

# Microsoft Information Protection (MIP) User Guide

Prepared By  
ITSC

Version: 5.0

*[Last update: Jan 2021]*

*[Initial version: Nov 2017]*

## Table of Contents

<b>1. About MIP.....</b>	<b>3</b>
<b>2. Client Installation .....</b>	<b>3</b>
2.1. Supported Environment.....	3
2.2. Download AIP Client Installation File.....	4
2.3. AIP Client Installation.....	4
2.4. Sign in for MIP Protection .....	6
<b>3. MIP Policy, Classification, Labeling and Protection.....</b>	<b>11</b>
3.1. Pre-defined Classification Labels and Permission Controls .....	11
3.2. Custom Permissions.....	12
<b>4. File Protection in Windows .....</b>	<b>13</b>
4.1. Create a Protected File with Classification .....	13
4.2. Create a Protected File with Custom Permission .....	16
4.3. Open a Protected file and View Permission.....	20
4.4. Change Classification and Protection .....	28
<b>5. Email Protection for O365 Email.....</b>	<b>32</b>
5.1. Send Protected Email with AIP Client .....	32
5.2. Send Protected Email with Subject Tag .....	39
5.3. Read Protected Email.....	41
<b>6. File Protection in SharePoint Online &amp; OneDrive .....</b>	<b>48</b>
6.1. Create a Protected document in SharePoint Online & OneDrive.....	48
6.2. Open a Protected document in SharePoint Online & OneDrive.....	48



## 1. About MIP

**Microsoft 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 Versions	Required applications	Operations can be done
Windows: - Win 10 - Win 8.1	- Office 365 ProPlus - Office Pro Plus 2019 - Office Pro Plus 2016	- Azure Information Protection client (v2.x)	- <b>Protect</b> MS Office files with <b>AIP toolbar</b> in Office applications - <b>Protect</b> non-MS Office files with <b>AIP client</b> - <b>Access</b> all protected files with Office applications (Office files) or AIP client (non-Office files)
Mac OS 10.9 or above	- Office 365 - Office 2019 for Mac	- RMS Sharing app 	- <b>Protect</b> MS Office files with <b>Sensitivity</b> button in Office applications - <b>Access</b> all protected files with Office applications (Office files) or AIP client (non-Office files)
	- Office 2016 for Mac		- <b>Access</b> all protected files with Office applications (Office files) or AIP client (non-Office files)
iOS 11.0 or above	- Latest Microsoft Office app	- Azure Information Protection apps (v2.x) 	- <b>Access</b> all protected files with Office applications (Office files) or AIP client (non-Office files)
Android OS 6.0 or above			

## 2.2. Download AIP Client Installation File

### For Windows:

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

For central deployment, you may download and extract the MSI file “AZInfoProtection\_UL\_MSI\_for\_central\_deployment.msi” at <https://www.microsoft.com/en-us/download/details.aspx?id=53018>.

### For Mac OS X:

Download the “RMS Sharing” app from App Store.


### For iOS and Android OS:

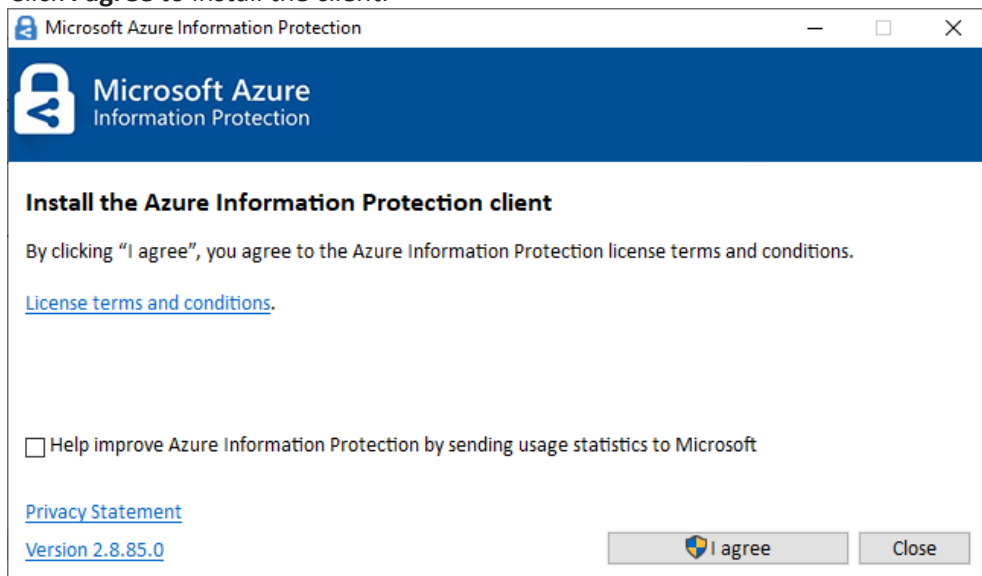
Download the “Azure Information Protection” app from Apple Store (iOS) and Google Play (Android OS).

## 2.3. AIP Client Installation

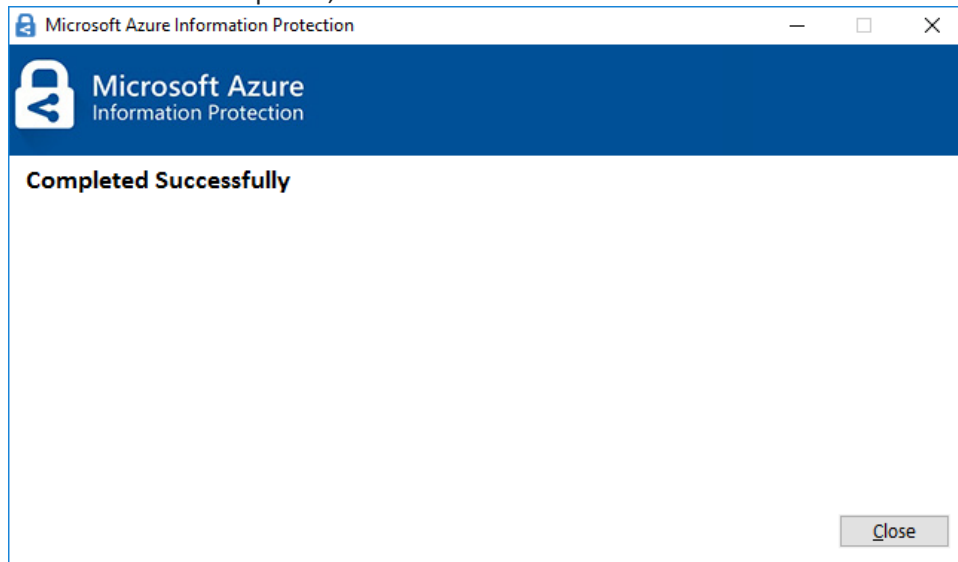
### 2.3.1. In Windows

#### Steps:

1. **Close all** Office applications and all instances of File Explorer.
2. **Double click** the installation file “AzInfoProtection\_UL.exe”.  AzInfoProtection\_UL.exe
3. Install the AIP Client:
  - 3.1. **Deselect** Help improve Azure Information Protection by sending usage statistics to Microsoft.
  - 3.2. Click **I agree** to install the client.



4. When the installation completes, click **Close**.



#### 2.3.2. In Mac OS X

**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 they will be installed automatically.

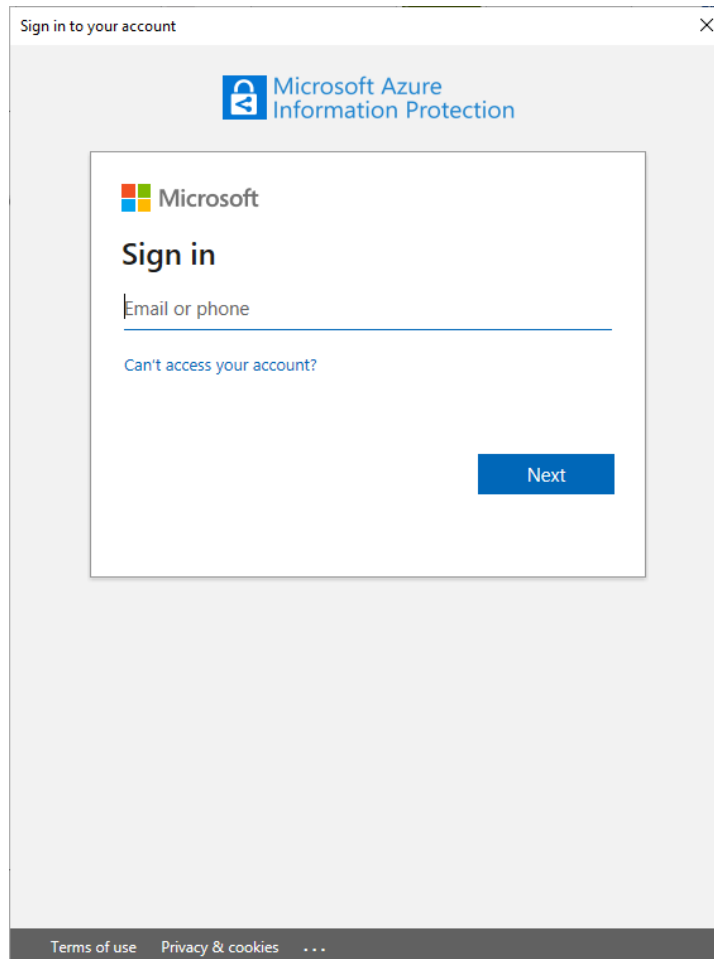
## 2.4. Sign in for MIP Protection

After the AIP Client is installed, please **sign in (i) AIP client and (ii) MS Office applications with your CUHK O365 account** in order to download the AIP policies for CUHK users.


### 2.4.1. Sign in AIP Client


#### Steps:

1. When you open any MS Office application, e.g. MS Word, the following screen to login Microsoft Azure Information Protection appears. **Sign in with your CUHK O365 account email address** and click **Next** button, then enter your **OnePass password** and click **Sign in** button.



Sign in to your account ✕

 Microsoft Azure  
Information Protection

 Microsoft

← test@cuhk.edu.hk

### Enter password

Password

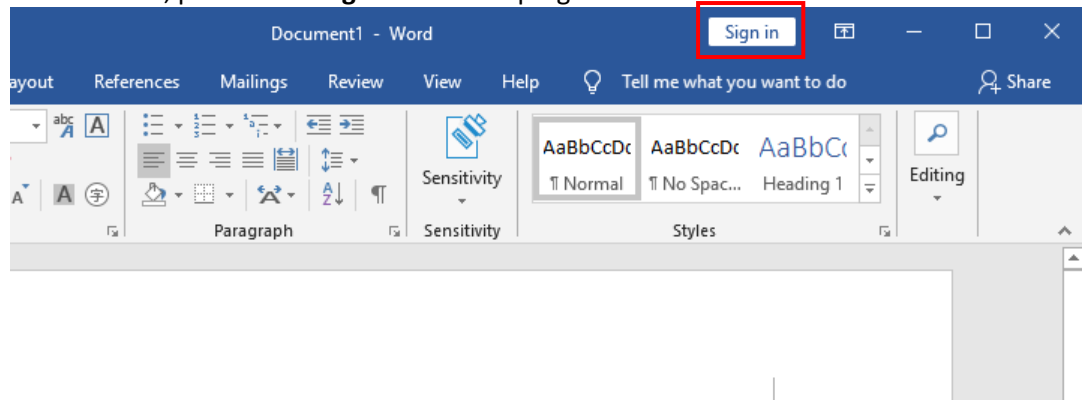
[Forgot my password](#)

[Terms of use](#) [Privacy & cookies](#) ...

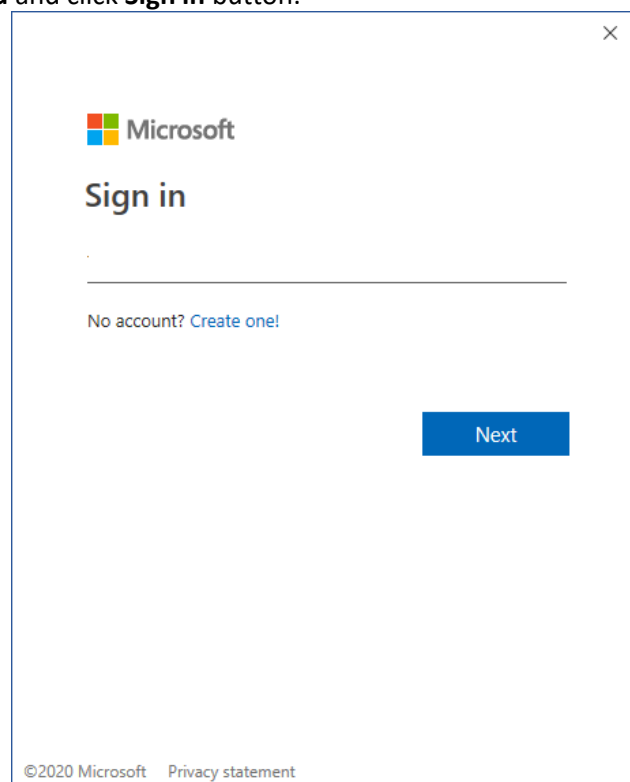
## 2.4.2. Sign in MS Office application

### Steps:

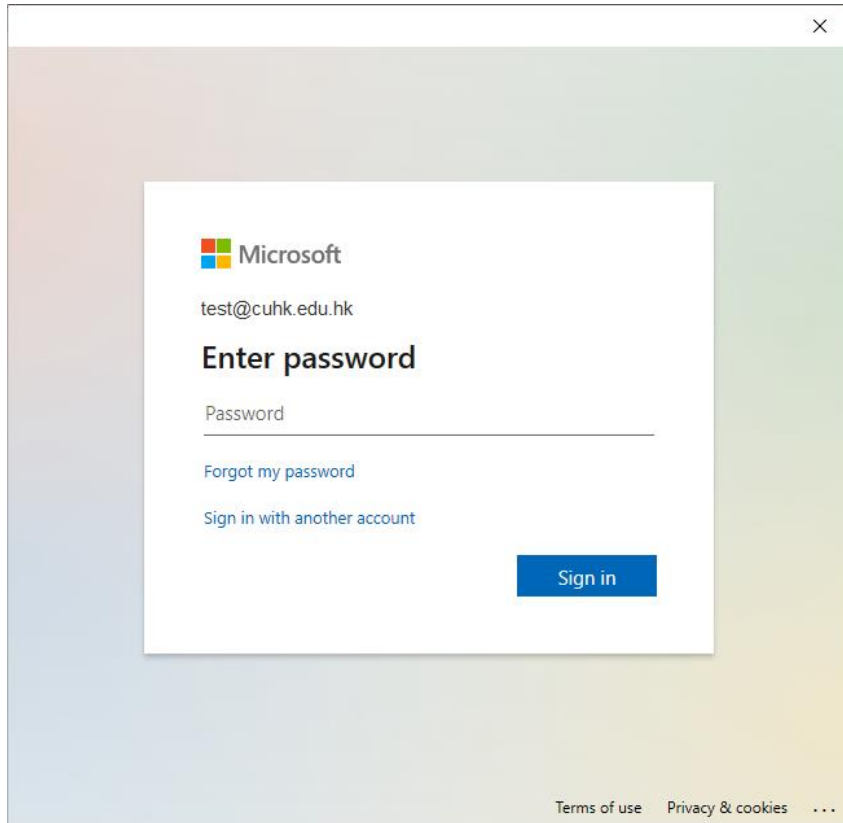
1. Start MS office application e.g. Word, Excel or PowerPoint, if you have not sign in your CUHK O365 account, please **click Sign in** on the top right hand corner.



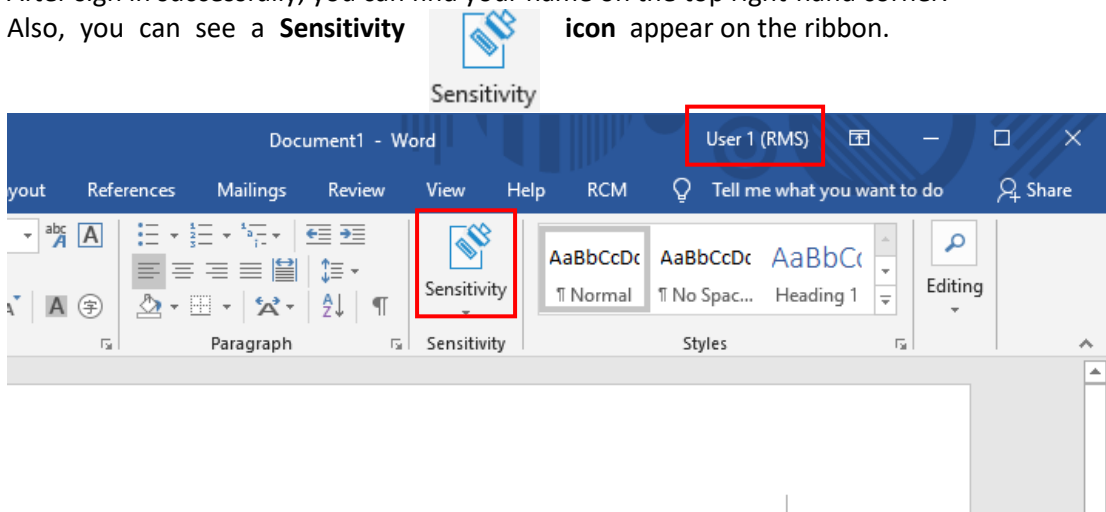
2. **Sign in with your CUHK O365 account email address** and click **Next** button, then enter your **OnePass password** and click **Sign in** button.



