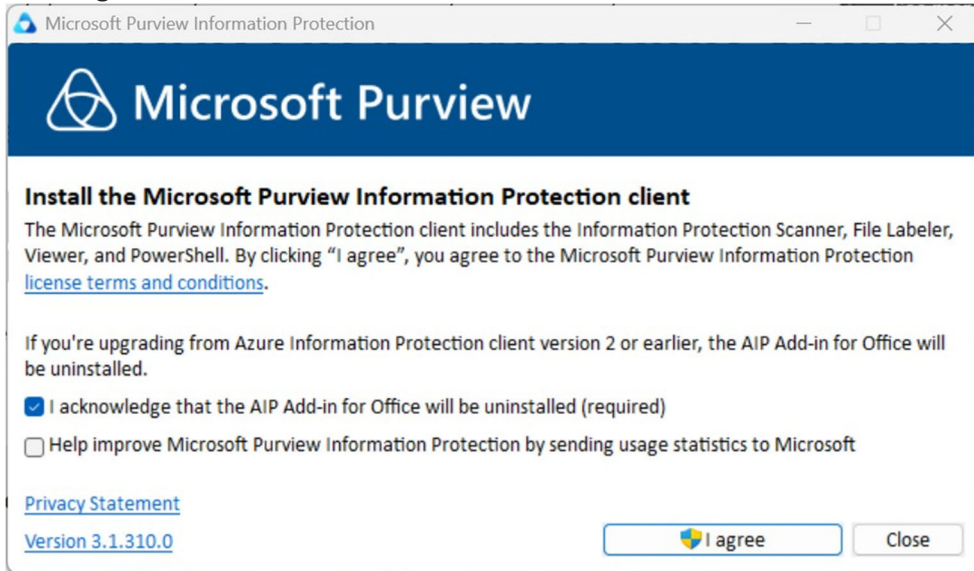
## 2.3. MIP Client Installation

### 2.3.1. In Windows

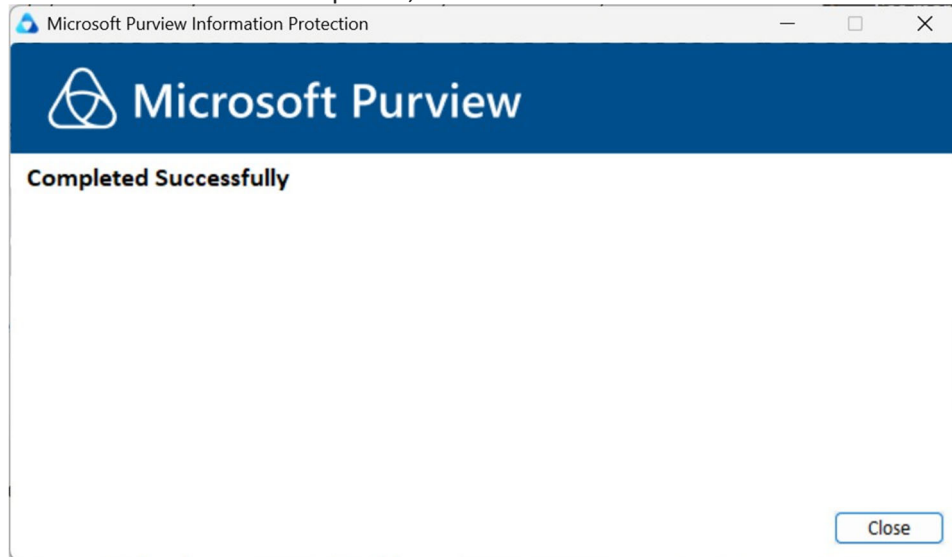
#### Steps:

1. **Close all** Office applications and all instances of File Explorer.
2. **Double click** the installation file “PurviewInfoProtection.exe”.
3. Install the MIP Client:
  - 3.1. **Deselect** Help improve Azure Information Protection by sending usage statistics to Microsoft.

3.2. Click **I agree** to install the client.



3.3. When the installation is completed, click Close.



### 2.3.2. In Mac OS

**Steps:**

1. After download the RMS Sharing app, it will be installed automatically.

### 2.3.3. In iOS & Android OS

**Steps:**

1. Download the Azure Information Protection app, and it will be installed automatically.

### 3. MIP Policy, Classification/Sensitivity Labeling and Protection

3 default settings in the MIP policy are configured:

- It is **NOT mandatory** to have a classification/sensitivity label for all documents or emails.
- There is **NO default classification/sensitivity label** for documents or emails.
- It is **REQUIRED to provide justification** to remove the classification/sensitivity label and protection in a protected document or email.

When you are going to protect your documents, you can use the pre-defined classification/sensitivity labels with permission controls.

#### 3.1. Pre-defined Sensitivity Labels and Permission Controls

The following table describes the details about the default Sensitivity classification, Labeling and Protection controls pre-defined.

Sensitivity	Label	Permissions Granted		Protection with Encryption	Visual Markings	Offline Access and Expiry Date
Confidential	Confidential – All Staff	Editable by All CUHK Staff	Permission includes: - View, Edit, Save, Save as, Export, Copy, Print, Reply, Reply all, Forward	Yes	- Header & Footer in <u>both</u> MS Office files and emails	- Allows <b>7</b> days offline access - <b>No</b> expiry date
Strictly Confidential	Strictly Confidential – All Staff	Viewable by All CUHK Staff	Permission includes: - View, Reply, Reply all	Yes	- Header, Footer & Watermark in MS Office files - Header & Footer in emails	- Allows <b>1</b> days offline access - <b>No</b> expiry date

## 4. File Protection in Windows

### 4.1. Create a MIP-Protected File with Sensitivity Label

Below sections demonstrate the steps to create protected MS Office files (i.e. Word, Excel & PowerPoint) and non-MS Office files.

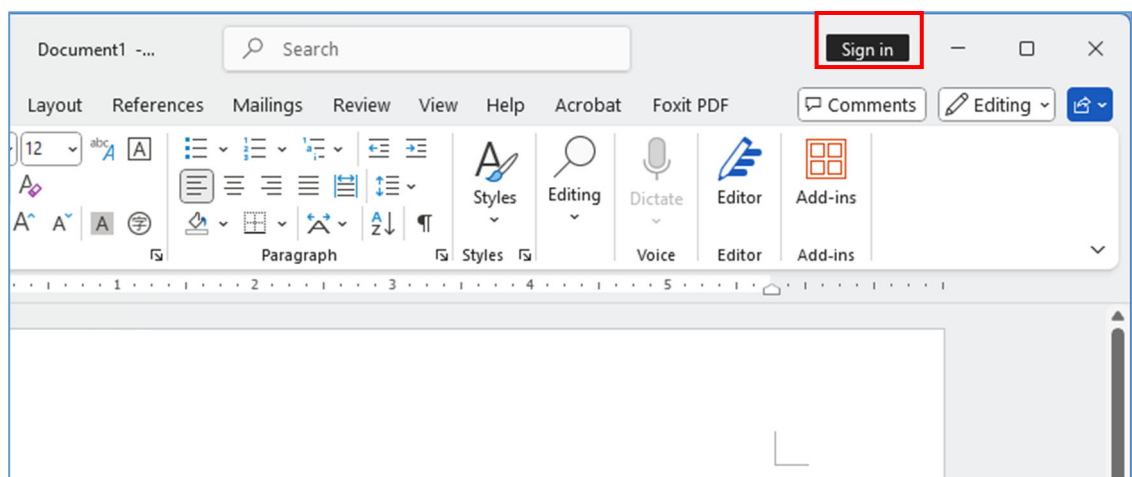
#### 4.1.1. For MS Office Files

For MS Office files, you can use the MIP Sensitivity button which builds into the M365 Office applications to protect the files. The following steps can be applied to MS Word, Excel & PowerPoint.

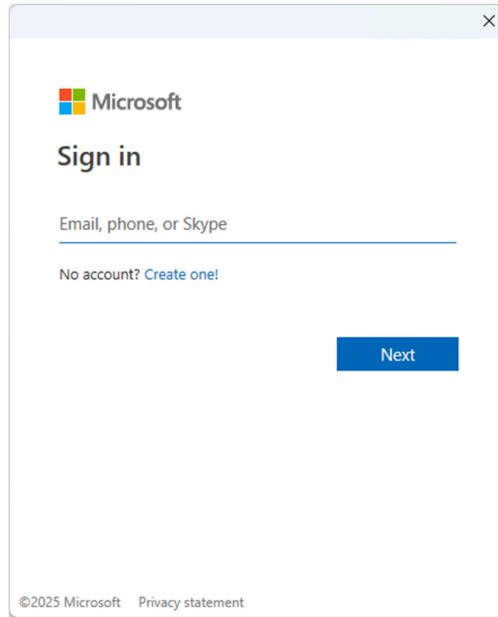
##### 4.1.1.1. Sign in MS Office applications and MIP

#### Steps:

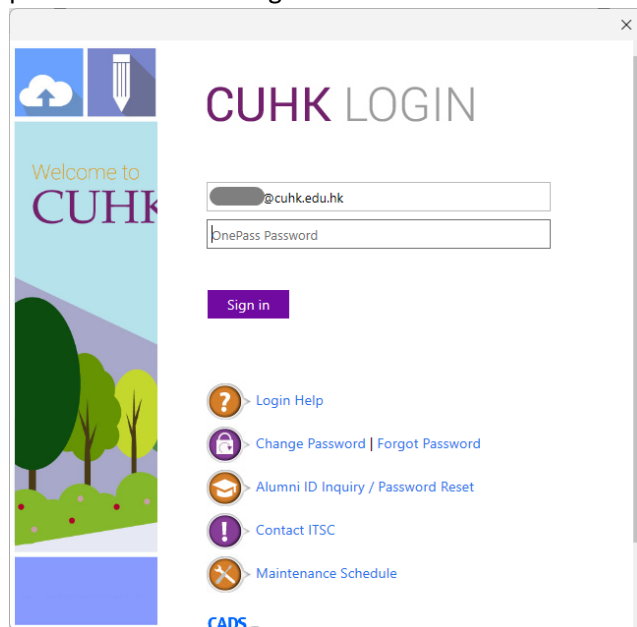
1. Start MS office application e.g. Word, Excel or PowerPoint. If you have not signed in your CUHK O365 account, please **click Sign in** on the top right-hand corner.



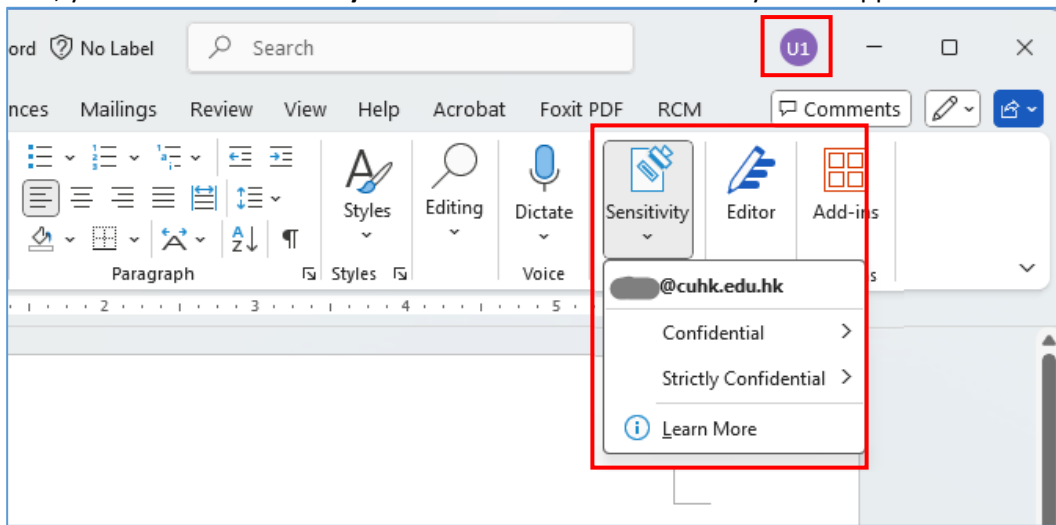
2. Sign in with your CUHK O365 account email address and click Next button.