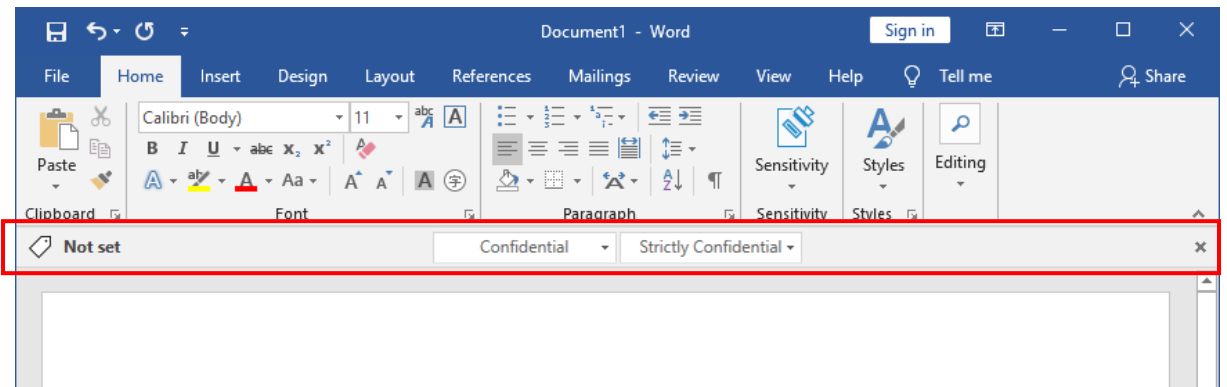
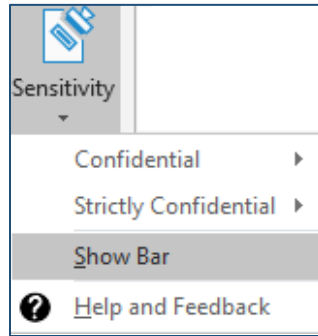




3. After sign in successfully, you can find your name on the top right-hand corner. Also, you can see a **Sensitivity** icon appear on the ribbon.



2. Click the **Sensitivity icon** and select **Show Bar**, then a new AIP bar is shown.



You can use it to label and protect your documents if necessary.

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

3 default settings in the MIP policy are configured:

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

When you are going to protect your documents, you can either use:

1. the pre-defined classification labels with permission controls
2. the custom permission which allows more flexibility for selecting the authorized persons, permissions and expiry date.

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

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

Classification	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

T

### 3.2. Custom Permissions

If it is not applicable to use the pre-defined classification labels in Section 3.1, you can use the custom permissions by assigning the appropriate user role:

User Role	Operations for authorized person	Permissions Granted							
		View	Edit, Save	Save As, Export	Copy	Print	Reply, Reply All	Forward	Full Control
<b>Viewer</b>	View the protected file only	Y					Y		
<b>Reviewer</b>	View and edit the protected file only	Y	Y				Y	Y	
<b>Co-Author</b>	All permissions as the document owner except changing the permissions	Y	Y	Y	Y	Y	Y	Y	
<b>Co-Owner</b>	Full control as the document owner	Y	Y	Y	Y	Y	Y	Y	Y

Also, you can freely select different individuals or groups of users who can access to the file, and define the expiry date as well.

## 4. File Protection in Windows

### 4.1. Create a Protected File with Classification

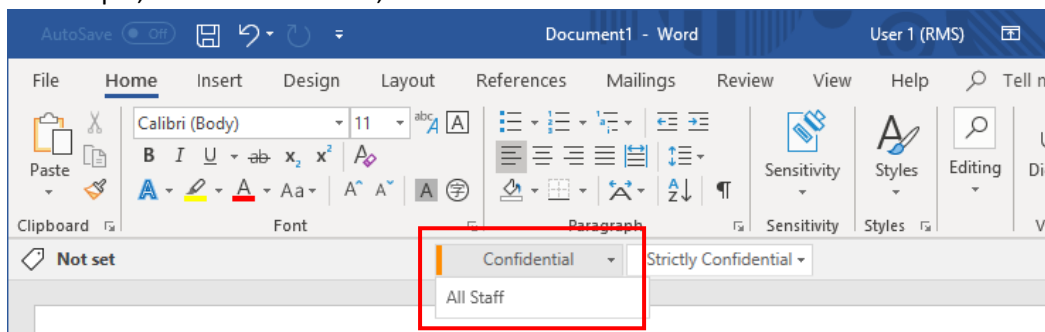
After AIP client is installed, and signed-in your CUHK O365 account, you can start to label and protect (with encryption) your files if necessary. However, the labeling and protection steps on MS Office files (i.e. Word, Excel & PowerPoint) and non-MS Office files are different.

#### 4.1.1. For MS Office Files

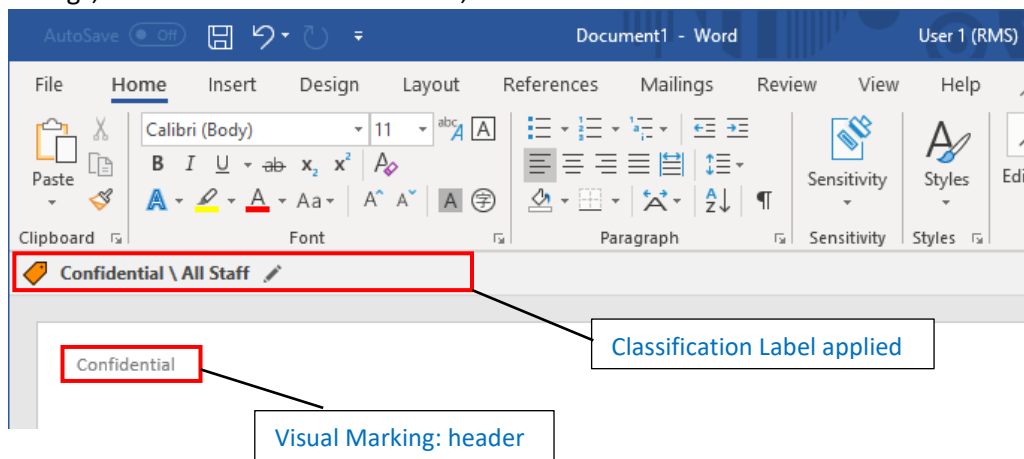
**Steps:** (The following steps can be applied to MS Excel & PowerPoint as well)

1. Open MS Word, on the Information Protection toolbar, select an appropriate classification label to classify and protect the document with pre-defined permissions.

For example, select **Confidential**, then **Confidential – All Staff**.



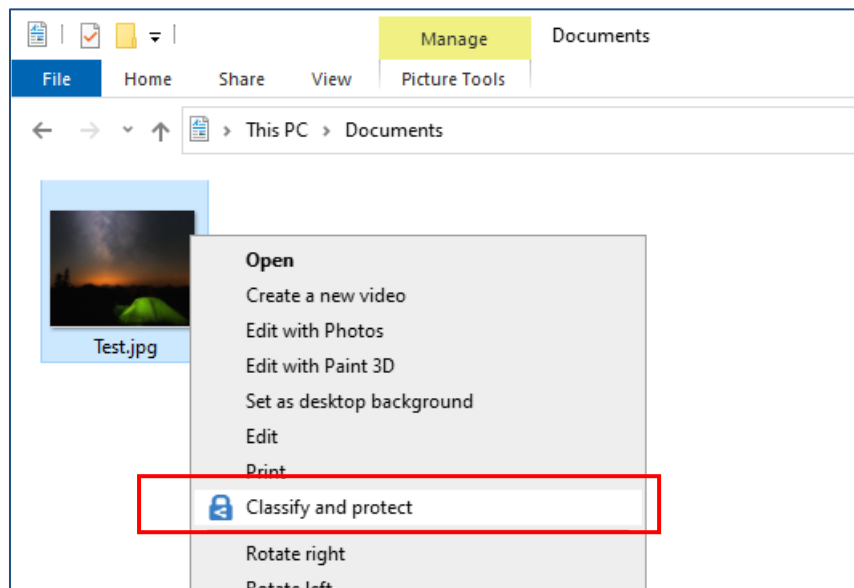
2. After the classification, you can see the sensitivity has changed to “Confidential” and visual markings, header and footer in this case, also indicate the current classification level.



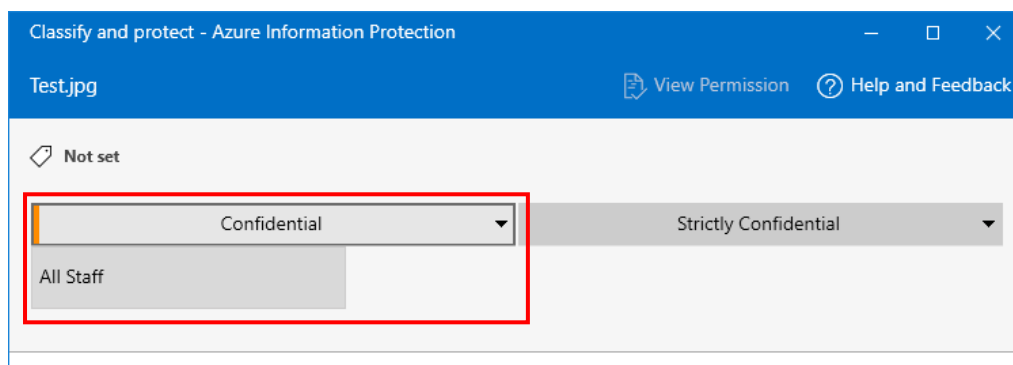
#### 4.1.2. For Non-MS Office Files

##### Steps:

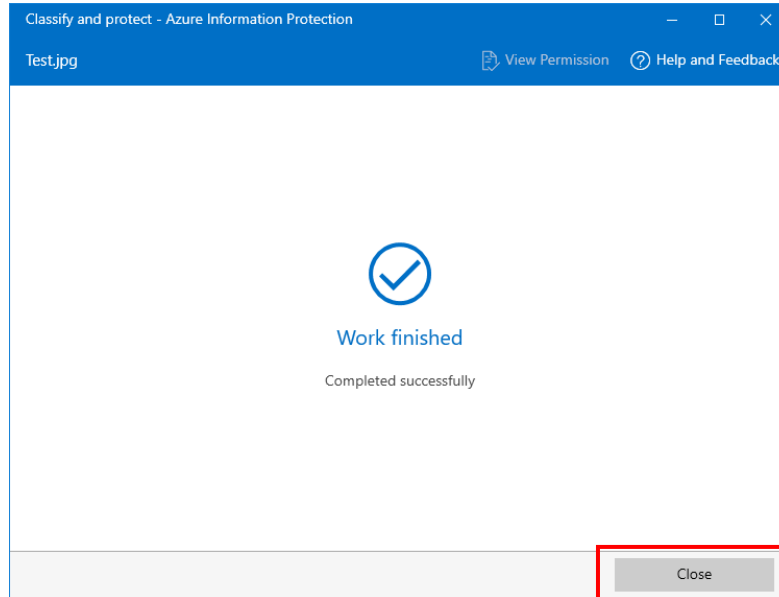
1. Select a non-MS Office file, e.g. jpg, txt or pdf file, right click and select “**Classify and protect**” on the context menu.




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

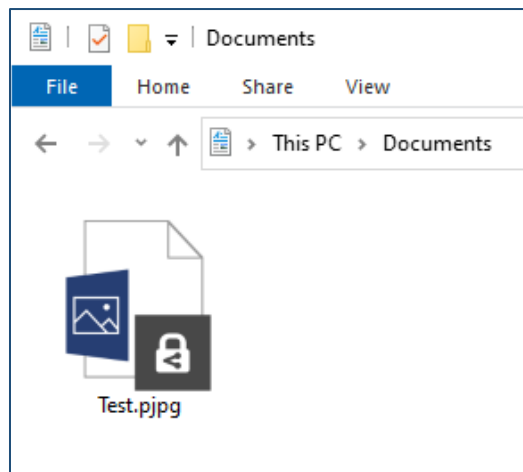


3. Click **Close** button to close the window.



4. After the classification is applied, the file format has changed to an AIP protected file format. You can see a  on the file icon which indicates that the file is AIP protected.

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



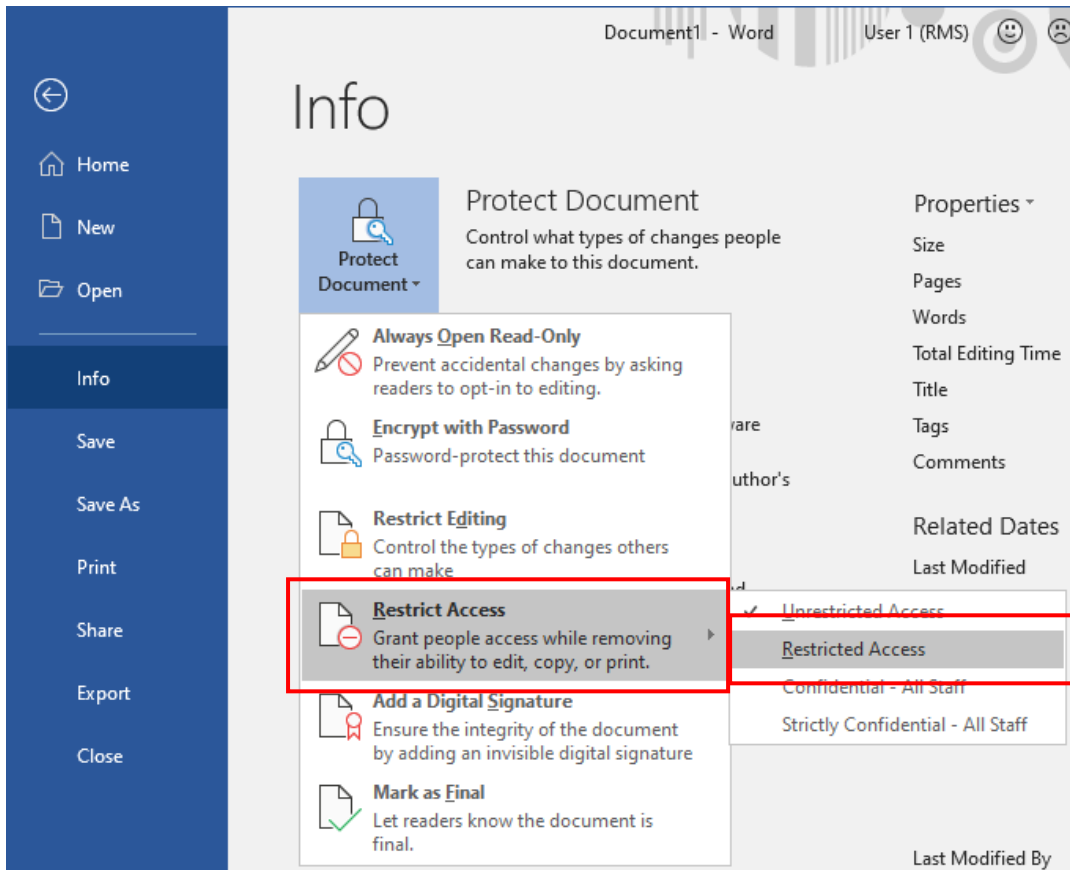
## 4.2. Create a Protected File with Custom Permission

If the pre-defined classification labels are not suitable, you may apply custom permissions.