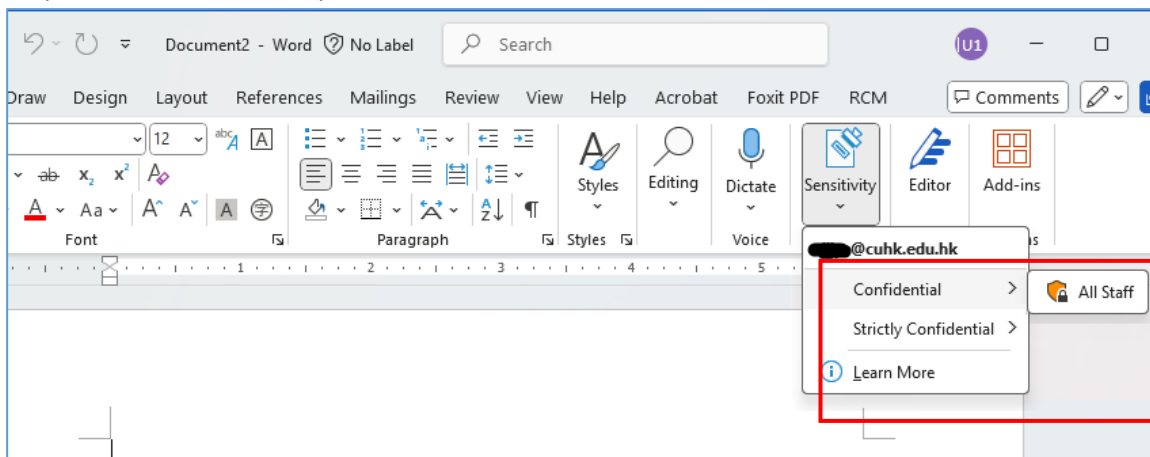
3. In CUHK login page, enter your **OnePass password**, then click **Sign in** button and provide the 2FA for login.



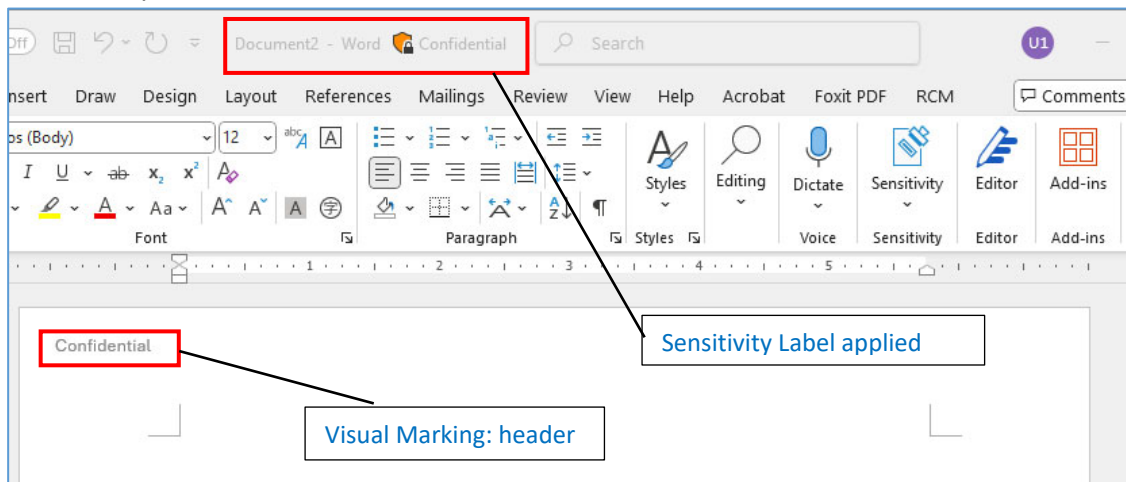
1. After signing in successfully, you can find your name on the top right-hand corner. Also, you can see a **Sensitivity icon** with the available sensitivity labels appear on the ribbon.



2. Select an appropriate sensitivity label to classify and protect the document with pre-defined permissions. For example, select **Confidential**, then **Confidential – All Staff**.



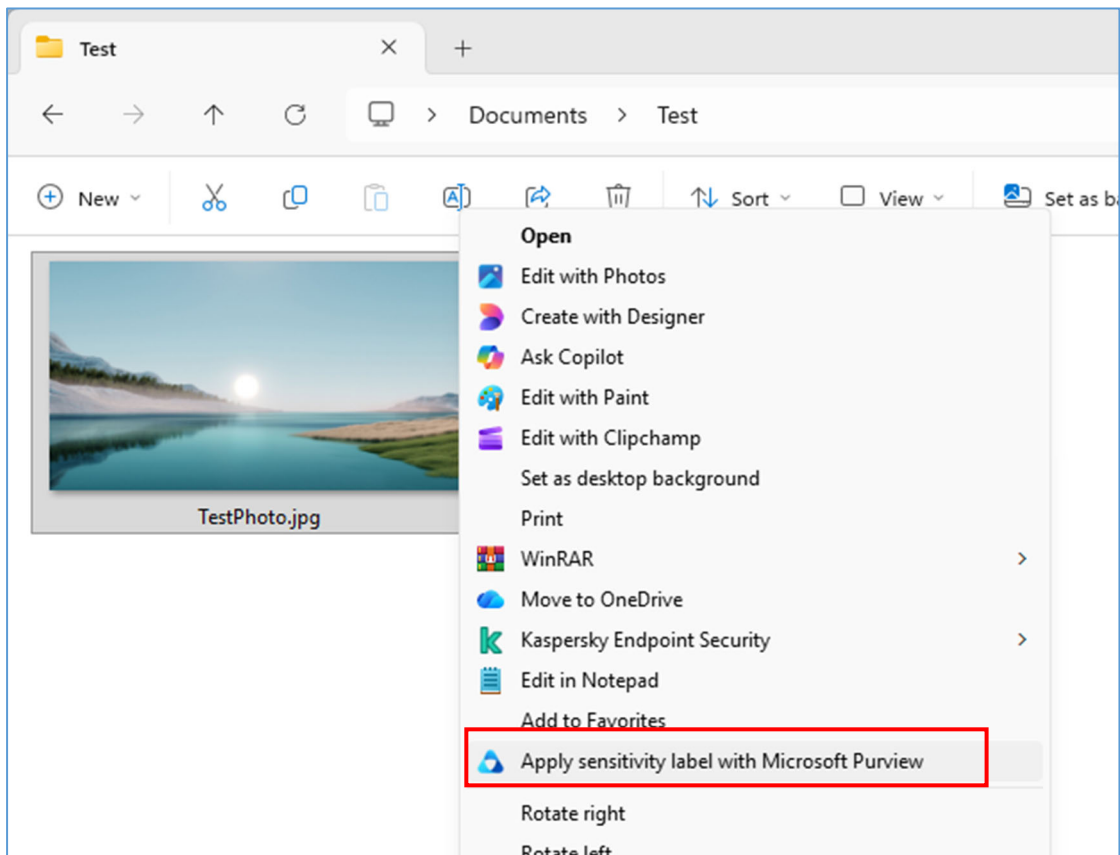
3. After the sensitivity label is applied, you can see the filename is labelled with the "Confidential" label, also, visual markings, i.e. header and footer in this case, indicate the sensitivity label as well.



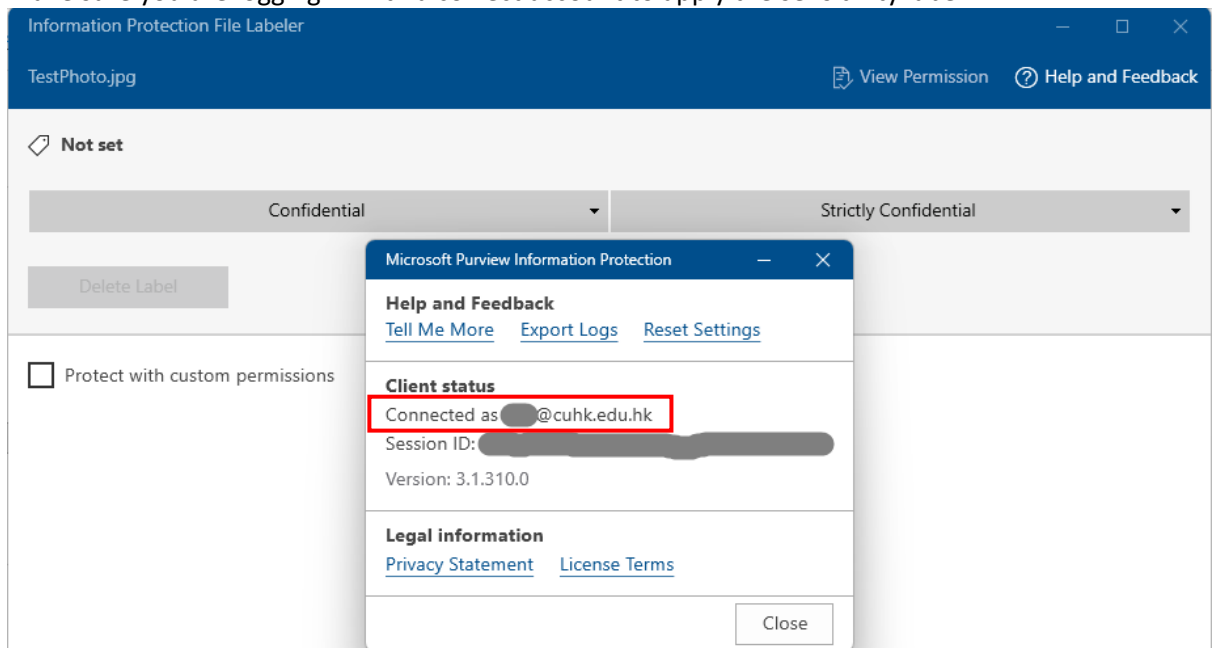
#### 4.1.2. For Non-MS Office Files

##### Steps:

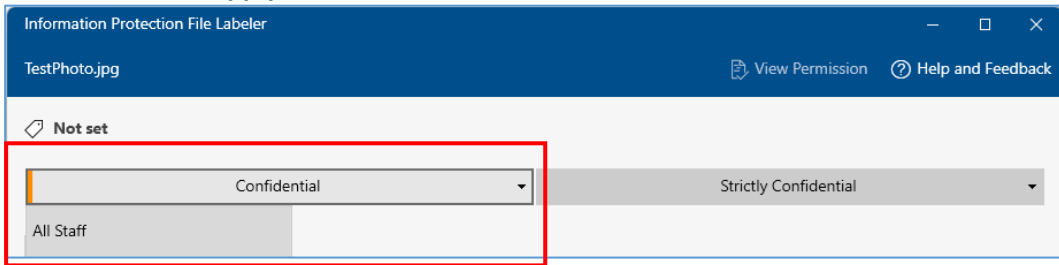
1. Select a non-MS Office file, e.g. jpg, txt or pdf file, right click and select “**Apply sensitivity label with Microsoft Purview**” on the context menu.



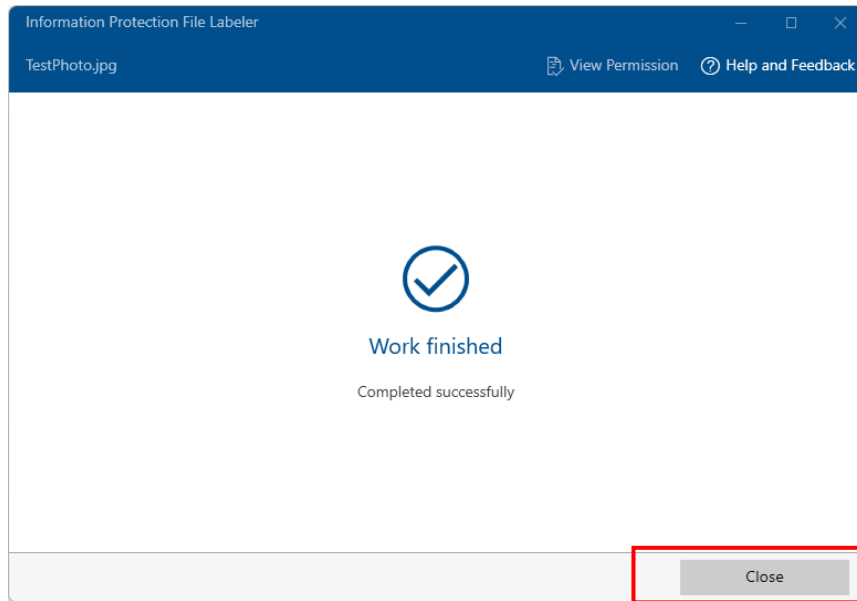
2. Make sure you are logging in with a correct account to apply the sensitivity label.




3. All available sensitivity labels are shown, select an appropriate sensitivity label and protect the file with pre-defined permissions. For example, click **Confidential** and **Confidential – All Staff**, then click **Apply** button.

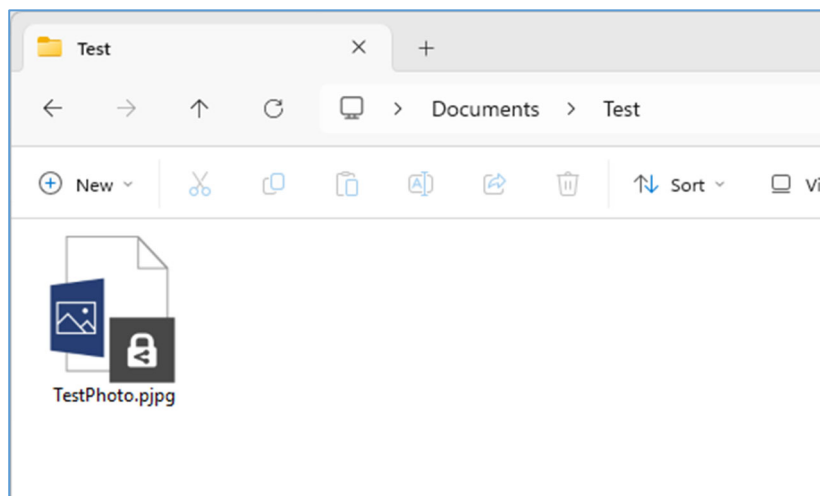


4. Click **Close** button to close the window.



5. After the sensitivity label is applied, the file format has changed to a MIP protected file format. You can see a  on the file icon which indicates that the file is MIP protected.