### 4.2.1. For MS Office File

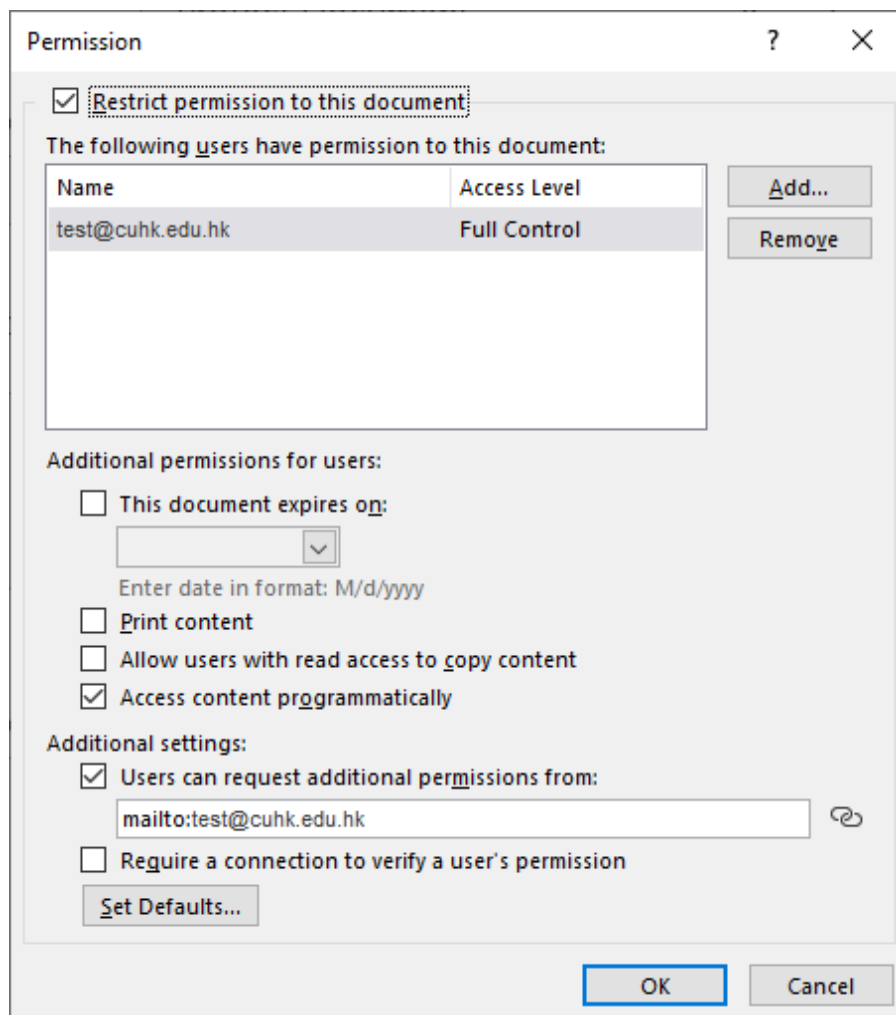
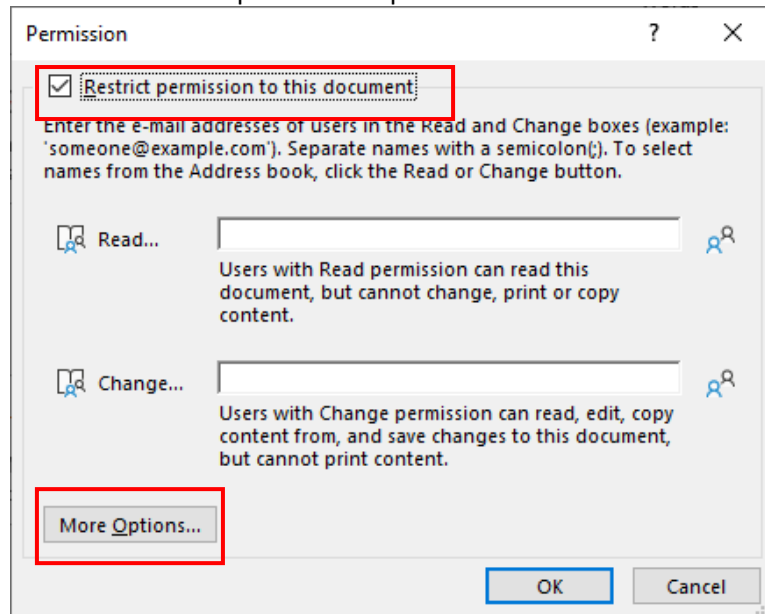
#### Steps:

1. Click **File > Info > Protect Document > Restrict Access > Restricted Access.**





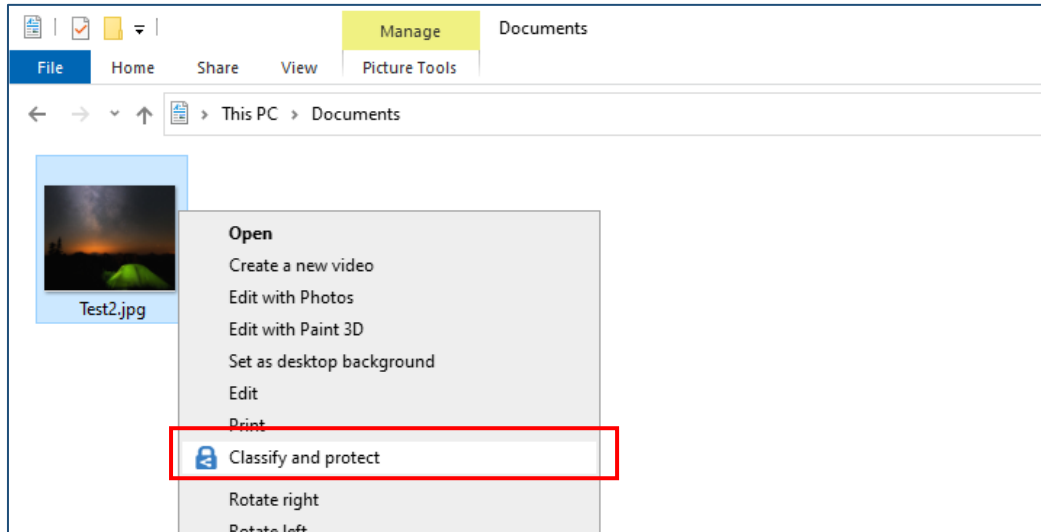
2. A custom permission window open, check the box “**Restrict permission to this document**”, then you can grant different permissions to different persons. You can click “**More Options...**” button to find more permission options.



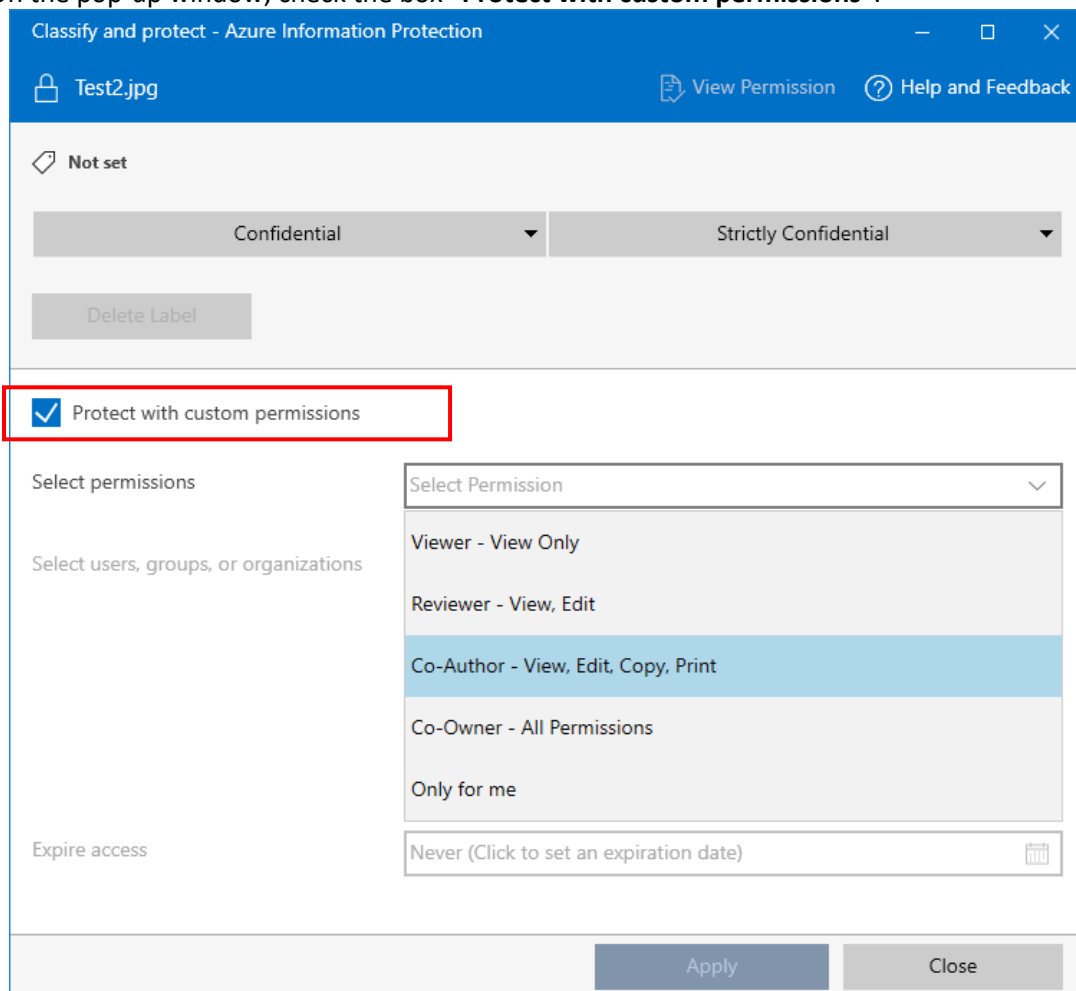
#### 4.2.2. For MS-Office & Non-MS Office File

##### Steps:

1. Select a file, e.g. jpg, pdf or MS Office file, right click and select **“Classify and protect”** on the context menu.



2. On the pop-up window, check the box **“Protect with custom permissions”**.



3. Select an appropriate **permission**, there are 5 types of permission available. Details about the permissions can be found in Section 3.2 .

Select **user**, from the Global Address List or type in the email address directly.

Select the date for **expire access**, if necessary.

Then, click “**Apply**” button to confirm the protection settings.

Classify and protect - Azure Information Protection

Test2.jpg View Permission Help and Feedback

Not set

Confidential Strictly Confidential

Delete Label

Protect with custom permissions

Select permissions: Co-Author - View, Edit, Copy, Print

Select users, groups, or organizations: chantaiman@cuhk.edu.hk

Expire access: Never (Click to set an expiration date)

Apply Close

Su	Mo	Tu	We	Th	Fr	Sa
			30	31	1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30
31	1	2	3	4	5	6

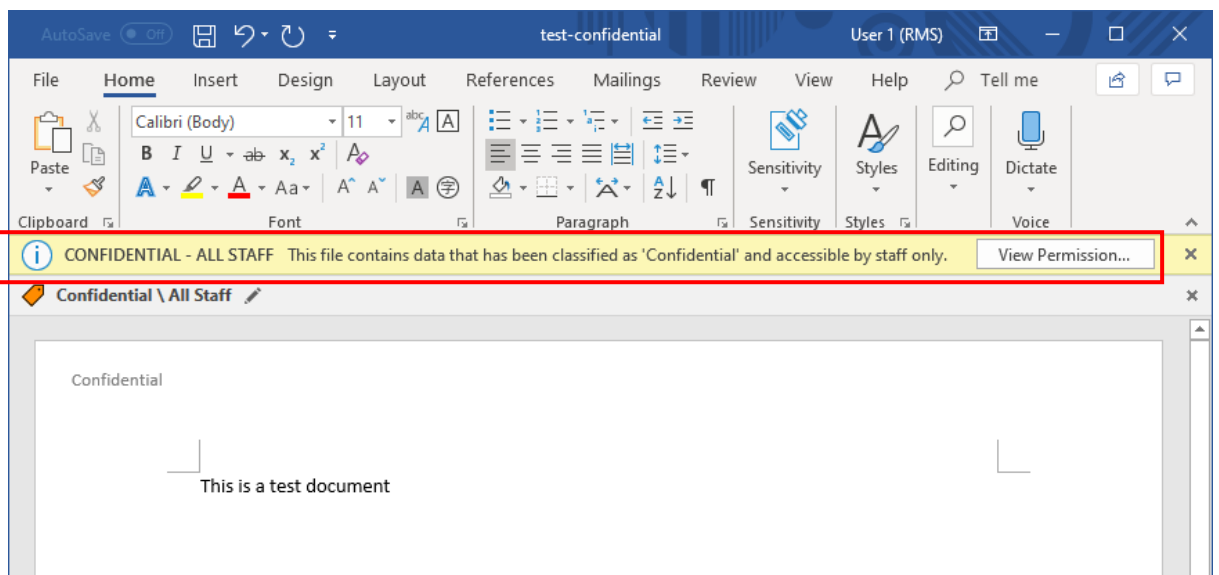
## 4.3. Open a Protected file and View Permission

### 4.3.1. In Windows

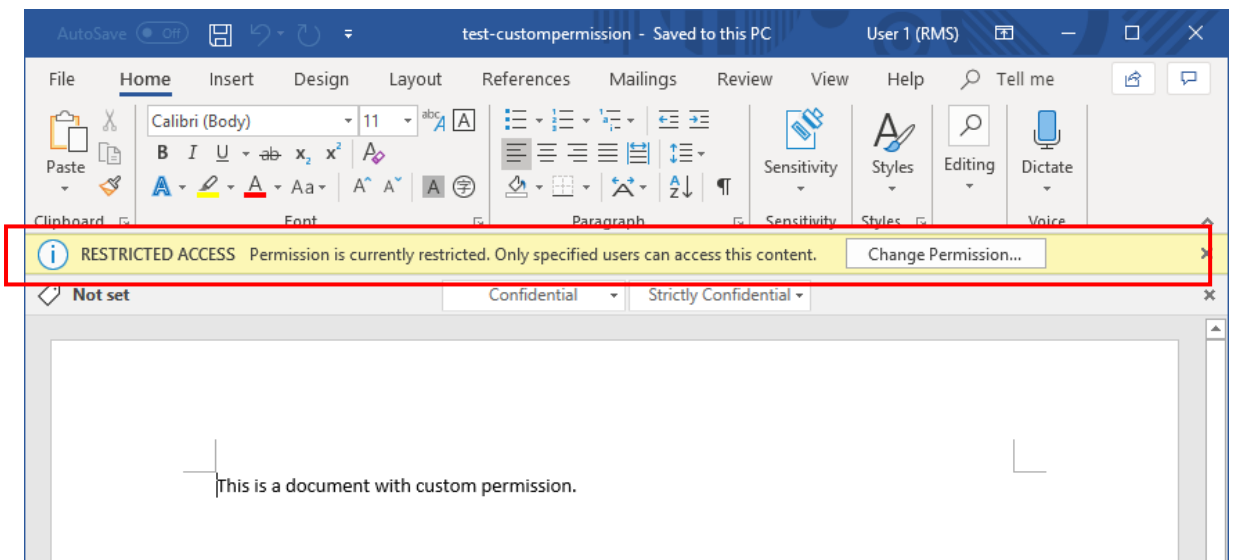
#### 4.3.1.1. View a Protected MS Office File

##### Steps:

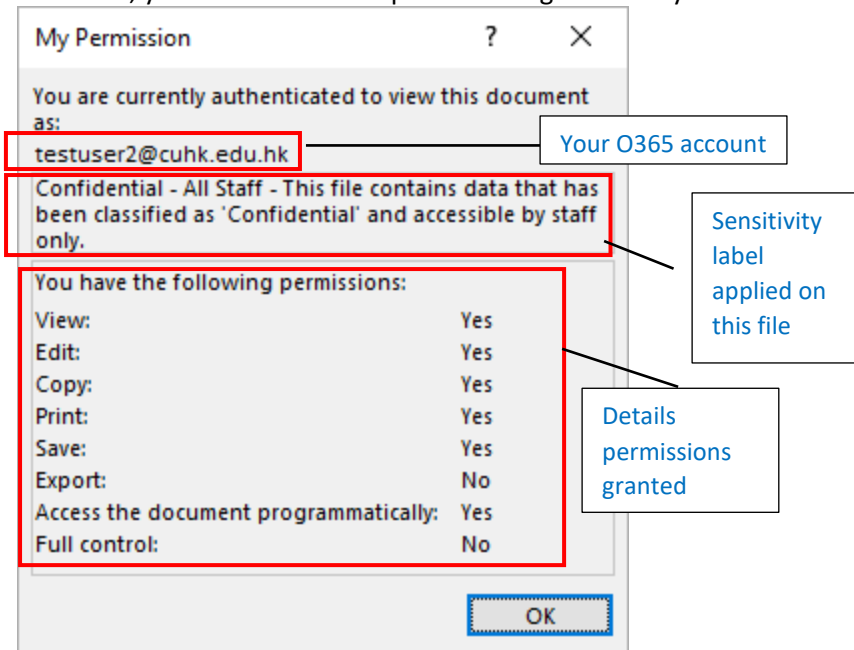
1. To access an AIP-protected MS Office file that granted the access to you, please make sure you have **signed-in your CUHK O365 account** in the Office application.
2. Open the protected file, an information bar indicating the sensitivity level (confidential, or strictly confidential) and the permission of the file would be shown.