Also, the file extension is changed from \*.jpg to \*.jpgg which indicates that it is a protected jpeg file.



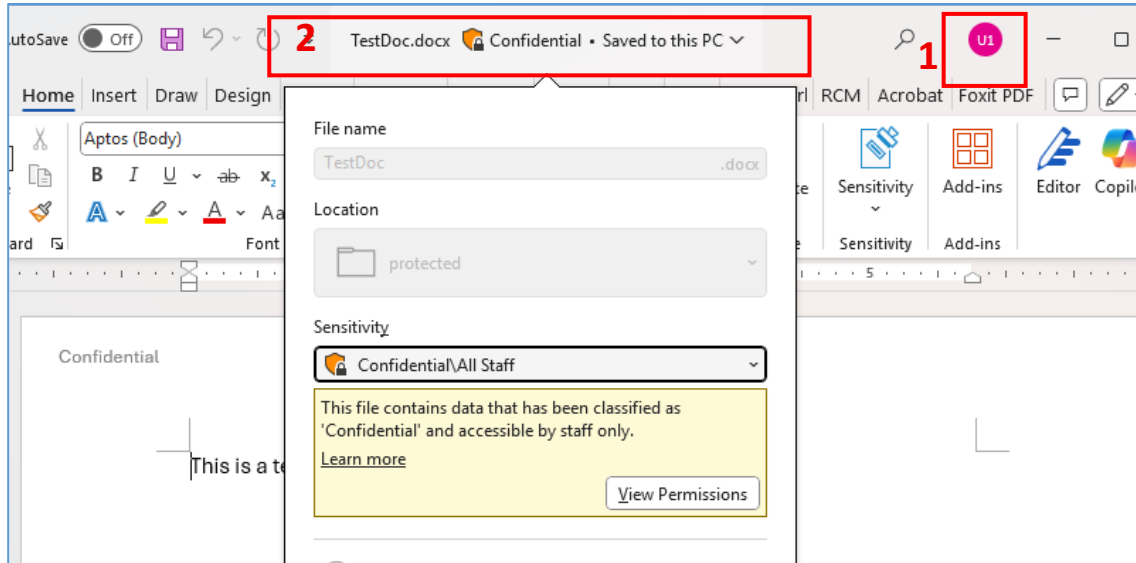
## 4.2. Open a MIP-Protected file and View Permission

### 4.2.1. Open a MIP-protected MS Office File

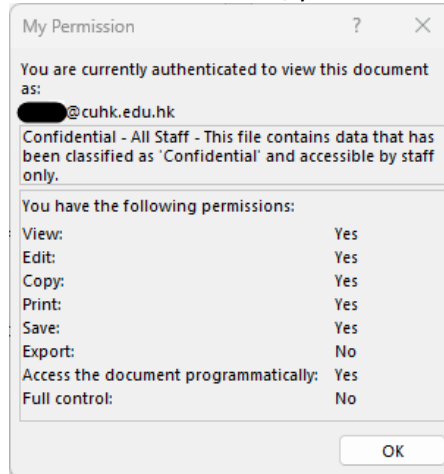
#### Steps:

1. To access a MIP-protected MS Office file that granted the access to you, please make sure you have **signed-in the Office application with the O365 account which has the permission to open the file.**

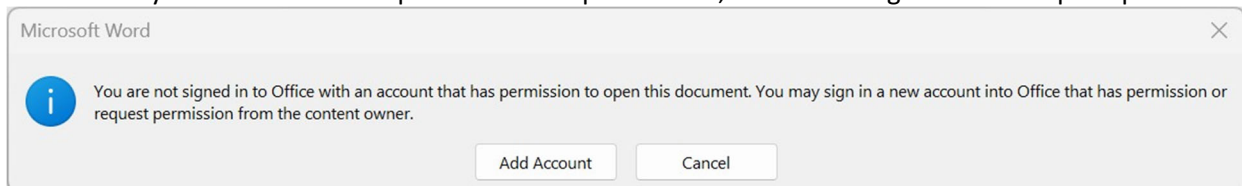
Open the protected file, you can see the sensitivity label applied on this file in the **filename.**



2. **Click the filename, then View Permission** button, you can also find the detail permission.



3. If your account has no permission to open the file, below message box will be prompted.

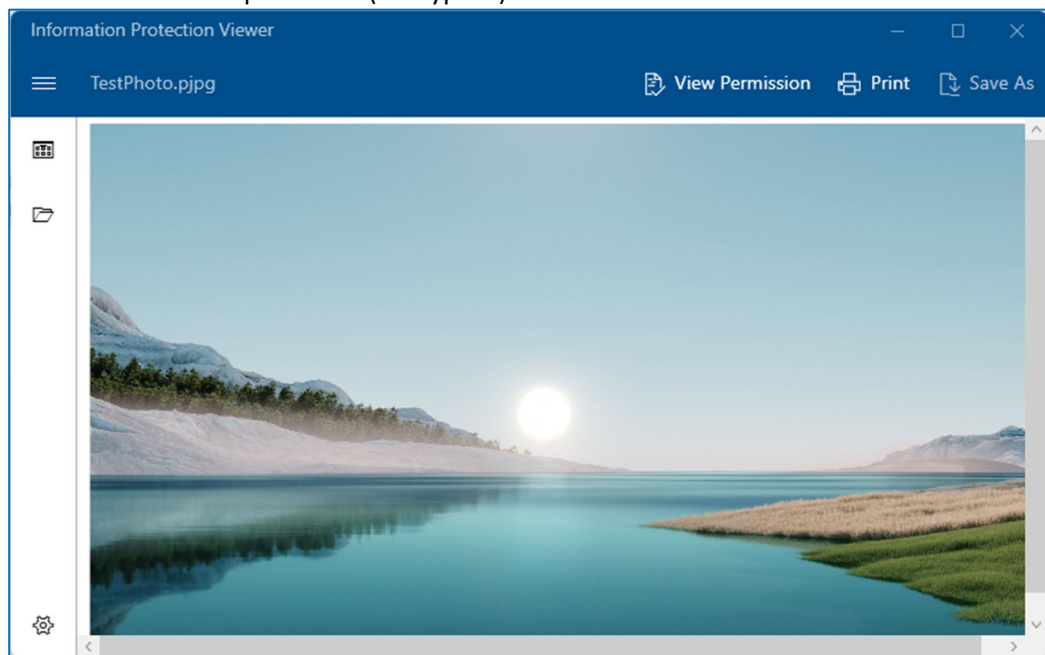


#### 4.2.2. Open a MIP-protected Non-MS Office File

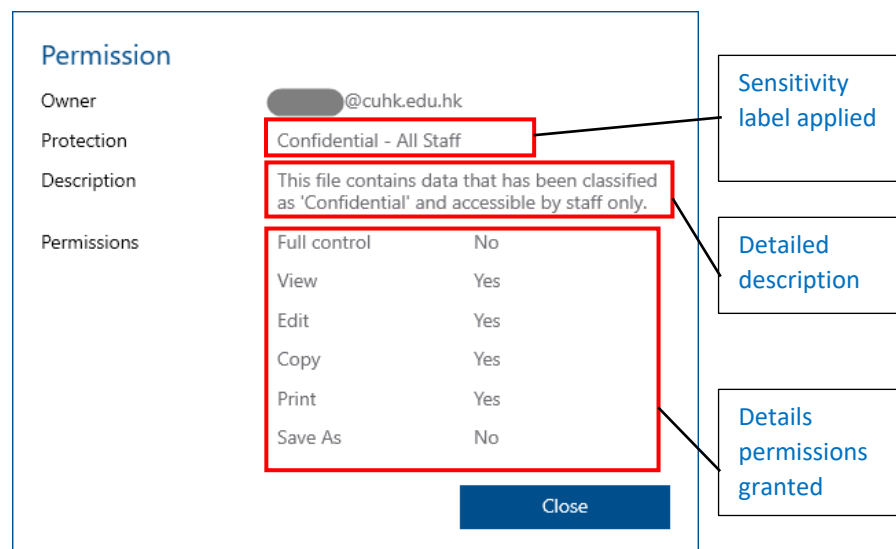
You need to have the Microsoft Purview Information Protection Client installed before you can open a protected non-MS Office file. Details can be found in Section 2.3.

##### Steps:

1. **Double click the protected non-MS Office file**, e.g. \*.jpg or \*.pdf, it will launch the Microsoft Purview Information Protection Viewer automatically which allow you view the content of the MIP-protected (encrypted) file.

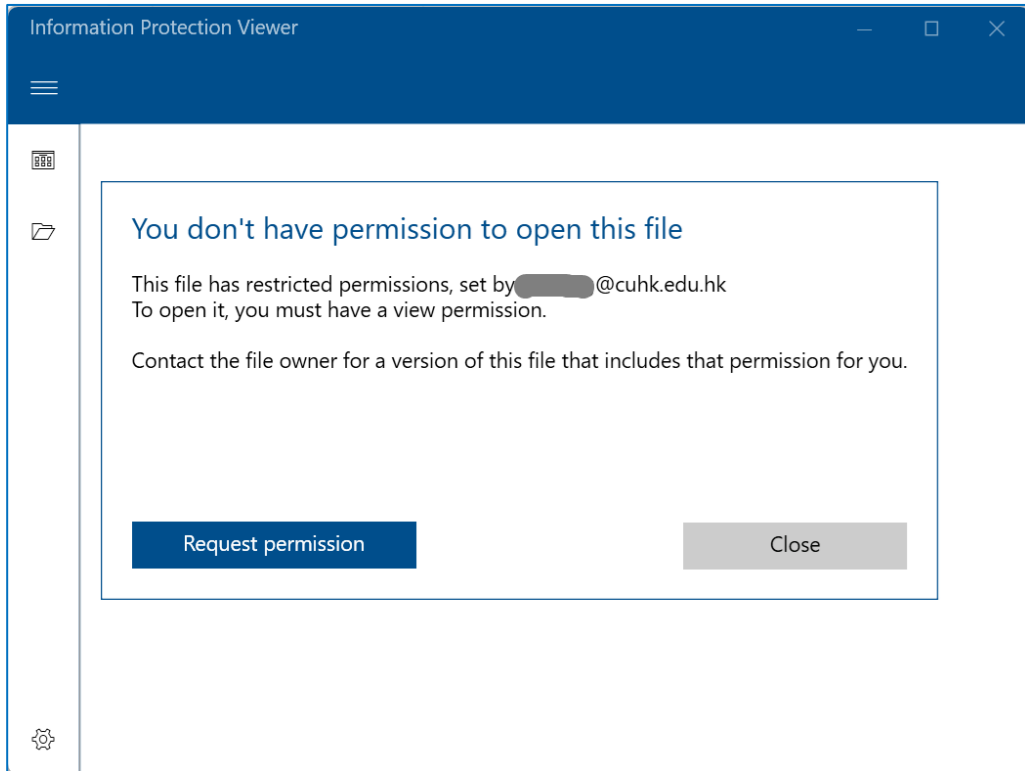


2. Click **View Permission** button to view the Sensitivity label and detail permission applied to this file.

The 'Permission' dialog box is shown with the following fields: Owner (@cuhk.edu.hk), Protection (Confidential - All Staff), Description (This file contains data that has been classified as 'Confidential' and accessible by staff only.), and Permissions (Full control: No, View: Yes, Edit: Yes, Copy: Yes, Print: Yes, Save As: No). A 'Close' button is at the bottom. Three callout boxes on the right point to: 'Confidential - All Staff' (Sensitivity label applied), the description text (Detailed description), and the permissions table (Details permissions granted).

Permission	Granted
Full control	No
View	Yes
Edit	Yes
Copy	Yes
Print	Yes
Save As	No

3. If your account is not authorized to open the file, below message box will be prompted.



## 5. File Protection in Mac OS

### 5.1. Create a MIP-Protected File with Sensitivity Label

In Mac OS, you can only create MIP-protected MS Office files via MS Word, Excel & PowerPoint apps. You can also apply MIP protection to PDF files via Foxit PDF editor app.

For other non-MS Office files, it is unable to apply MIP protection in Mac OS currently.

#### 5.1.1. For MS Office Files

For MS Office files, you can use the MIP Sensitivity button which builds into the M365 Office apps to protect the files. The steps are same as Section 4.1.1.

### 5.2. Open a MIP-Protected file and View Permission

#### 5.2.1. Open the MIP-Protected MS Office file

The steps to open MIP-protected MS Office in Mac OS are same as in Windows, steps can be found in Section 4.2.1.