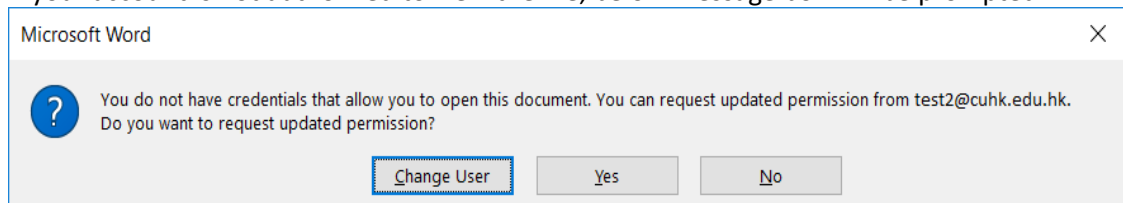
If the file is protected with custom permissions, information about 'only specified users can access' and other information would be shown.



3. Click **View Permission** button, you can view details permissions granted to you.



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

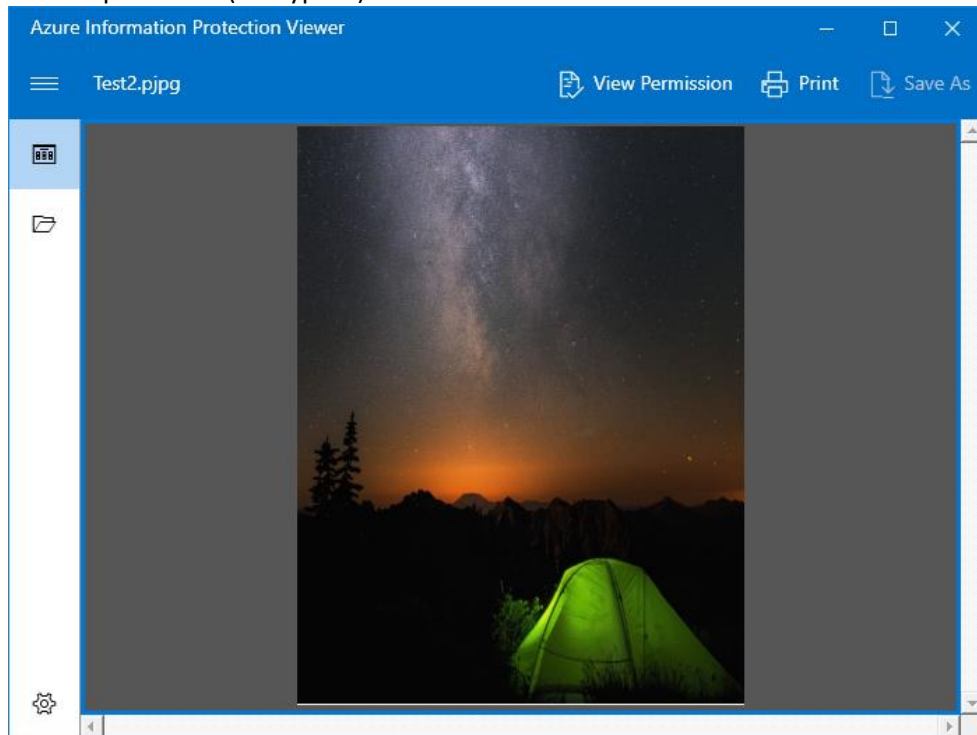


#### 4.3.1.2. View a Protected Non-MS Office File

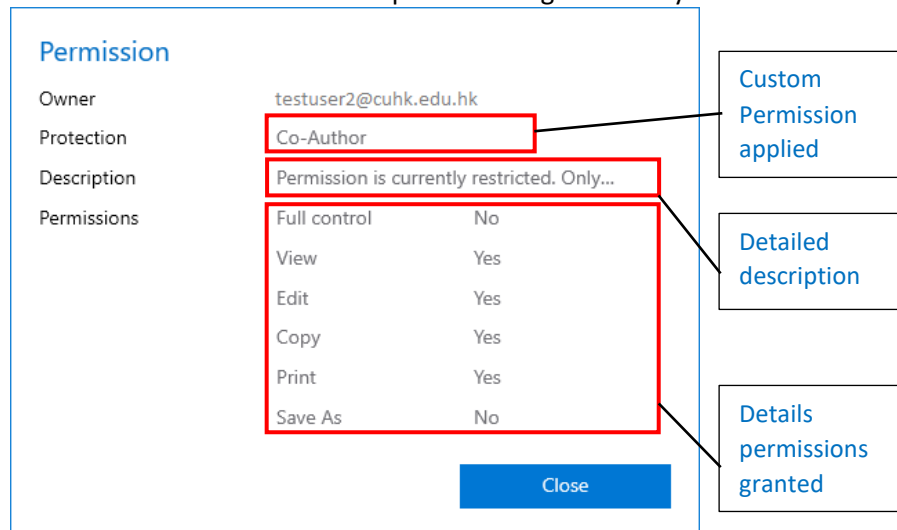
You need to have the Azure Information Protection Client installed before you can open a protected non-MS Office file.

#### Steps:

1. Double click to open the protected non-MS Office file, e.g. \*.jpg or \*.pdf, it will launch the Azure Information Protection Viewer automatically which allow you see the content inside the protected (encrypted) file.



2. Click "View Permission" button to view details permissions granted to you.



**Permission**

Owner: testuser2@cuhk.edu.hk

Protection: Co-Author

Description: Permission is currently restricted. Only...

Permissions:

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

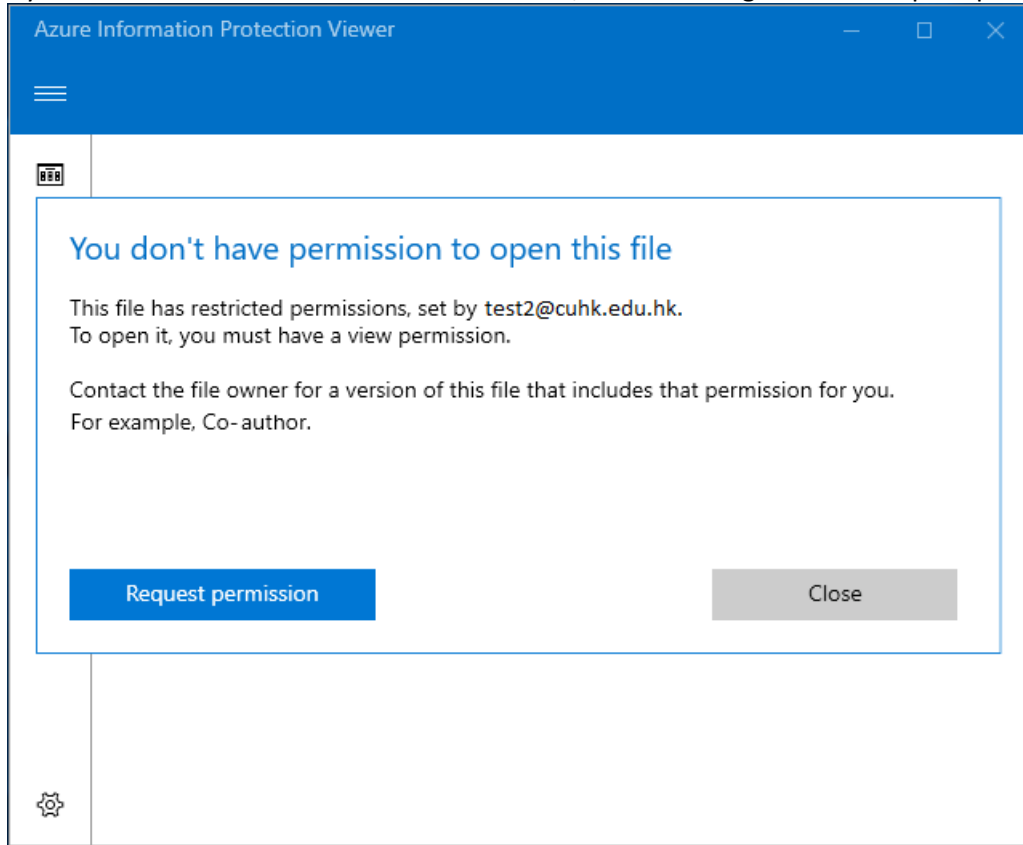
Close

Custom Permission applied

Detailed description

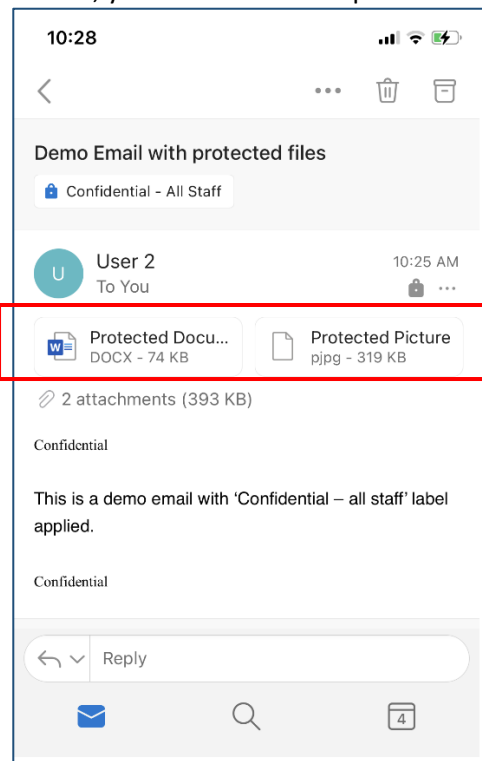
Details permissions granted

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



### 4.3.2. In iOS & Android

Most probably, in mobile platforms, you would receive a protected file via emails.



In order to open the protected file, you need to download and install the following apps in your mobile in advance (as mentioned in Sec 2.1):

Microsoft Word, Excel, and PowerPoint apps for opening MS Office files



AIP Viewer app for opening non-MS Office files



After the above apps are installed, **login these apps with your O365 account** for authentication and authorization checking when you open any protected files.

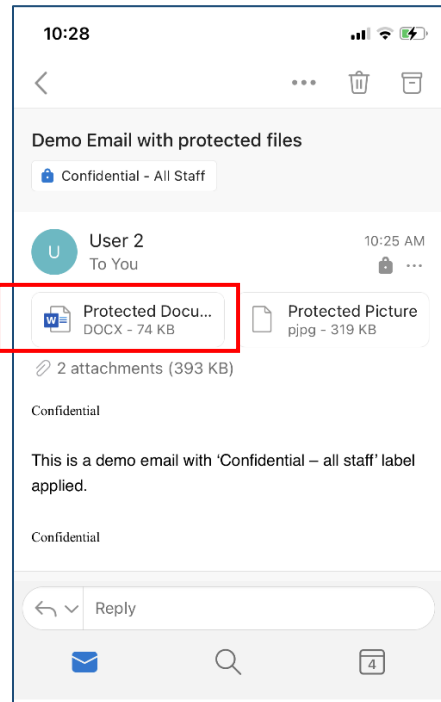


#### 4.3.2.1. Open the Protected Word file (MS Office file)

##### Steps:

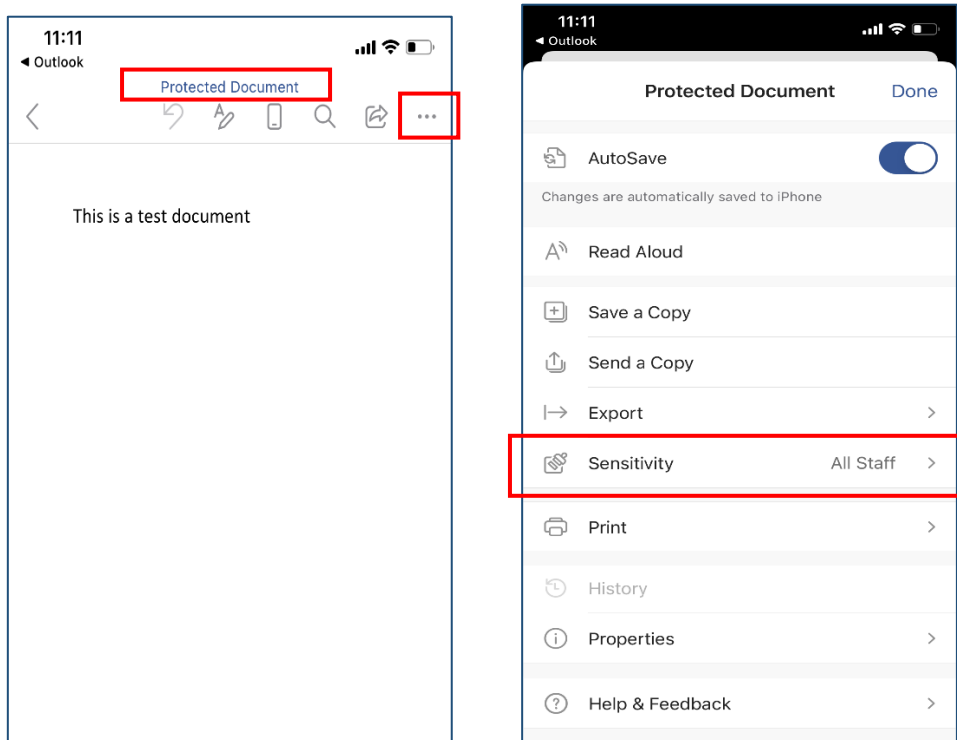
[Take iOS as an example, you can apply similar steps in Android OS.]

1. Click on the MS Word attachment in the email.



2. If the file access is granted to you, and you had login your O365 account, it will open the Word app automatically and open the protected word file.

Click on  icon, you can check the Sensitivity label applied on this document.

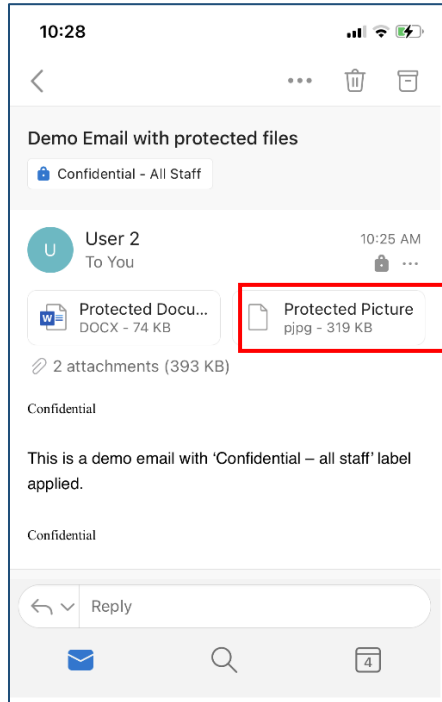



#### 4.3.2.2. Open the protected JPG file (non-Office file)

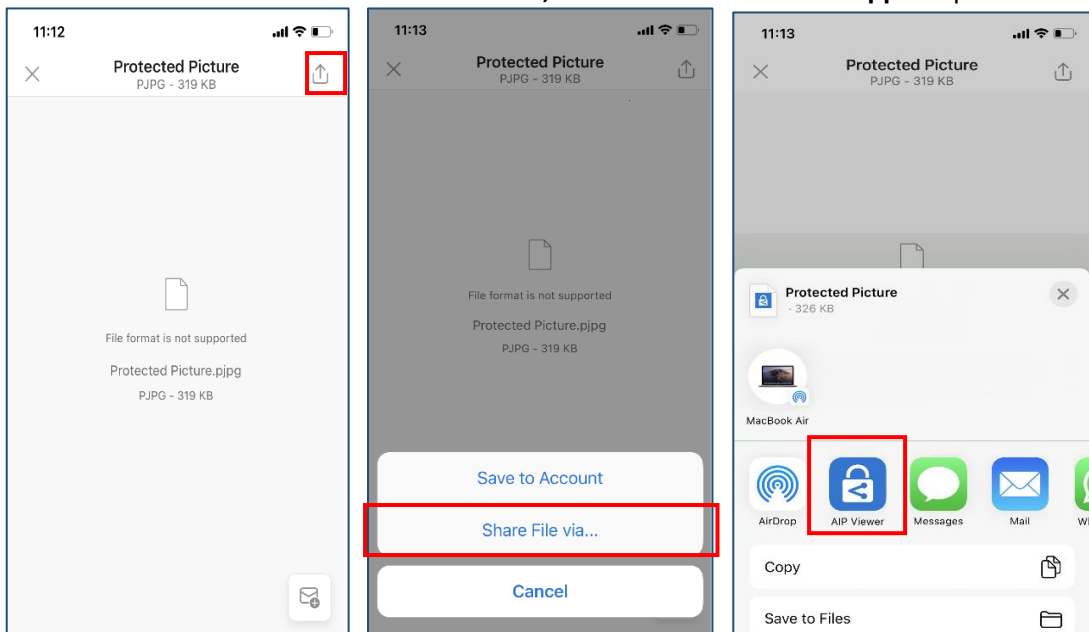
##### Steps:

[Take iOS as an example, you can apply similar steps in Android OS.]

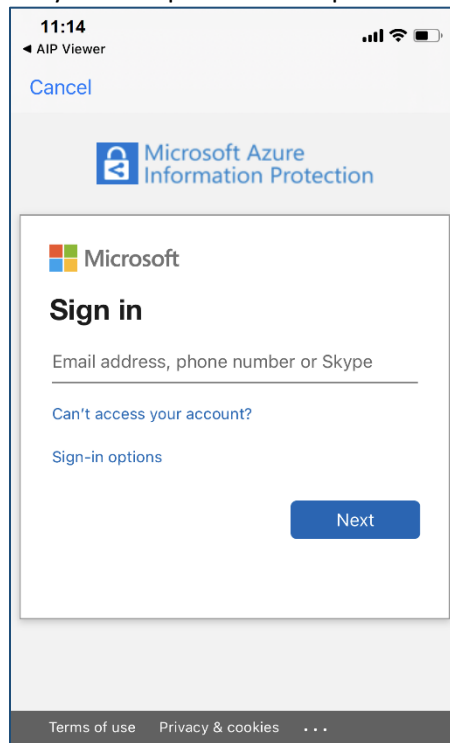
1. Click on the file JPG attachment in the email.




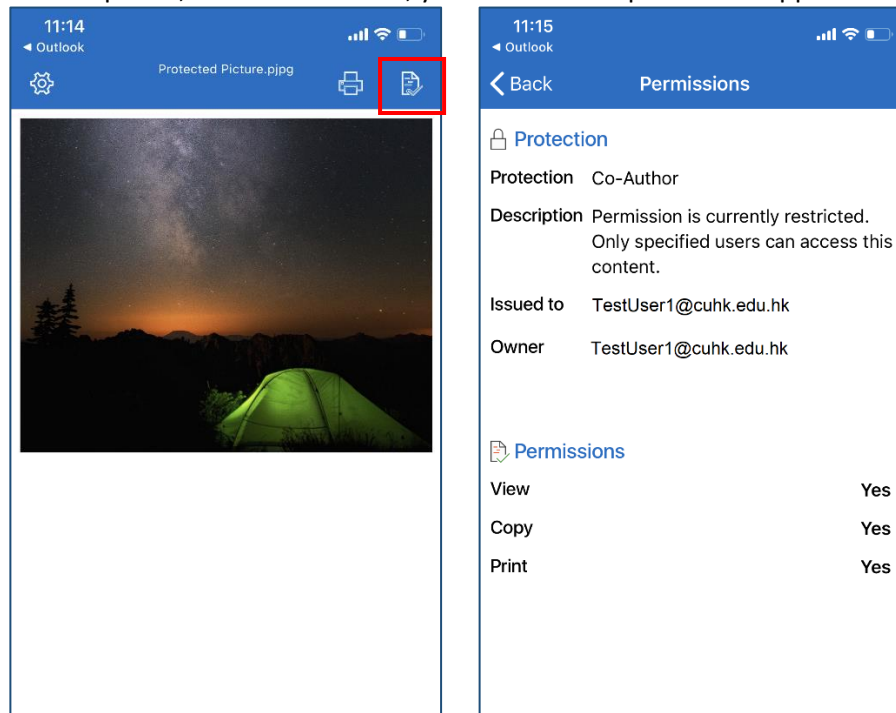
2. Click on the  icon and click **Share File via...**, then choose **AIP Viewer app** to open the file.



3. If you have not sign 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.



4. After the file is opened, click on  icon, you can view the permission applied on this file.



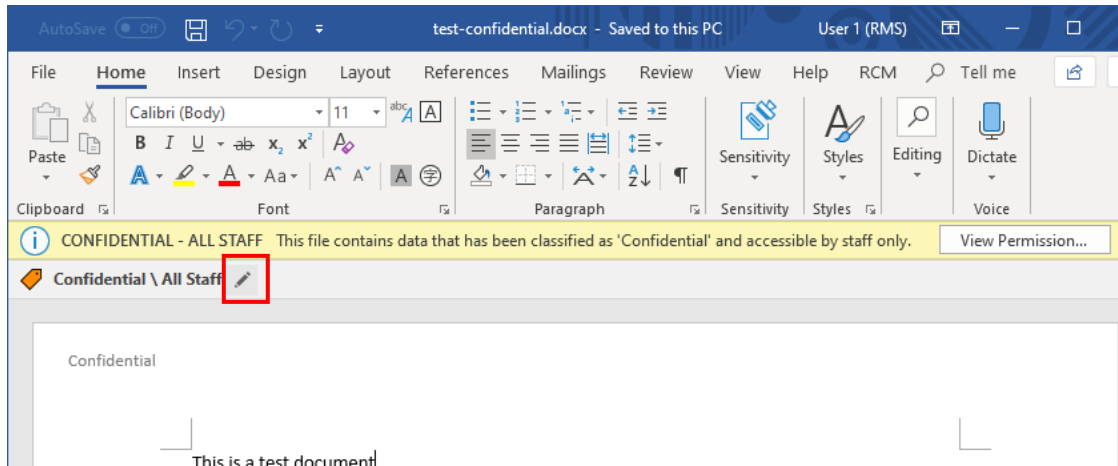
## 4.4. Change Classification and Protection

Please note that only the file owner can change the classification or permission of a protected file.

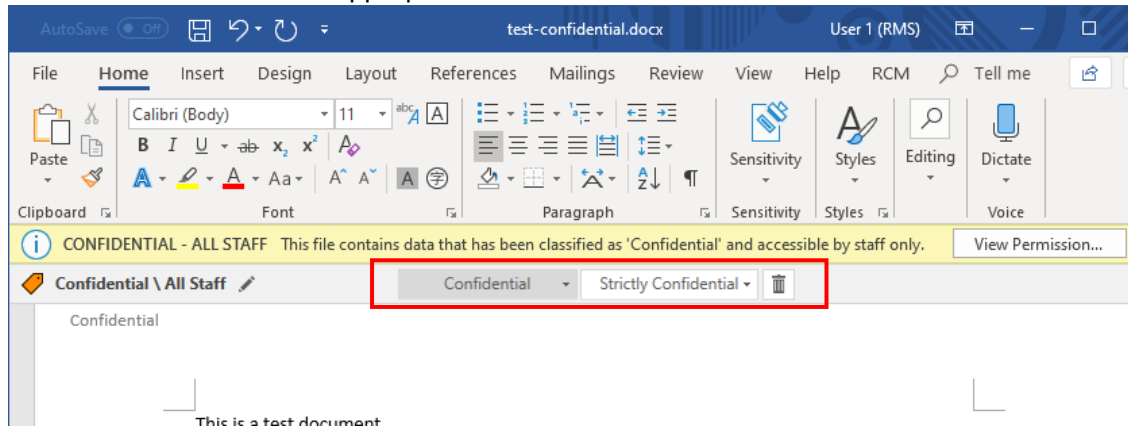
### 4.4.1. For MS Office File

#### Steps:

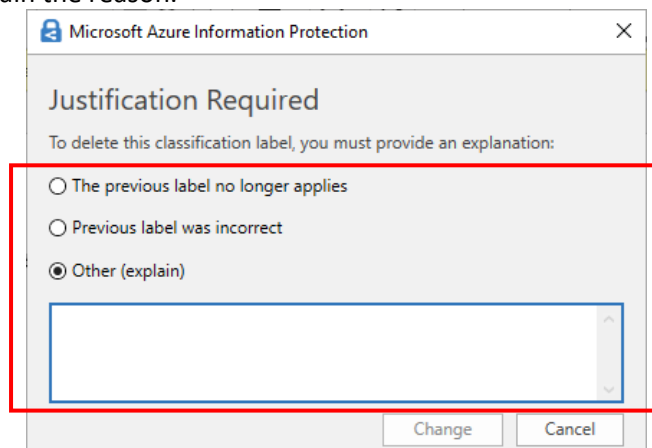
1. Click the **Edit Label** icon to edit classification label.



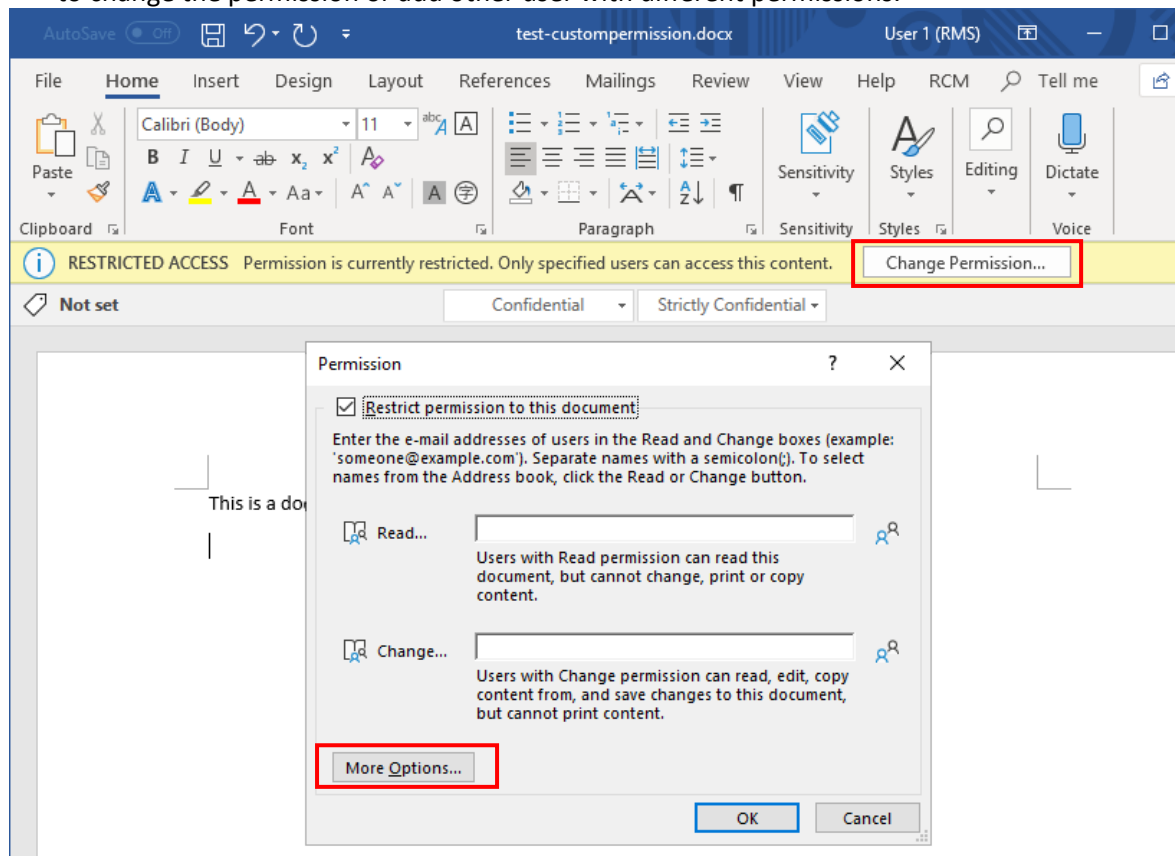
2. You can select another appropriate label or delete current selected label:



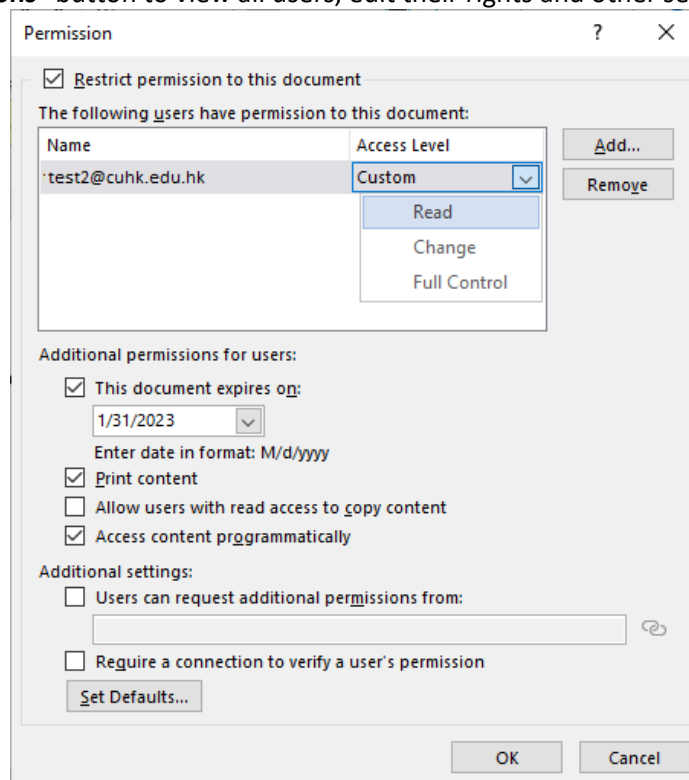
3. If delete a classification label, or change the label to a lower level, you need to provide the justification to explain the reason.



- If a custom permission was applied on the document, you can click **Change Permission** button to change the permission or add other user with different permissions.



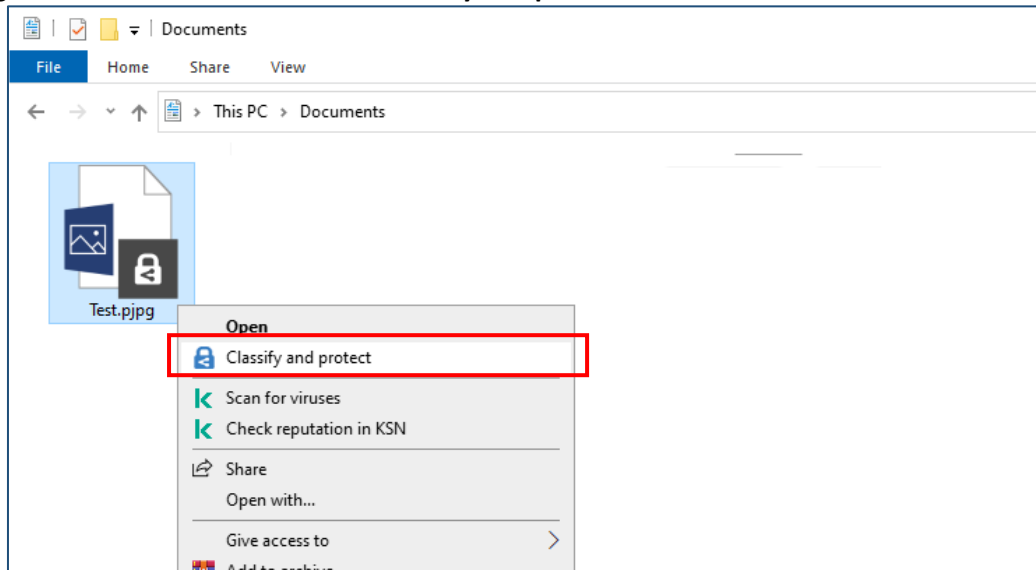
- Click **More Options** button to view all users, edit their rights and other settings.