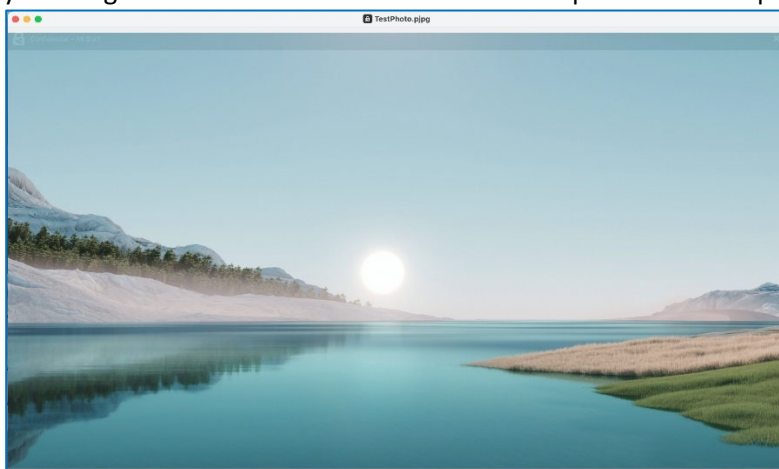
#### 5.2.2. Open the MIP-protected JPG file (non-Office file)

To open a MIP-protected non-MS Office file, you need to download and install the RMS

Sharing app  from App Store in advance.

#### Steps:

1. Double click on a MIP-protected JPG file, it will open the RMS Sharing app to open the non-MS Office file directly. If you are not signed-in the RMS Sharing app, it will prompt you to sign in with the O365 account which has permission to open the file.



## 6. File Protection in Mobile Devices

### 6.1. Create a MIP-Protected File with Sensitivity Label

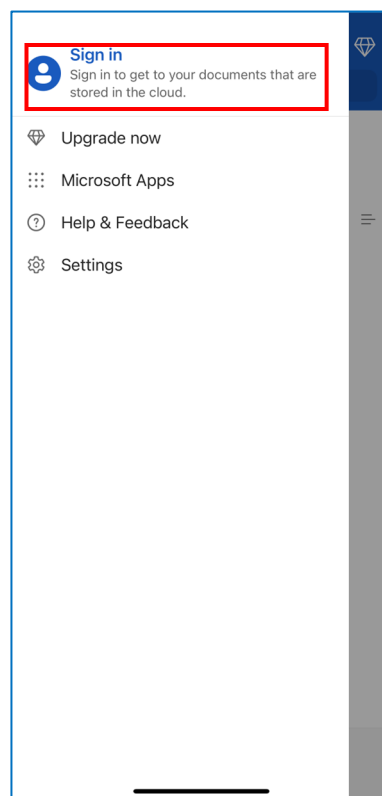
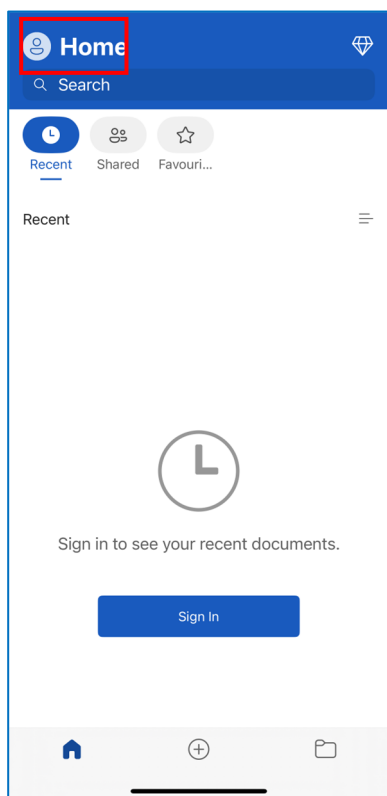
Below sections demonstrate the steps to create protected MS Office files via MS Word, Excel & PowerPoint apps and non-MS Office files via MIP viewer app in iOS and Android devices.

#### 6.1.1. For MS Office Files

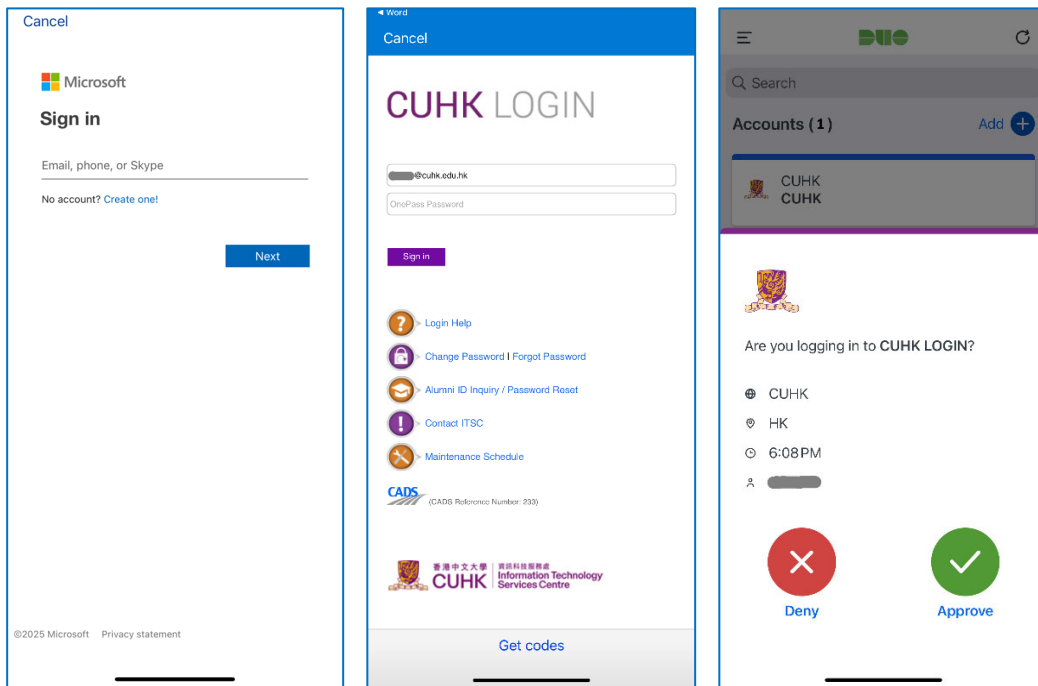
For MS Office files, you can use the MIP Sensitivity button which builds into the M365 Office apps to protect the files. The following steps can be applied to MS Word, Excel & PowerPoint apps.

#### Steps:

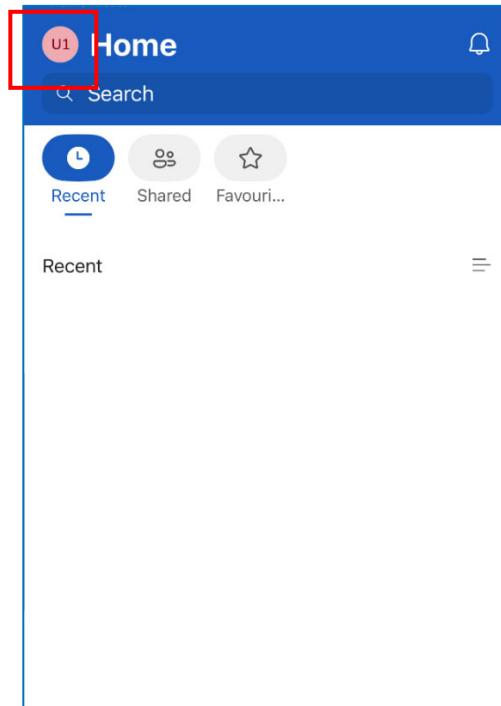
1. Start MS office app e.g. Word, Excel or PowerPoint app. If you have not signed in your CUHK O365 account, **click Sign in** button or **User icon then Sign in** on the top left-hand corner.



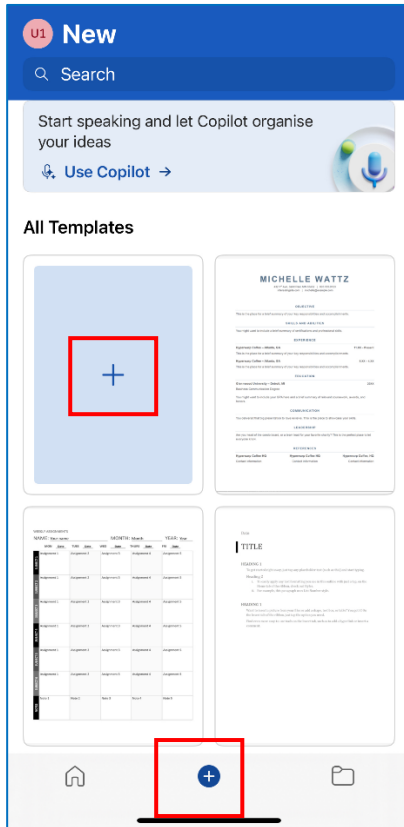
2. Sign in with your CUHK O365 account and provide the 2FA for login.



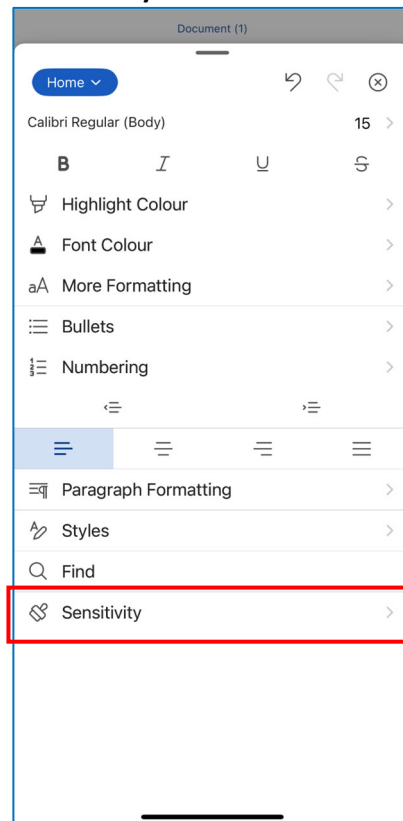
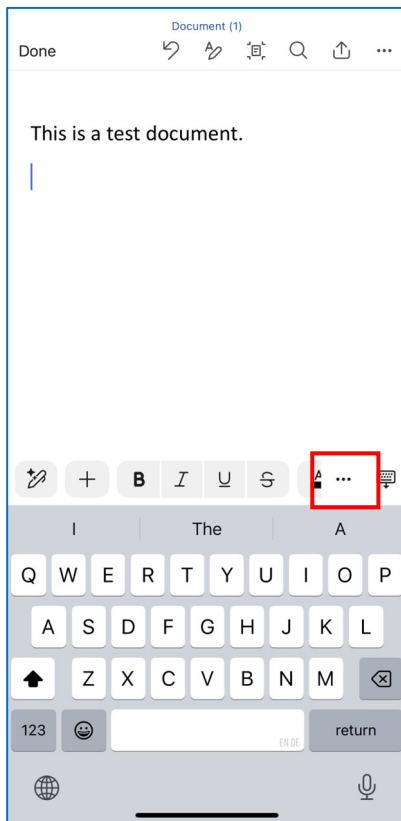
3. After signing in successfully, you can find your name on the top left-hand corner of MS Word app.



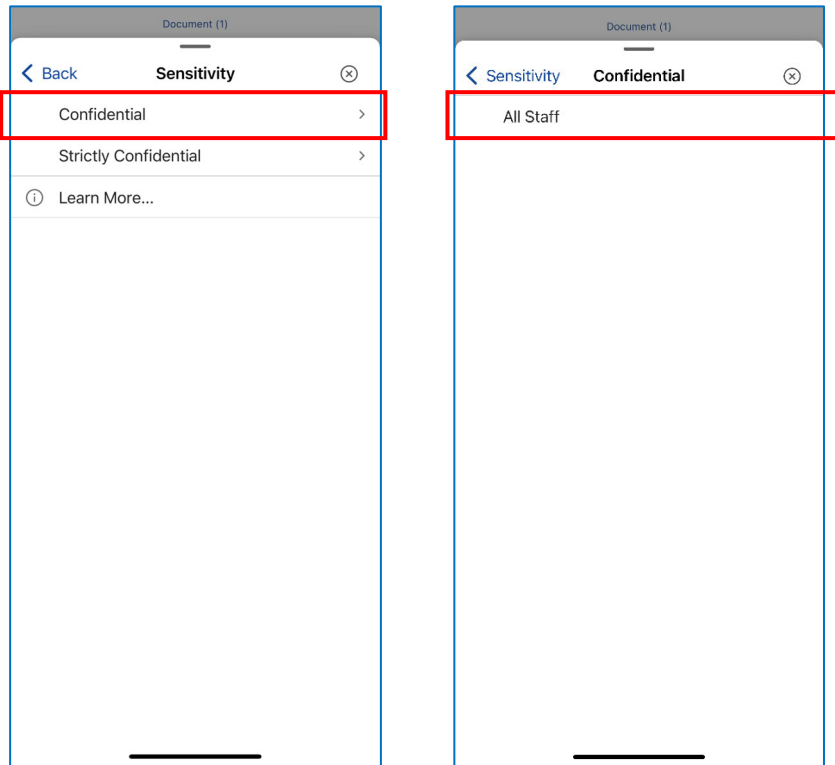
4. Click “+” icon to create a new document.



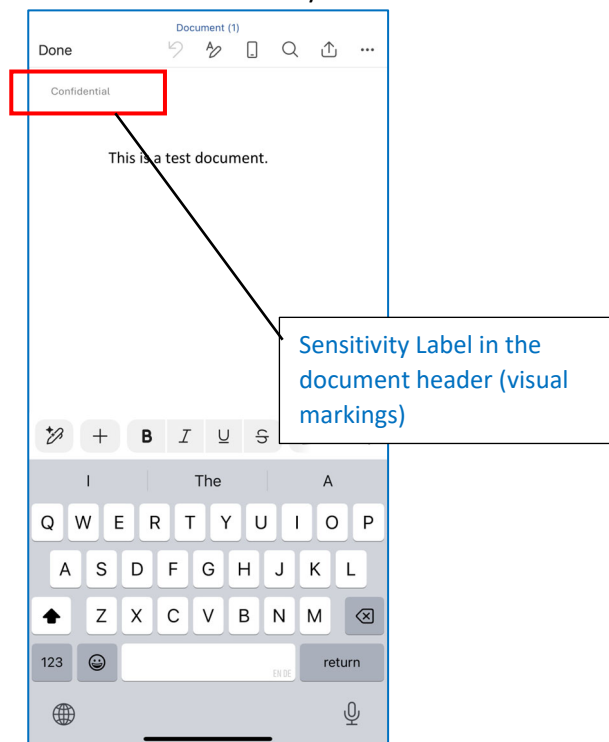
5. Click “...” icon on the toolbar and find the Sensitivity function.



6. Select an appropriate classification label to classify and protect the document with pre-defined permissions. For example, select **Confidential**, then **Confidential – All Staff**.



7. After the sensitivity label is applied, you can see the visual markings of the sensitivity labels added in the header and footer indicate the sensitivity label as well.

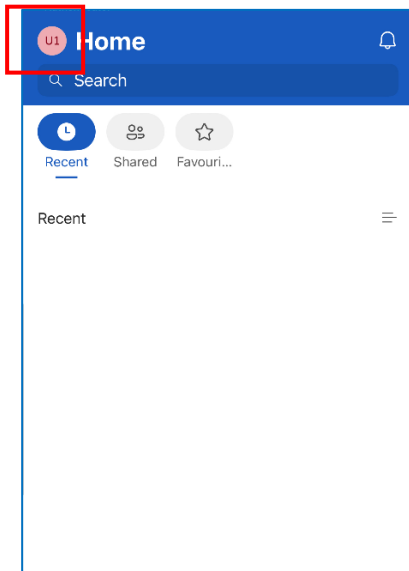


## 6.2. Open a MIP-Protected file and View Permission

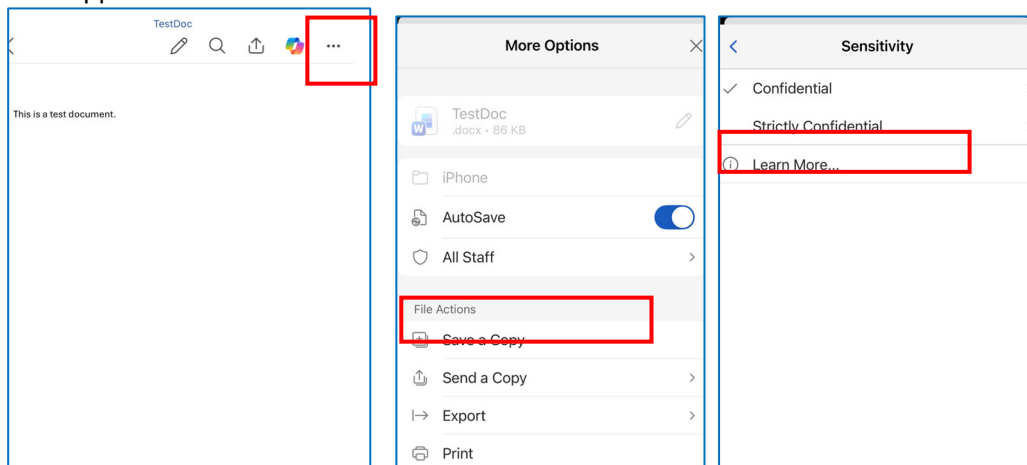
### 6.2.1. Open the MIP-Protected MS Office file

#### Steps:

1. Before opening a MIP-protected MS Office, make sure you have **signed-in the MS Office app with the O365 account which has permission to open the file.**



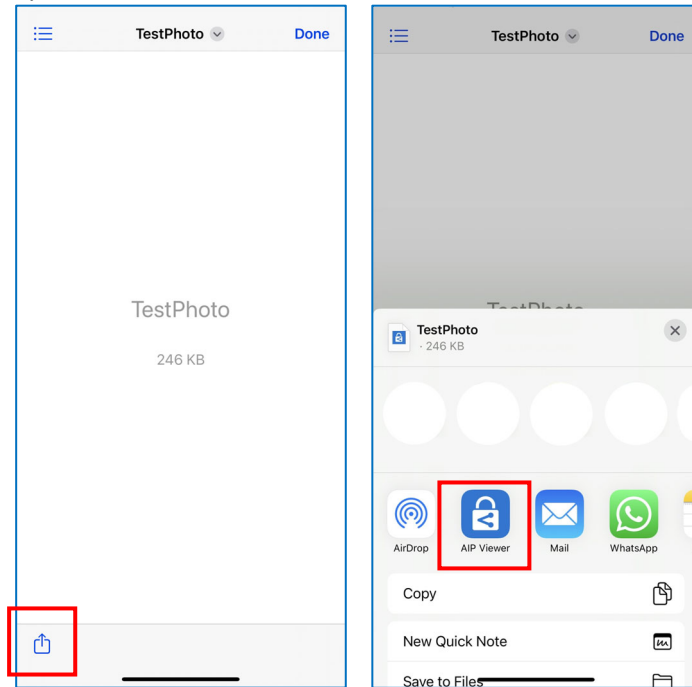
2. Open the MS Office file, **click "..."** icon on the top right-hand corner, you can find the sensitivity label applied on this document.




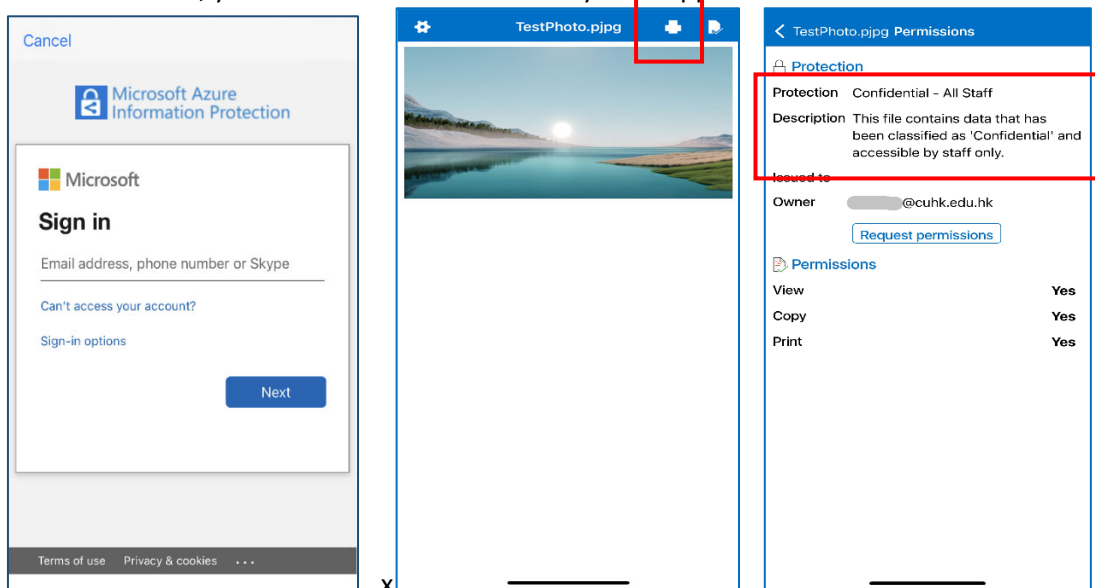
## 6.2.2. Open the MIP-protected JPG file (non-Office file)

### Steps:

- Open a MIP-protected JPG file, then click **Sent to**  icon then find **AIP Viewer**  icon to open the file.



- If you have not signed in AIP Viewer before, the AIP Viewer apps will be triggered, **sign in with your CUHK O365 account**, and you can open the file if permission is granted to you. Then, click on  icon, you can also view the sensitivity label applied on this file.



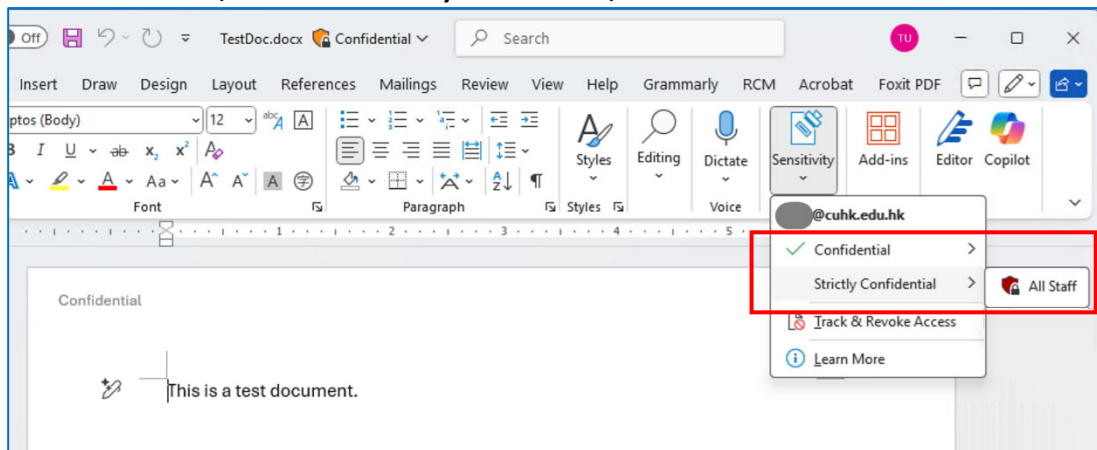
## 6.3. Change or Remove Sensitivity Label of MIP-protected file

Please note that only the file owner can change or remove the sensitivity label of a MIP-protected file.

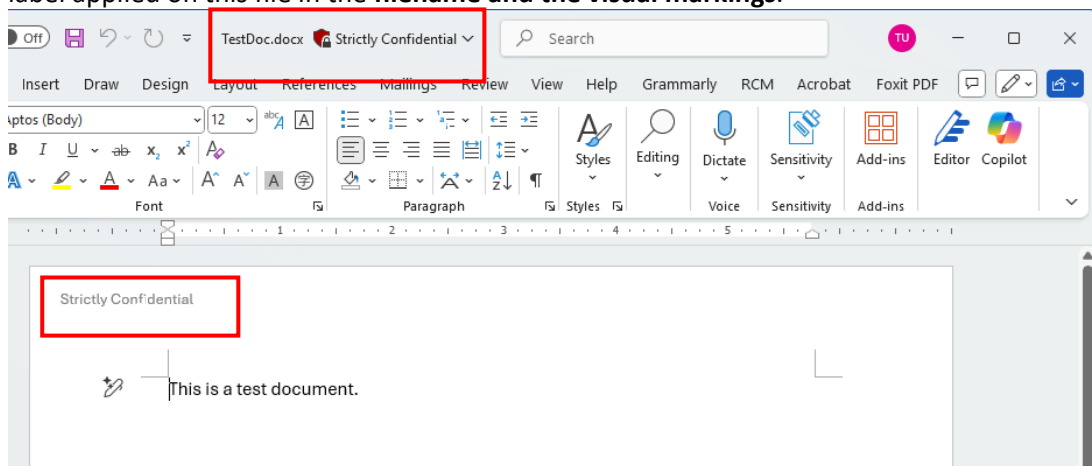
### 6.3.1. For MS Office File

#### Steps:

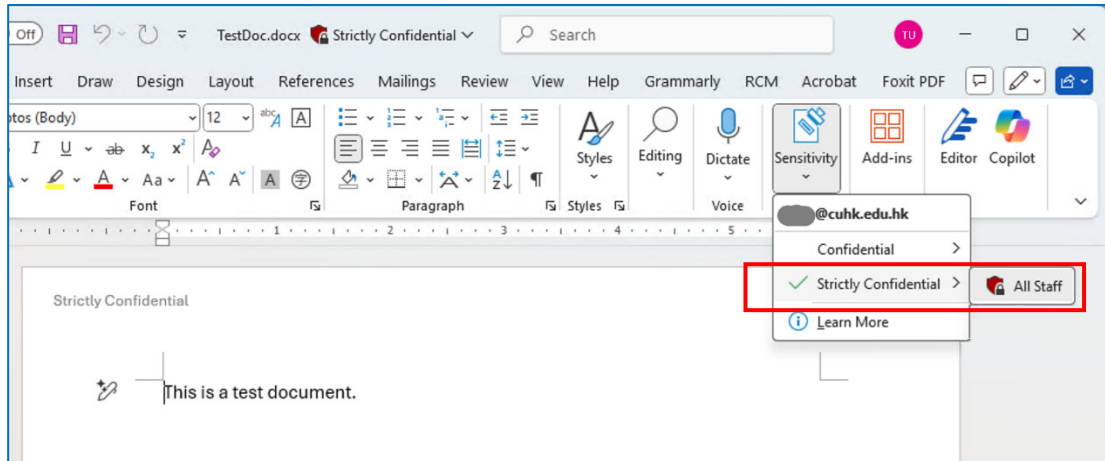
1. Open a MIP-protected file, then click the **Sensitivity** button and **change the sensitivity label from Confidential, All Staff to Strictly Confidential, All Staff**.