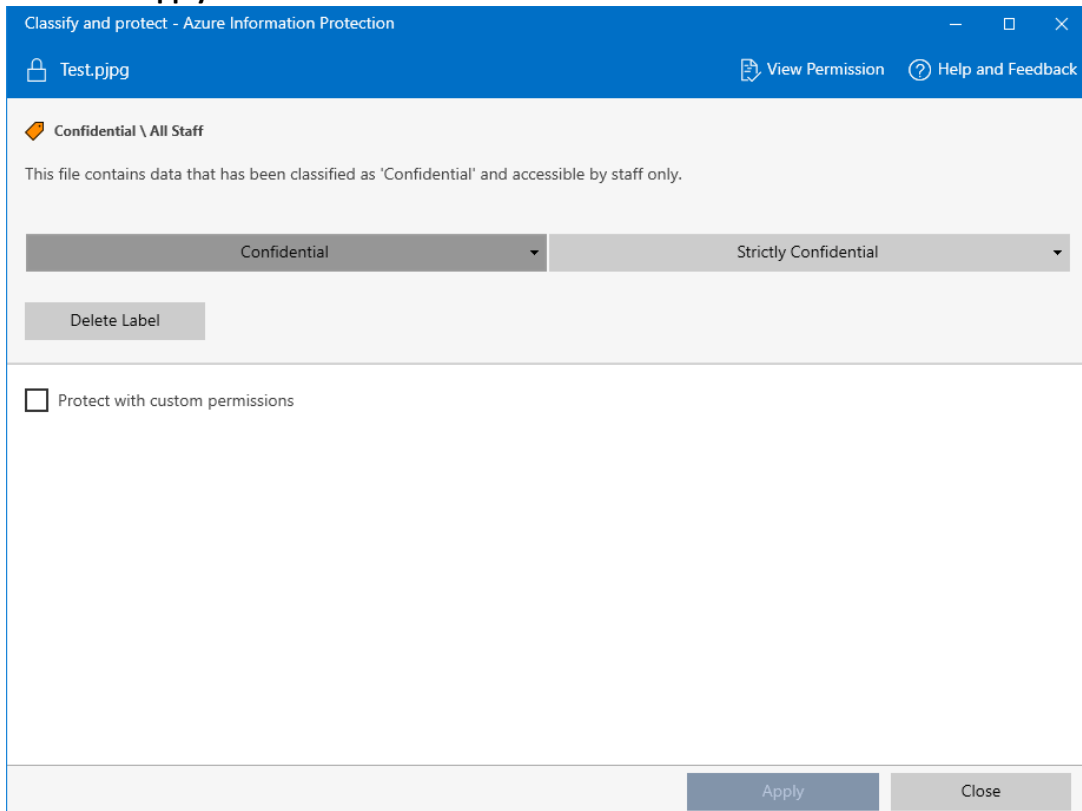
#### 4.4.2. For Non-MS Office File

##### 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.

Classify and protect - Azure Information Protection

Test.pjpg View Permission Help and Feedback

To delete this classification label, you must provide an explanation:

- The previous label no longer applies
- Previous label was incorrect
- Other (explain)

Confirm Back

## 5. Email Protection for O365 Email

### 5.1. Send Protected Email with AIP Client

As the AIP is integrated with the MS Exchange Online, users of the Exchange servers which had been joined to the CUHK University AD can use the AIP to protect their emails.

#### Prerequisites:

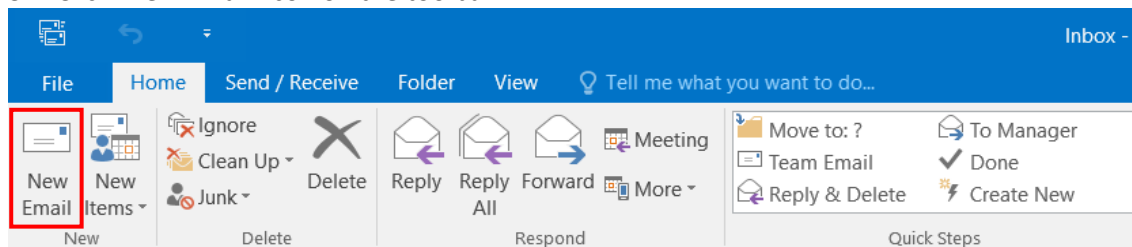
- Departmental Exchange server joined to the University AD
- Client PC installed AIP Client (refer to Section 2.3.1)

#### 5.1.1. In MS Outlook 2016, 2019, Office 365

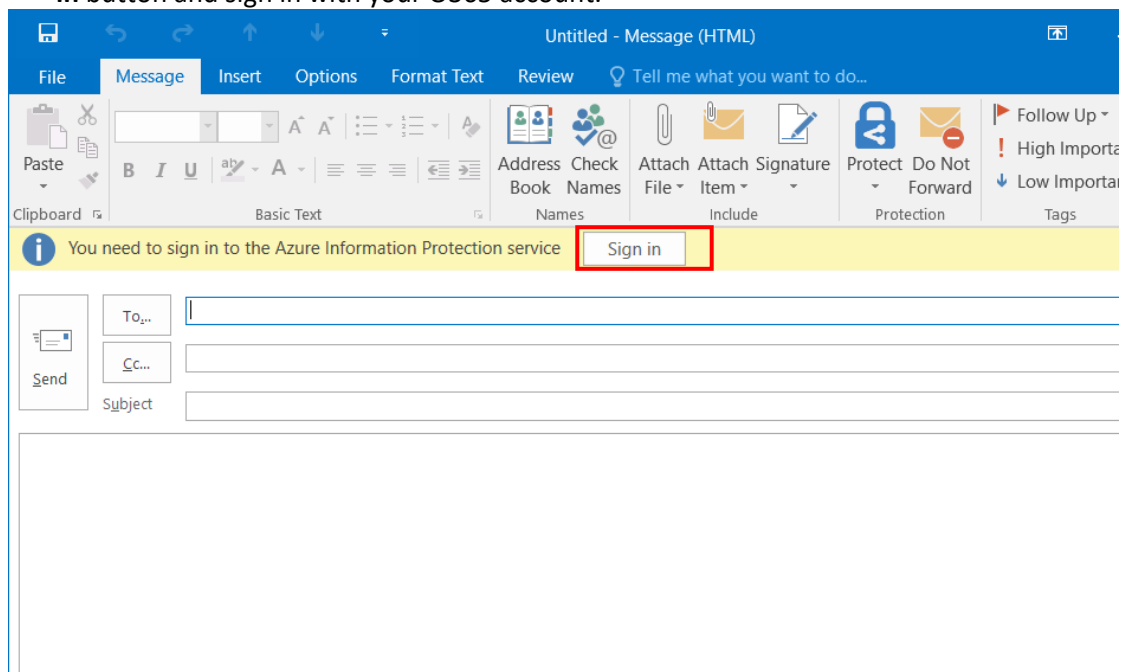
##### 5.1.1.1. Activate AIP Protection in MS Outlook for Windows

#### Steps:

1. Open MS Outlook.
2. Login with your CUHK Exchange account.
3. Click 'New Email' icon on the toolbar

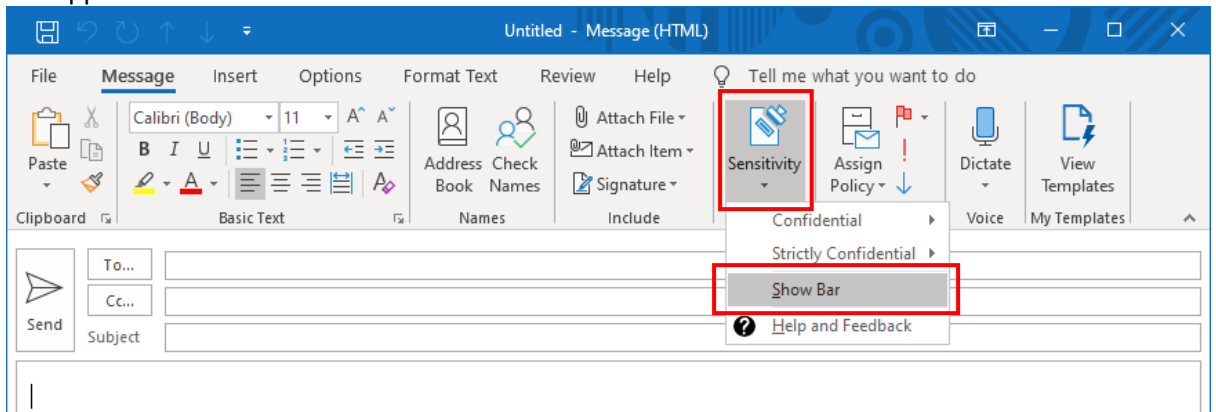


4. In the new compose window, if you have not signed-in to the AIP service before, click **Sign in** button and sign in with your O365 account.

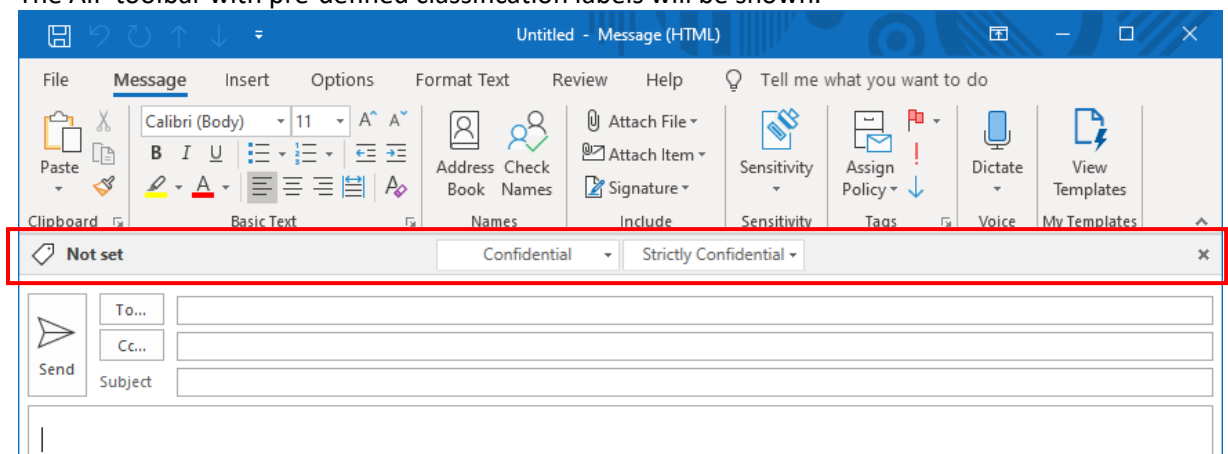




5. When you are signed-in, click **'Sensitivity'** icon, then click **Show Bar**, the AIP bar would appear.



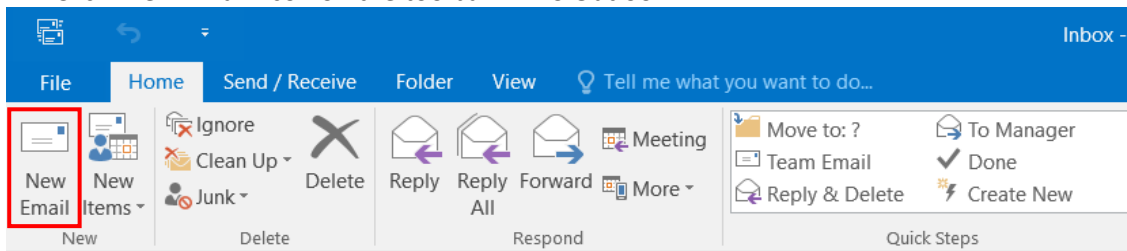
The AIP toolbar with pre-defined classification labels will be shown.



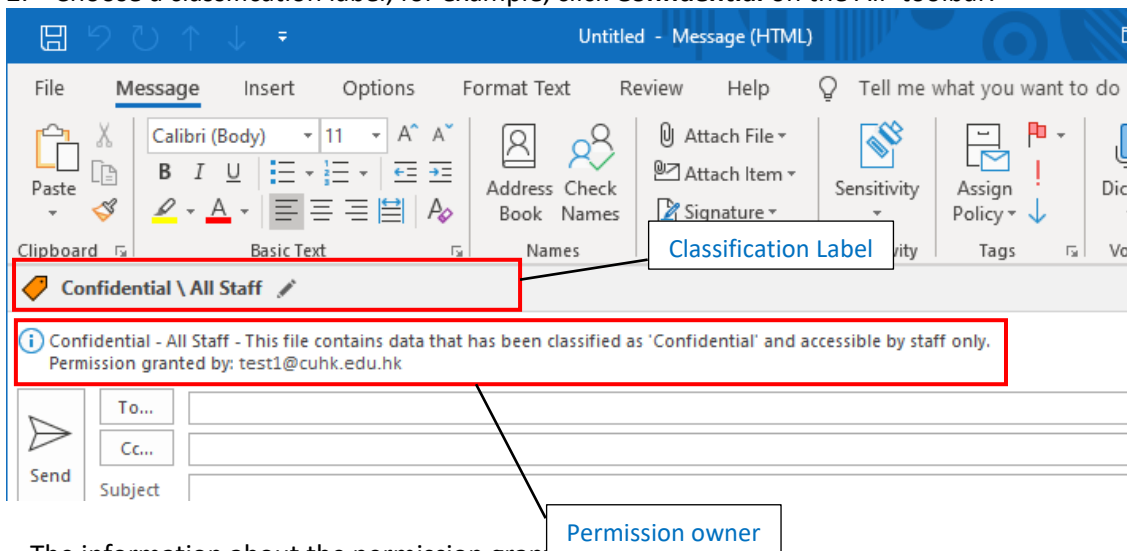
### 5.1.1.2. Apply a Classification Label in MS Outlook

#### Steps:

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



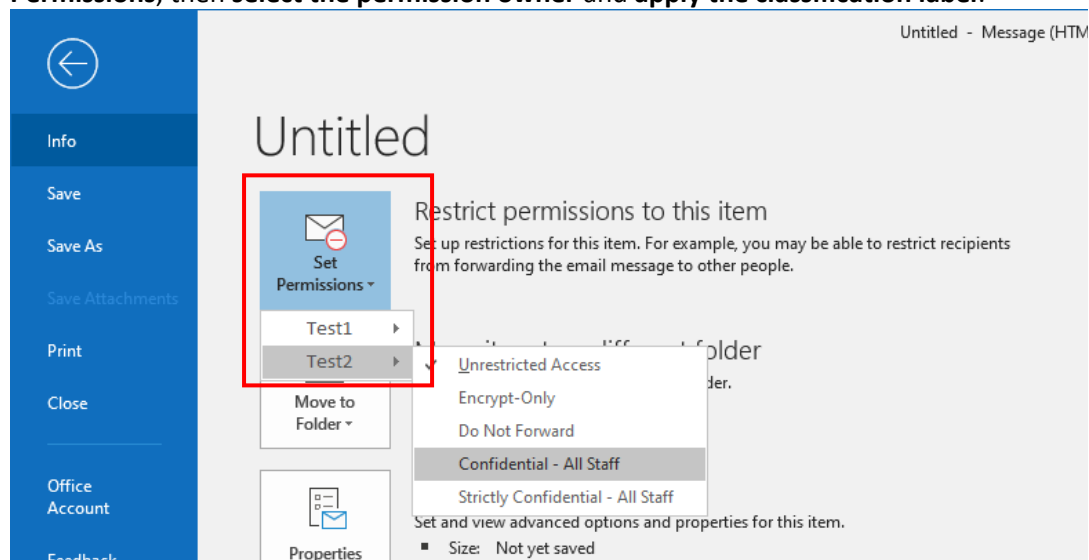
2. Choose a classification label, for example, click **Confidential** on the AIP toolbar.



The information about the permission granted will be shown.

3. If there are **more than 1 profile** in your MS Outlook, please make sure to select the correct permission owner for applying a classification label.

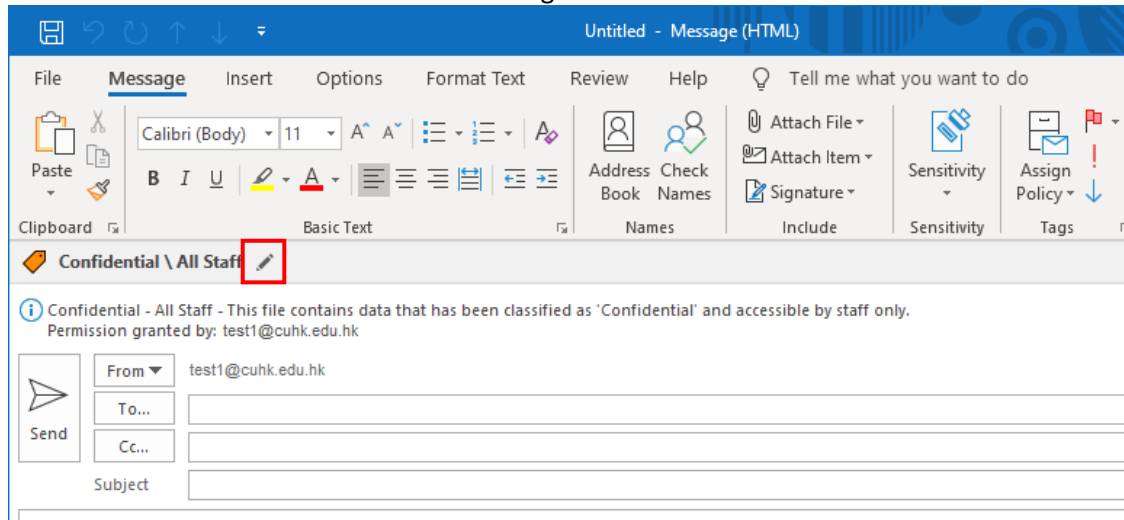
To select the permission owner, in your email composing window, click **File > Info > Set Permissions**, then **select the permission owner and apply the classification label**.