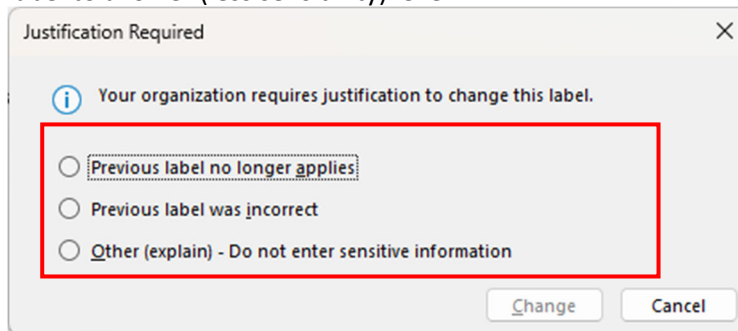
2. If a higher (stricter) sensitivity label is applied, you can immediately see the new sensitivity label applied on this file in the **filename and the visual markings**.



3. To remove the sensitivity label, **click on the same sensitivity label** applied currently.



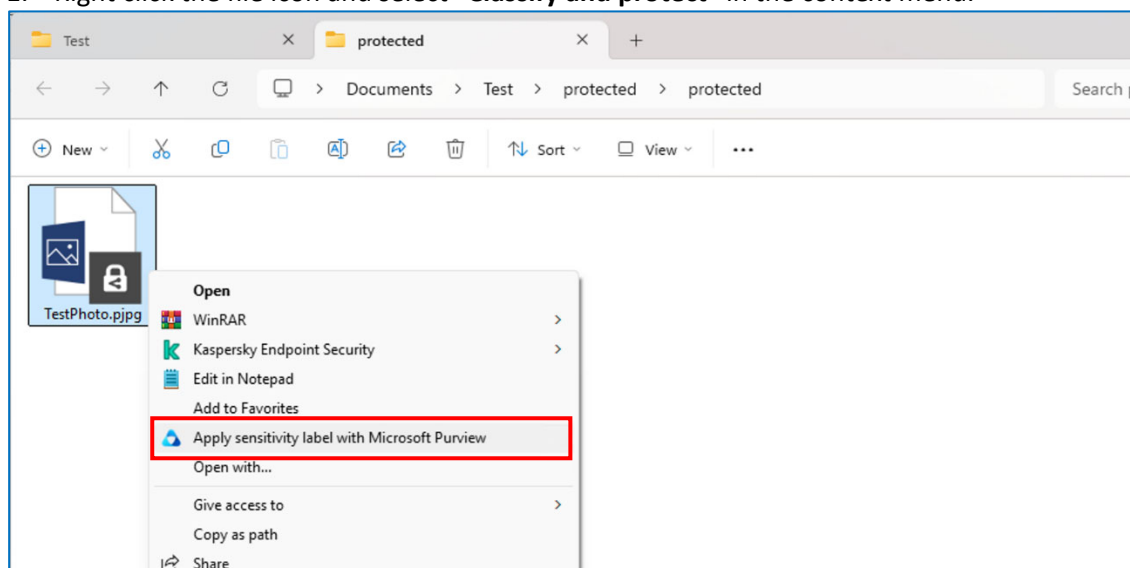
4. You are required to provide the justification for removing a sensitivity label or change the label to a lower (less sensitivity) level.



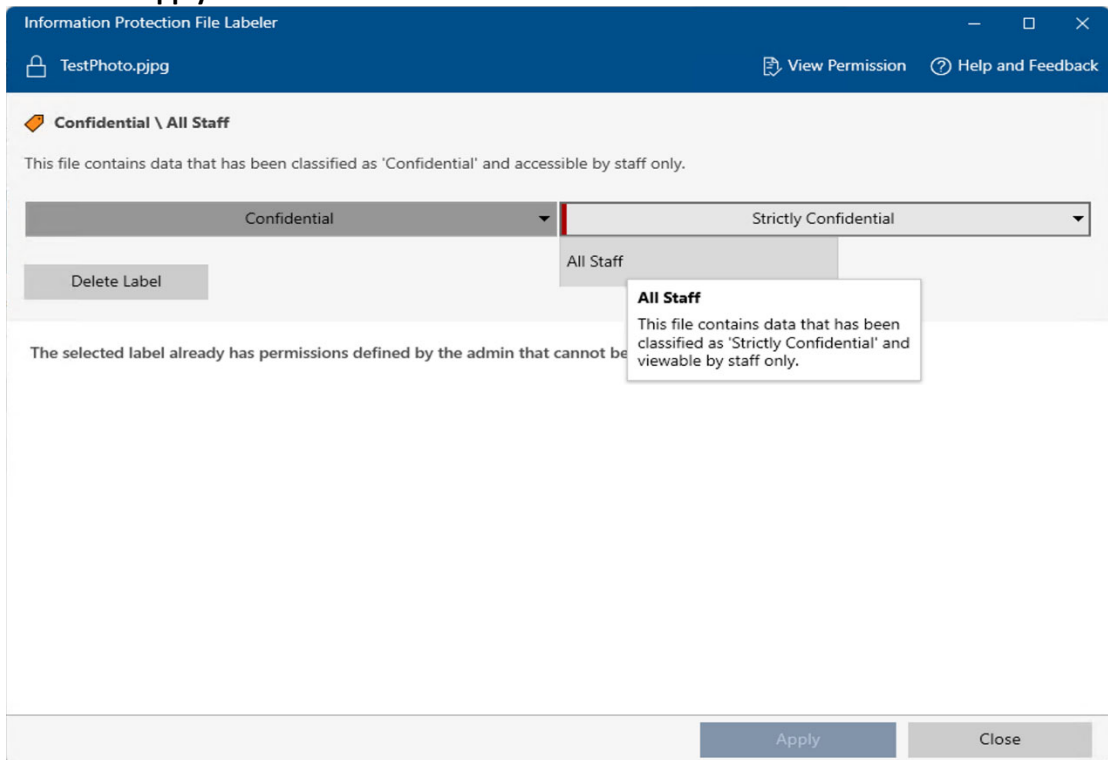
### 6.3.2. For Non-MS Office File

#### Steps:

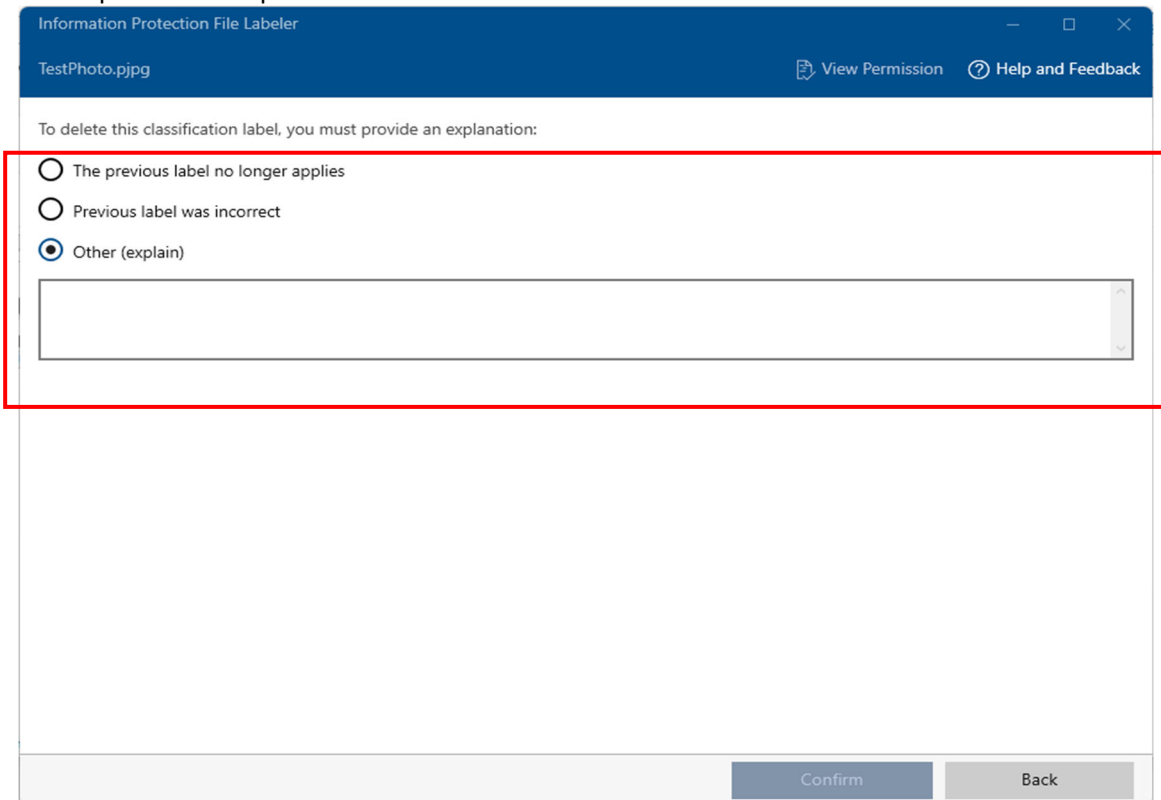
1. Right click the file icon and select **“Classify and protect”** in the context menu.



2. You can select another classification label, or delete current label with the **Delete Label** button, then click **Apply** button to confirm.



3. If you delete a label, click Delete label button and then click Apply button, you will be asked to provide an explanation.



## 7. Email Protection for O365 Email

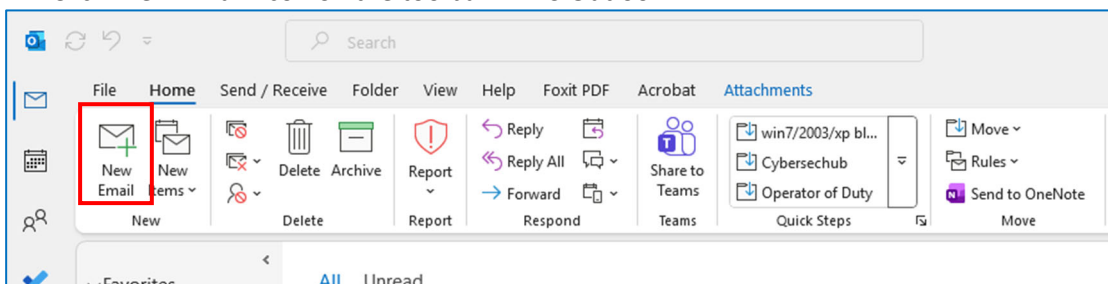
### 7.1. Send MIP-Protected Email with Sensitivity label in MS Outlook

As the MIP is built in with the M365 Office applications, users with O365 accounts can use the MIP to protect their emails.

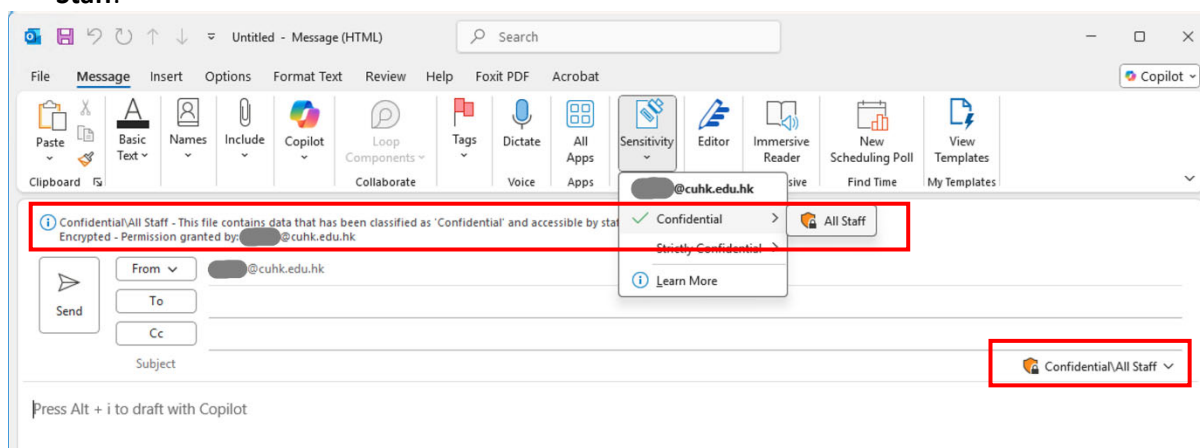
#### 7.1.1. Apply a Sensitivity Label in MS Outlook

##### Steps:

1. Click 'New Email' icon on the toolbar in MS Outlook



2. Click **Sensitivity** button, then select a sensitivity label, for example, click **Confidential, All Staff**.



If there are **more than 1 profile** in your MS Outlook, please make sure to **select the correct owner, under "From" address**, for applying a sensitivity label.

#### 7.1.2. Change / Remove the Sensitivity Label in MS Outlook Windows

##### Steps:

1. To change the sensitivity label, click **Sensitivity** button, then **select another sensitivity label** again.
2. To remove the sensitivity label, click **Sensitivity** button and the **same sensitivity label**, then **provide the justification** for removing the label.

### 7.1.3. Attach File in a MIP-Protected Email

**Steps:**

1. In a MIP-protected email with sensitivity label applied, you can attach any file as usual by clicking the **Attach File** icon.

Different protection between email and attachment would have different behavior:

Email	Attachment	Behavior in Email	Authorized Recipient	Unauthorized Recipient
MIP-Protected	Unprotected	Sensitivity label applied to the email will be applied to attached MS Office files as well, while non-MS Office remains unprotected	✓ Can access both email and attachment	✗ Cannot access both email and attachment
MIP-Protected	MIP-Protected	Email and attachment will be protected by their own sensitivity label.	✓ Can access both email and attachment	✗ Cannot access both email and attachment
Unprotected	MIP-Protected	No protection would be applied to the email.	✓ Can access both email and attachment	✓ Can access the email ✗ Cannot access the attachment
Unprotected	Unprotected	No change in both email and attachment	✓ Can access both email and attachment	✓ Can access both email and attachment

## 7.2. Send MIP-Protected Email with Sensitivity label in Outlook Web Access (OWA)

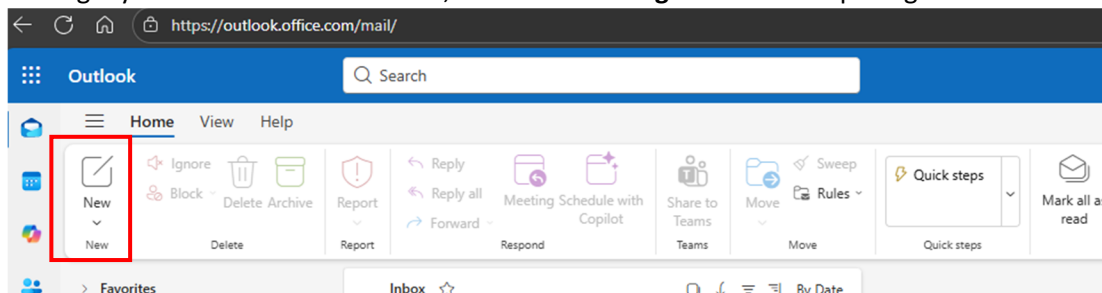
In OWA, **4 types of protection** can be applied to an email:

Types of protection	Description
Confidential	Encryption would be applied to the email. Accessible by all CUHK Staff only Permission includes: View, Edit, Save, Save as, Export, Copy, Print, Reply, Reply all, Forward
Strictly Confidential	Encryption would be applied to the email. Viewable by all CUHK Staff only Permission includes: View, Reply, Reply all
Encrypt	Encryption would be applied to the email.
Do Not Forward	Recipients can read the email, but they cannot forward, print, or copy content.

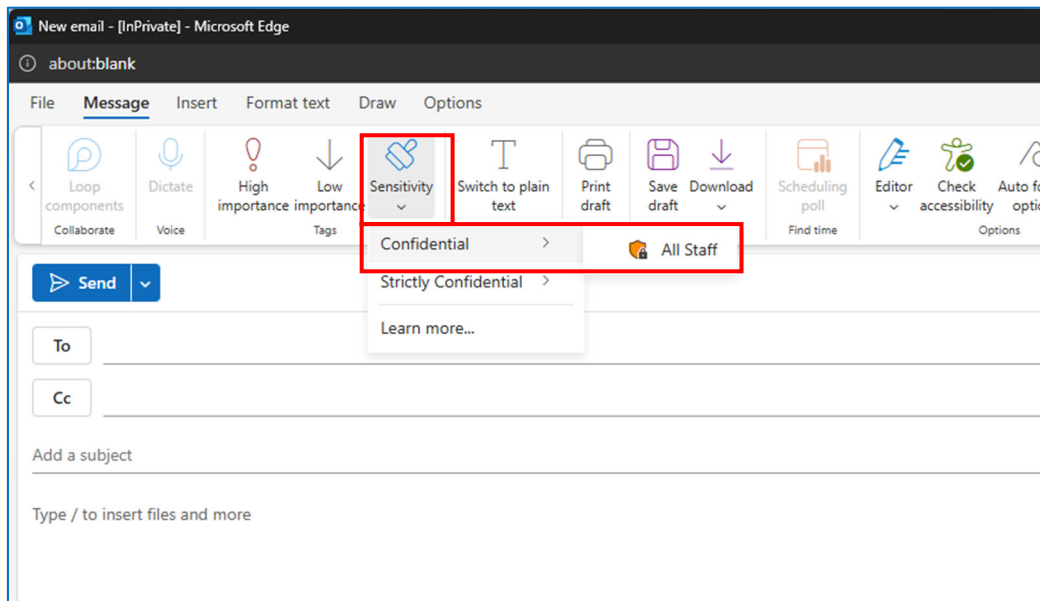
### 7.2.1. Apply a Sensitivity Label in OWA

#### Steps:

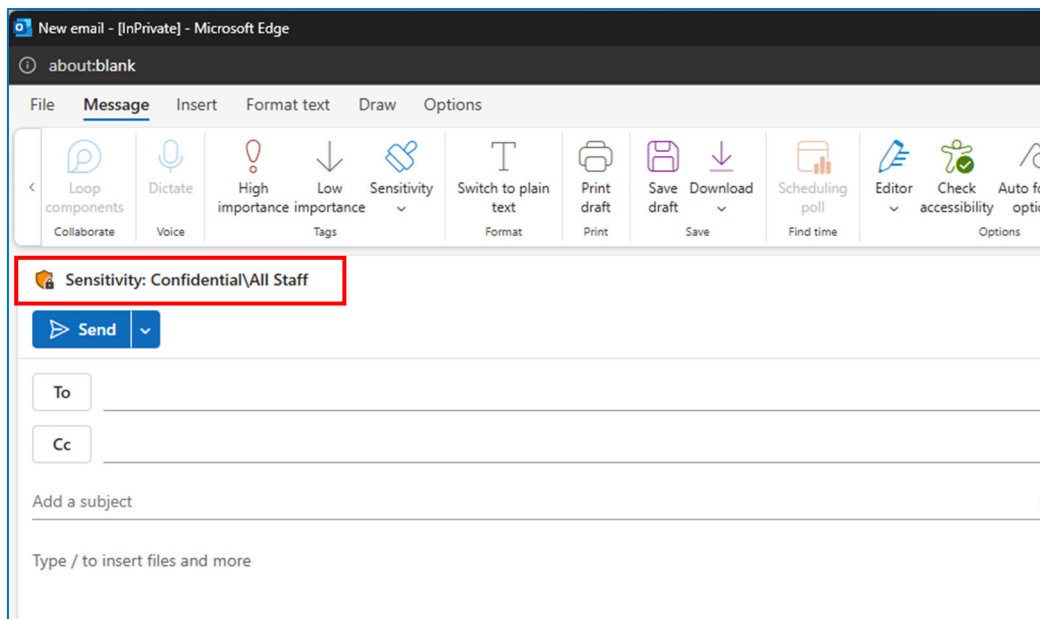
1. Login your O365 account in OWA, click **New message** icon for composing a new email:



2. In the New Email window, click **Sensitivity** button, then select the sensitivity label, e.g. **Confidential > All Staff**.



The information about the classification label chosen will be shown.

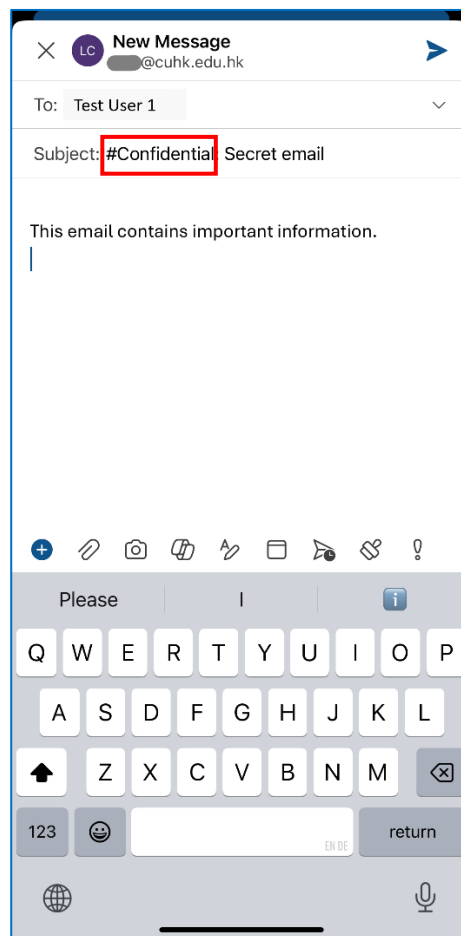


### 7.3. Send MIP-Protected Email with Subject Tag

You can include the following **tags** in the email subject to apply the same sensitivity labels as in MS Outlook.

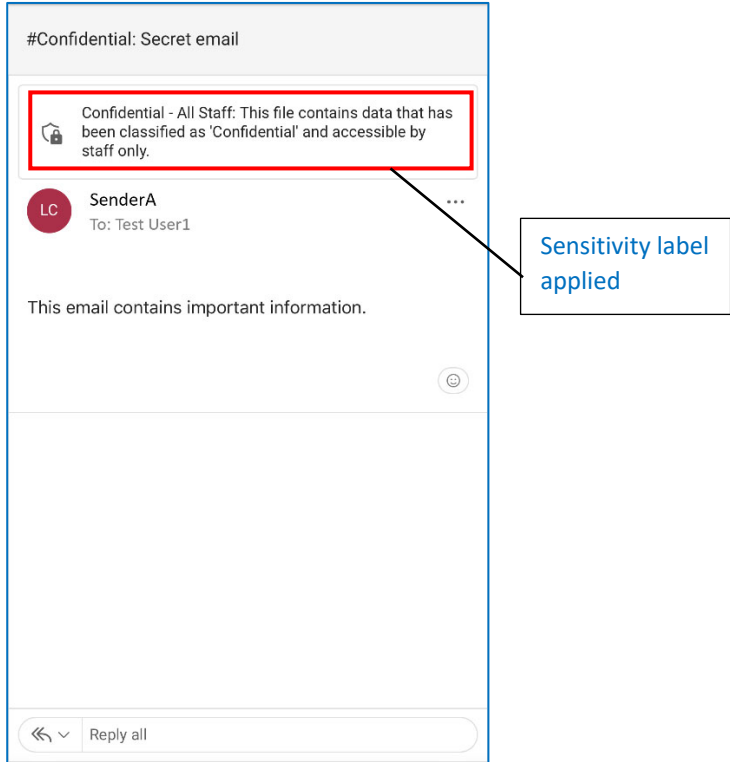
- Email subject with keyword “**#Confidential**”
  - o Apply permission control: Confidential – All CUHK Staff
- Email subject with keyword “**#StrictlyConfidential**”
  - o Apply permission control: Strictly Confidential – All CUHK Staff

For example, try to send an email with the email client in your mobile device, include with keyword “**#Confidential**” in the email subject.

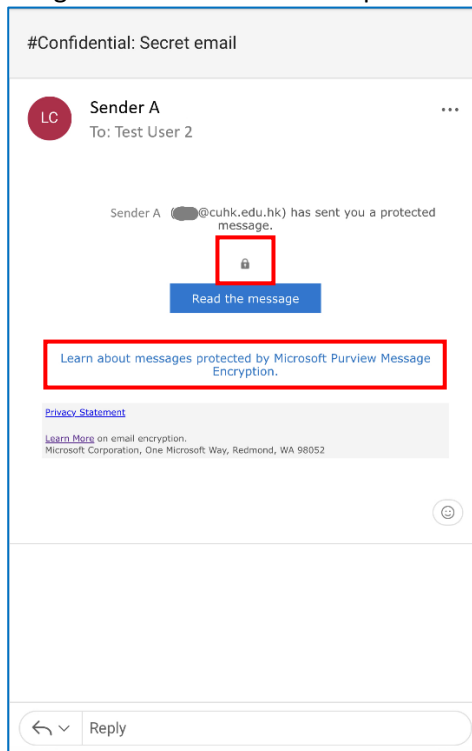


After the email is sent:

- i. **Authorized recipient** can open the email & see the sensitivity label applied.