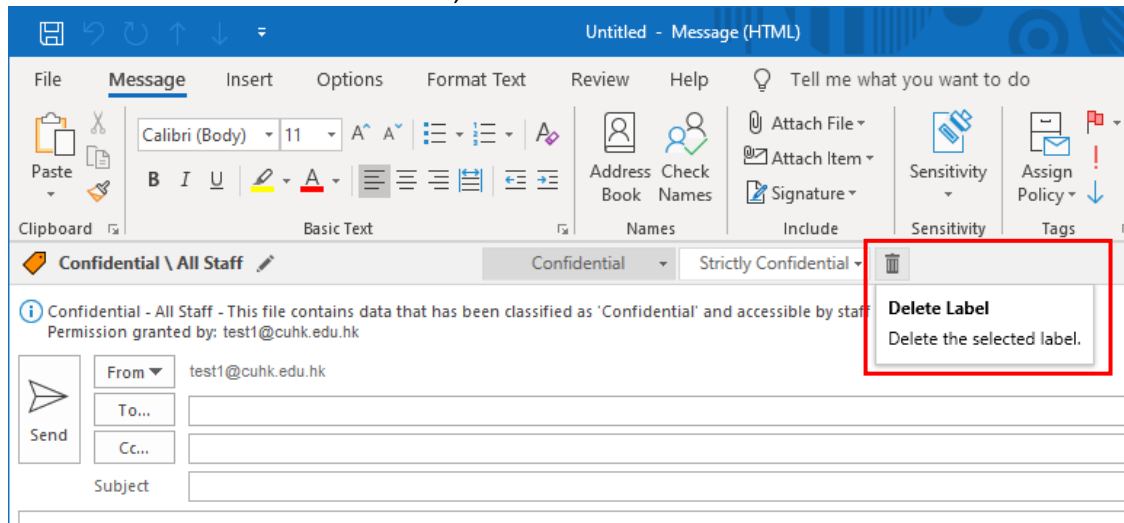
### 5.1.1.3. Change / Delete the Classification Label in MS Outlook Windows

#### Steps:

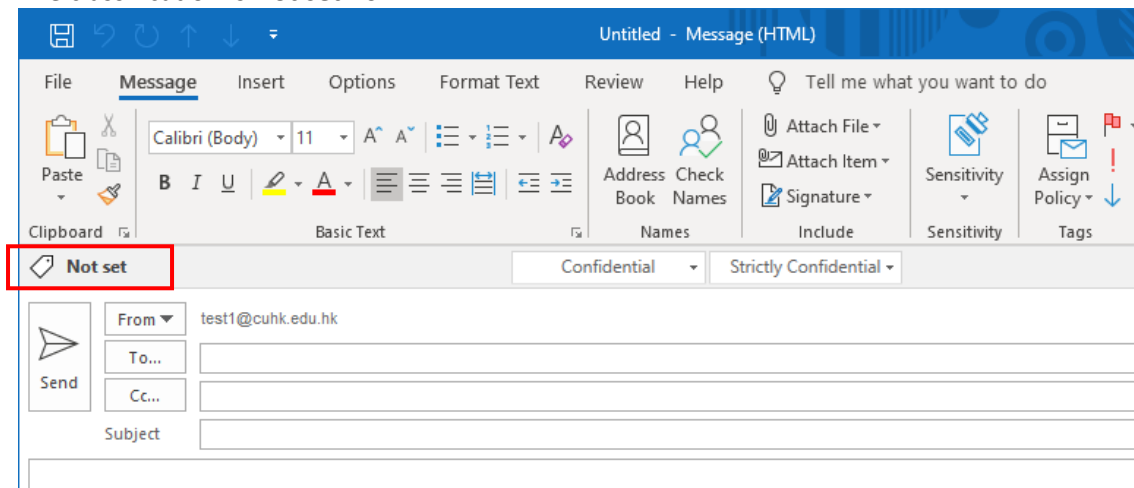
1. You can click **Edit Label** icon  to change the classification label.



2. To remove the classification label, click **Edit Label** icon  and then **Delete Label** icon .



The classification is **Not set** now.



#### 5.1.1.4. Attach File in a Protected Email

##### Steps:

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

Different classification / protection between email and attachment would have different behavior:

Email	Attachment	Behavior in Email	Authorized Recipient	Unauthorized Recipient
Protected	Unprotected	Classification 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
Protected	Protected	Email and attachment will apply their own classification label.	✓ Can access both email and attachment	✗ Cannot access both email and attachment
Unprotected	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

### 5.1.2. In Outlook Web Access (OWA)

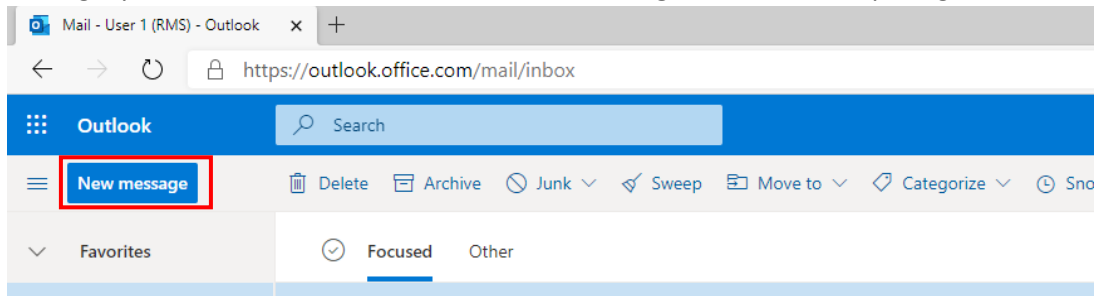
In OWA, **4 types of protection** can be applied to an email:

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.

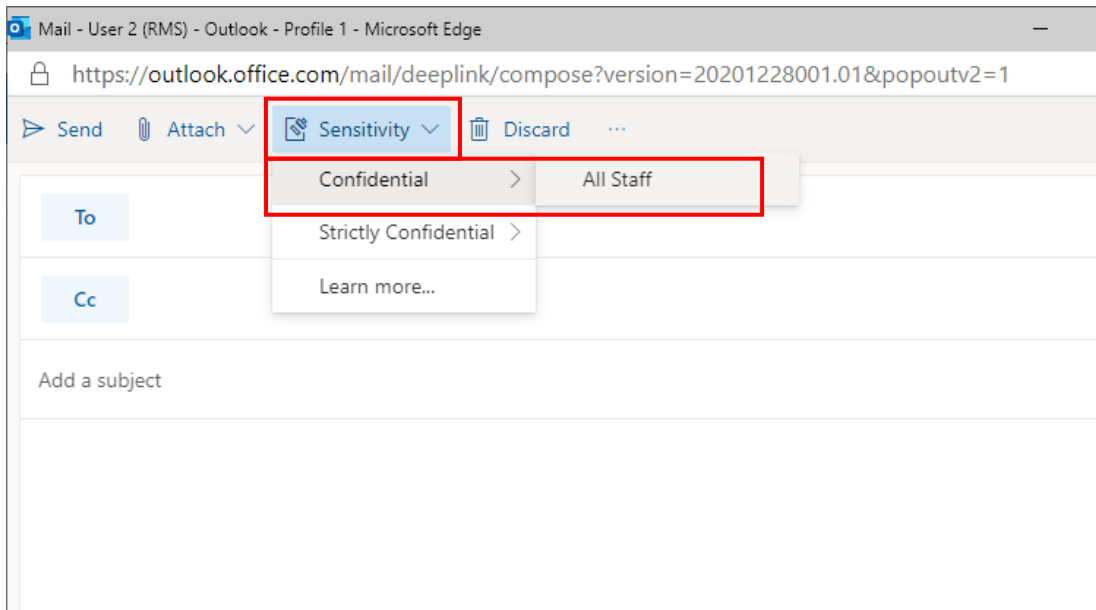
#### 5.1.2.1. Apply a Permission in OWA

**Steps:**

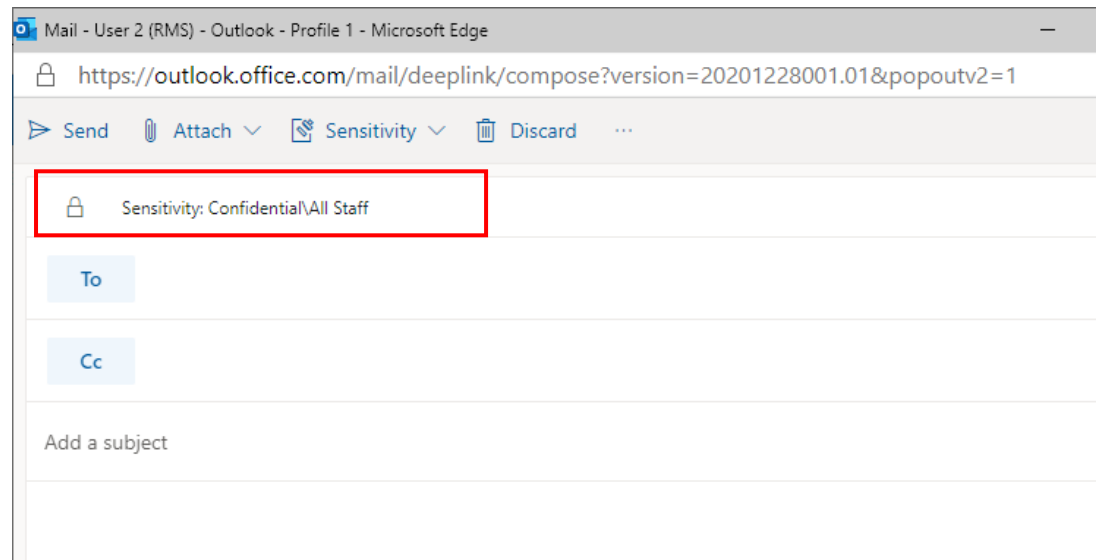
1. Login your O365 account in OWA, click **New message** button for composing a new email:



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



The information about the classification label chosen will be shown.



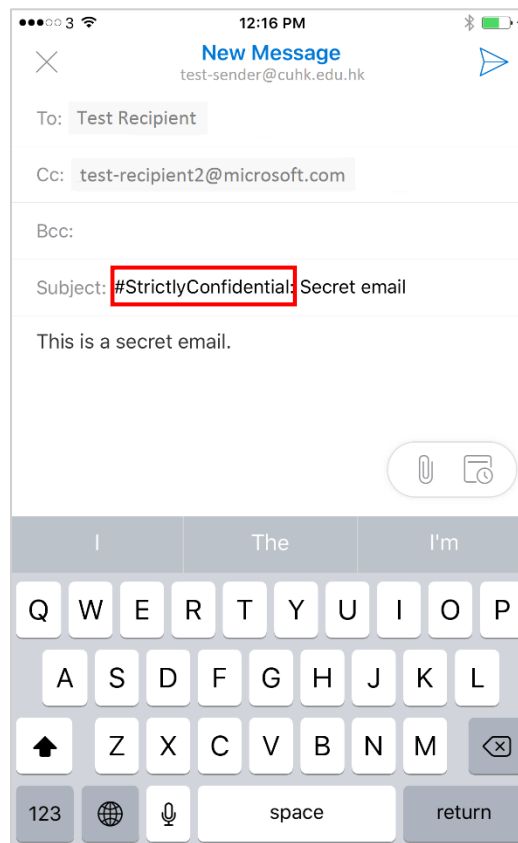
## 5.2. Send Protected Email with Subject Tag

In Exchange Online, 2 transport rules had been setup for email protection in case AIP client is not applicable in some platforms, e.g. mobile environment.

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

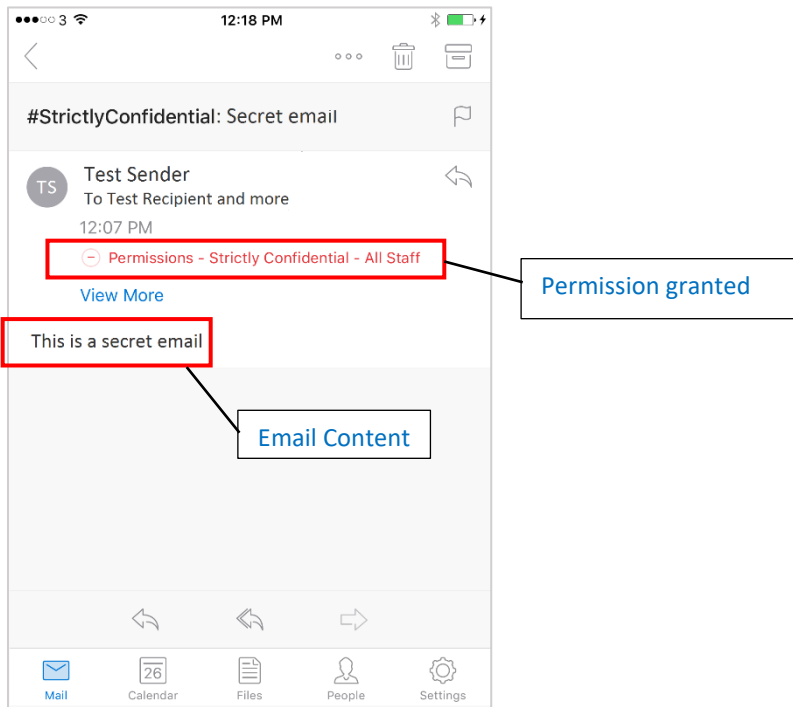
- Email subject with keyword “**#Confidential**”
  - o Apply permission control: Confidential – All CUHK Staff
- Email subject with keyword “**#StrictlyConfidential**”
  - o Apply permission control: Strictly Confidential – All CUHK Staff

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

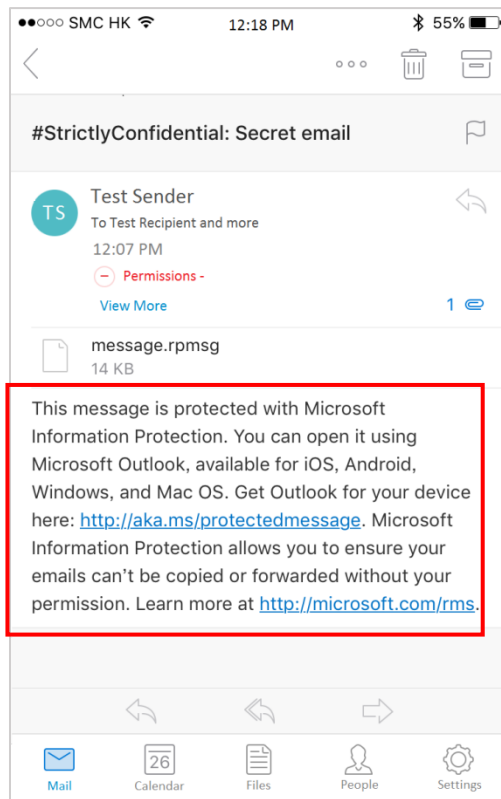


After the email is sent:

- i. **Authorized recipient** can access the email content & see the classification and permission granted.



- ii. If you are **unauthorized recipient**, you cannot access the email and below message about the email is AIP protected would be shown.