- ii. If you are **unauthorized recipient**, the email content will be locked, you cannot open the email and below message about the email is MIP protected would be shown.

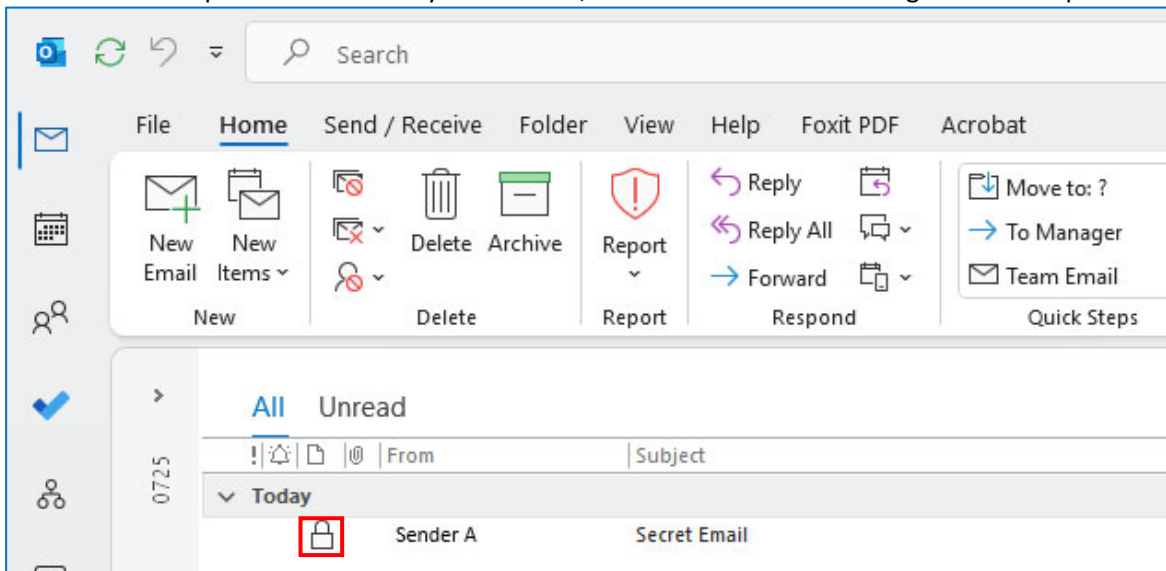


## 7.4. Read MIP-Protected Email

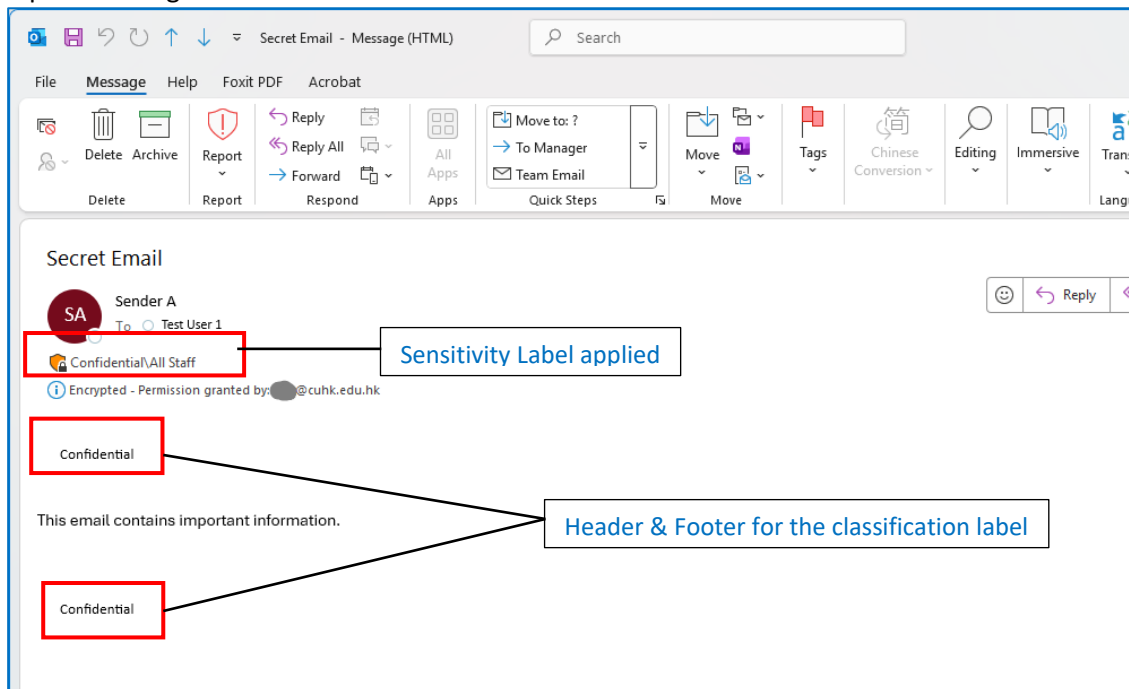
### 7.4.1. In MS Outlook for Windows

#### Steps:

1. Open MS Outlook.
2. Login with your CUHK Exchange account.
3. Locate the protected email in your mailbox, there is a  icon indicating the email is protected.



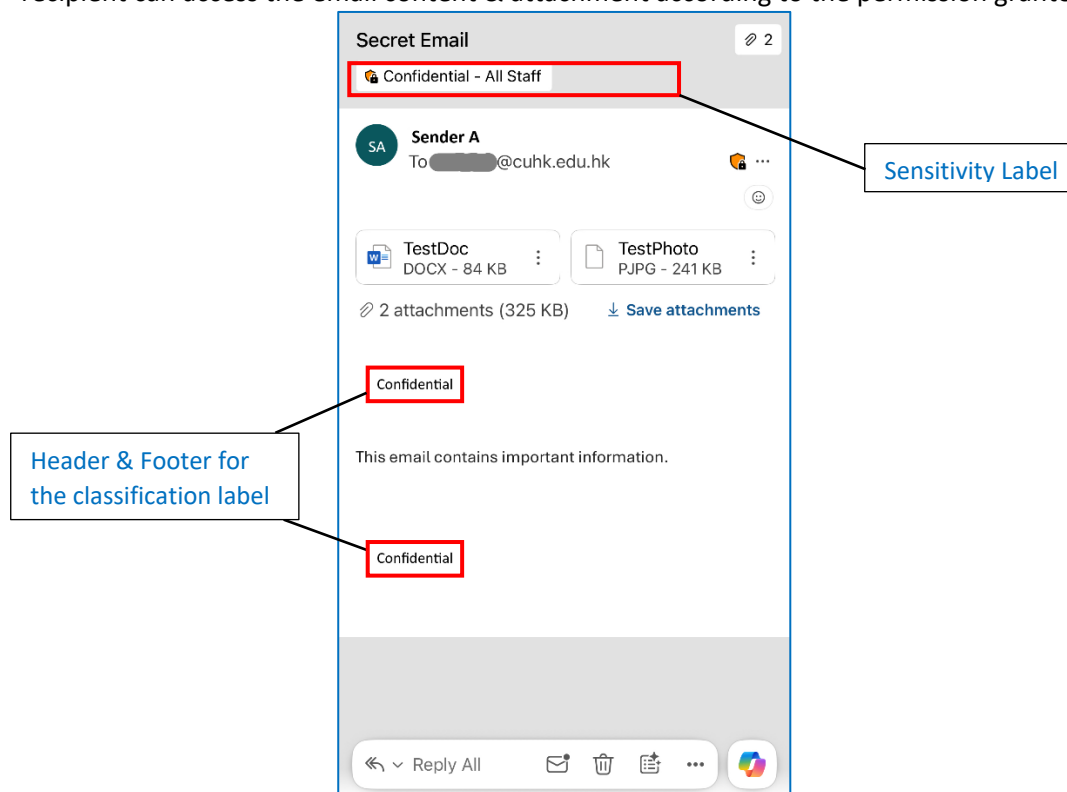
4. Open the protected email, you access the email content & attachment according to the permission granted.



## 7.4.2. In MS Outlook app for iOS and Android

### Steps:

1. Open MS Outlook.
2. Login with your CUHK O365 account.
3. Locate the protected email in your mailbox, and click on the email to view details. Authorized recipient can access the email content & attachment according to the permission granted.



4. To open the MIP-protected attachments in the email, please refer to Section 5.2.

## 8. File Protection in SharePoint Online & OneDrive

### 8.1. Create a MIP-Protected document in SharePoint Online & OneDrive

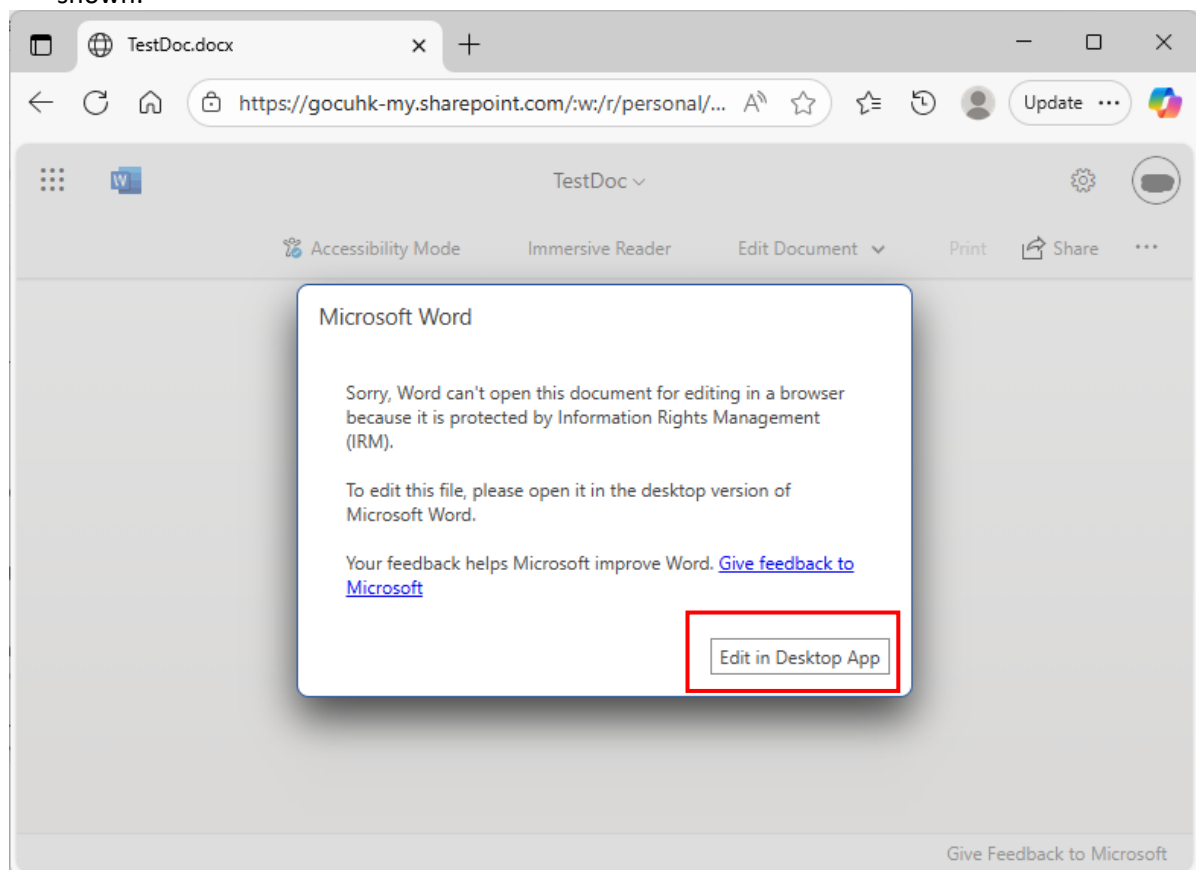
Currently, MIP is not integrated in MS SharePoint Online and OneDrive. However, you can upload a MIP protected file to these environment as usual, and the file should be protected in your local computer in advance. Detailed steps about File Protection can be found in Section 4.

### 8.2. Open a MIP-Protected document in SharePoint Online & OneDrive

MIP-Protected documents in SharePoint Online and OneDrive cannot be opened and edited directly with the Office Web App, error message would be shown.

#### Steps:

1. Open a protected Word document in SharePoint Online, the following message box will be shown:



2. Click **Edit in Desktop App** to launch the MS Word in your local computer and open the MIP-protected file.
3. If you have the permission to edit the file, you can edit and save the file as usual, the updated file would be saved in SharePoint or OneDrive.