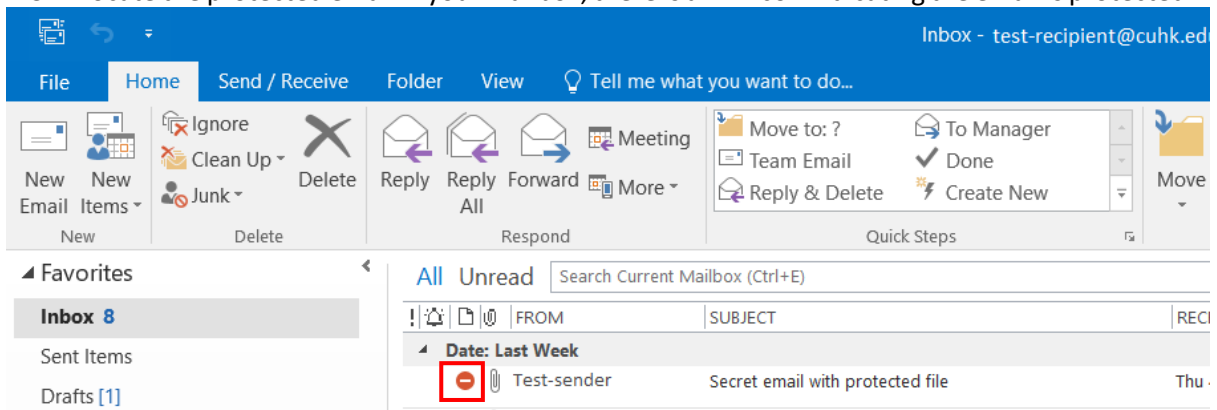


## 5.3. Read Protected Email

### 5.3.1. In Outlook for Windows

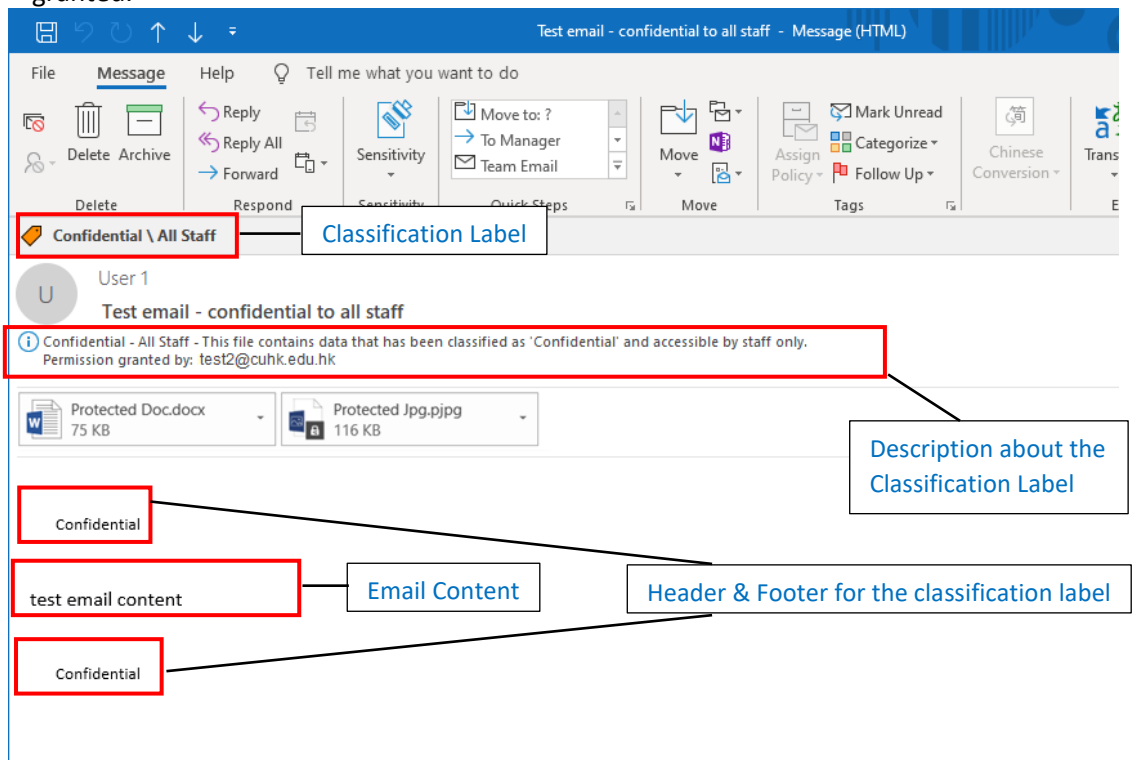
#### Steps:

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.

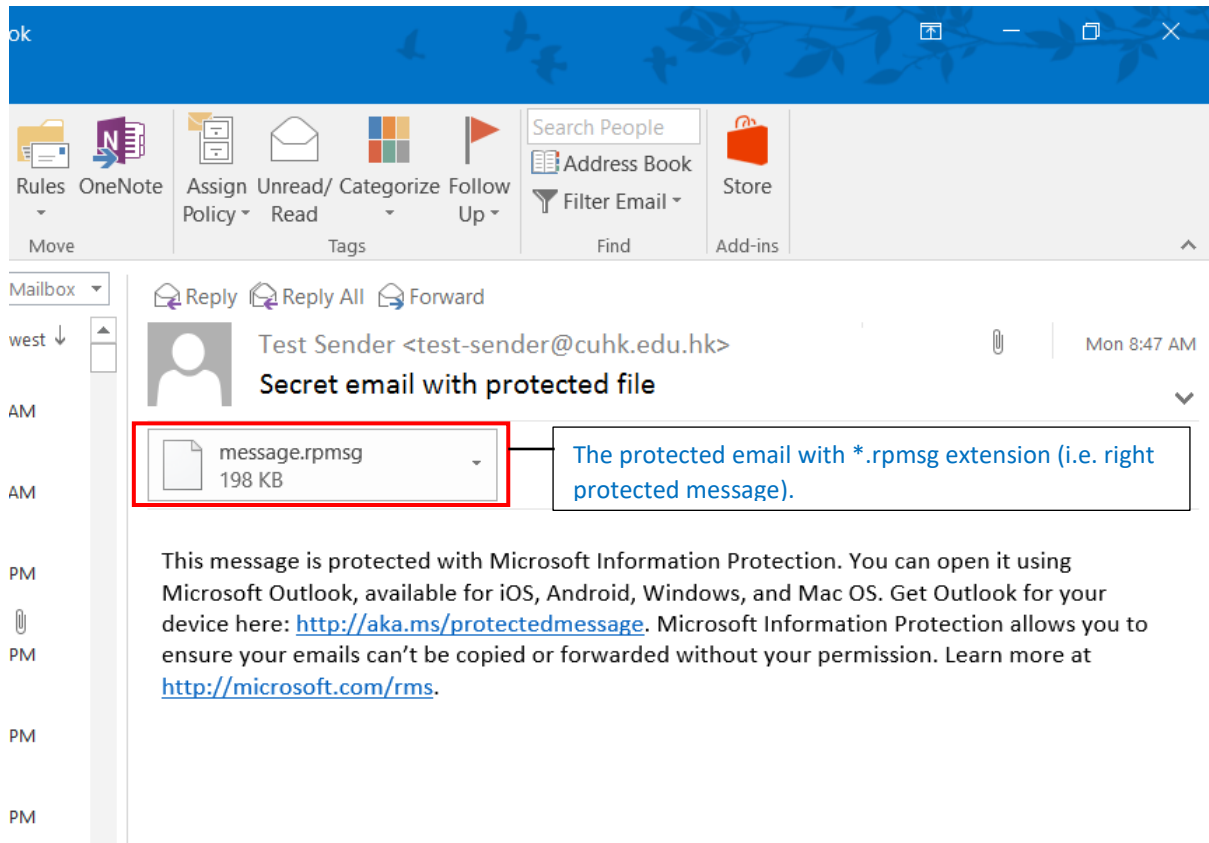


4. Open the protected email by double clicking the email subject.

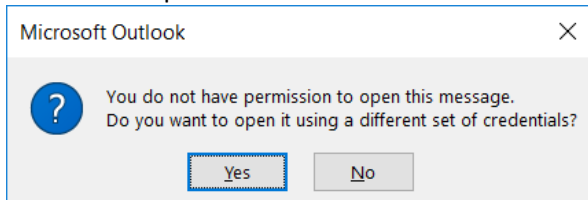
Authorized recipient can access the email content & attachment according to the permission granted.



5. If you are unauthorized recipient, you will not be able to access the content of email and the attachment. In the reading pane, the following message about the email is AIP protected would be shown.



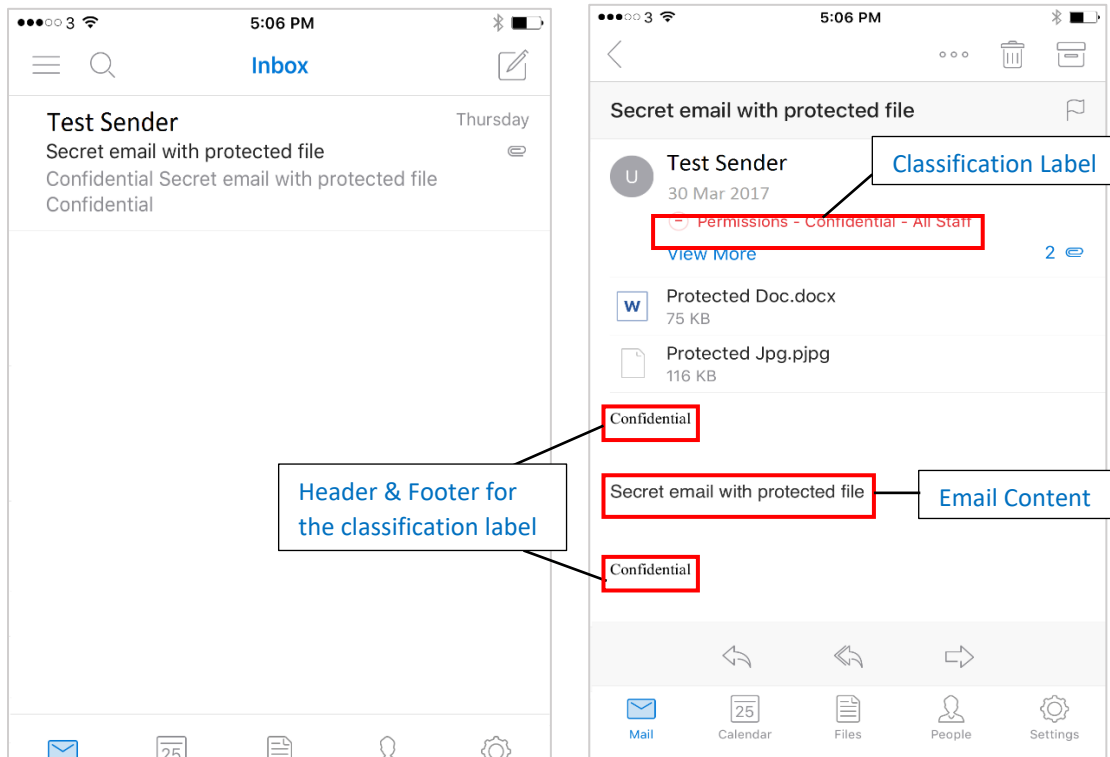
Open the protected email by double clicking the email subject, the following message will popup. Click **Yes** to open the email with an authorized account, click **No** to close the window.



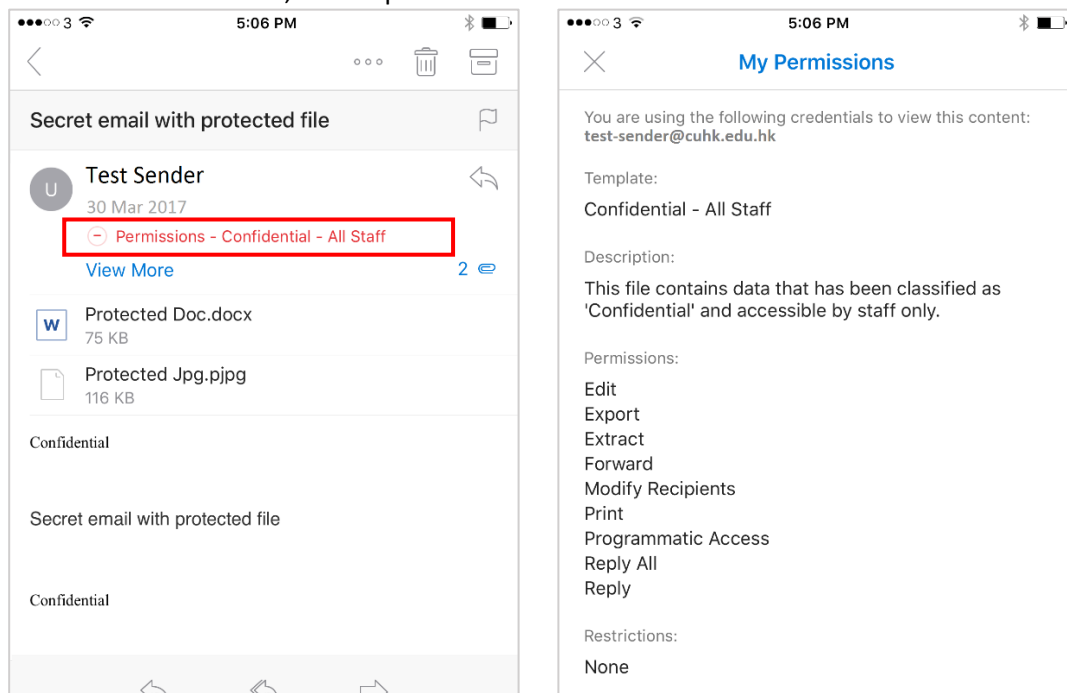
### 5.3.2. In Outlook for iOS and Android

#### Steps:

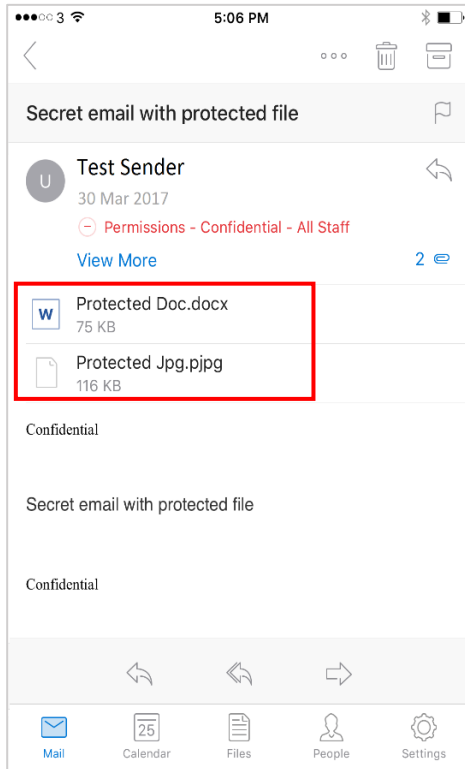
1. Open MS Outlook.
2. Login with your CUHK Exchange account.
3. Locate the protected email in your mailbox, and click on the email to view details. Authorized recipient can access the email content & attachment according to the permission granted.



4. Click on the Permissions, details permissions would be shown.



5. Back to the email content, you need specific apps to open the protected attachments.



You need to **download and install the following apps in your mobile** in advance (refer to Section 2.1):

- **Microsoft Word, Excel, and PowerPoint** for opening MS Office files




- **Azure Information Protection** for opening non-MS Office files

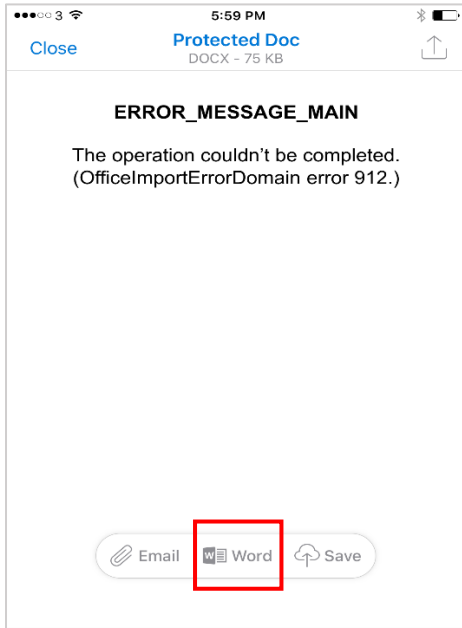


After the above apps are installed, **login your O365 account** with these apps for authentication and authorization checking when you open any protected files.

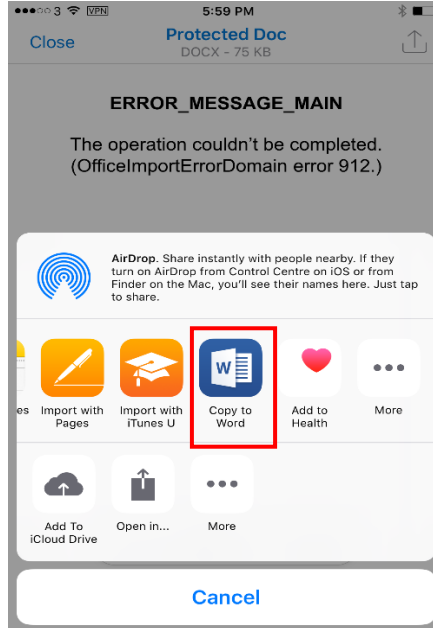
6. To open the protected Word file (Office file), click on the MS Word attachment in the email.

**In iOS:**

Click on the MS Word app to open the file. Alternatively, you can click  icon and click **Copy to Word** to open it by MS Word apps.

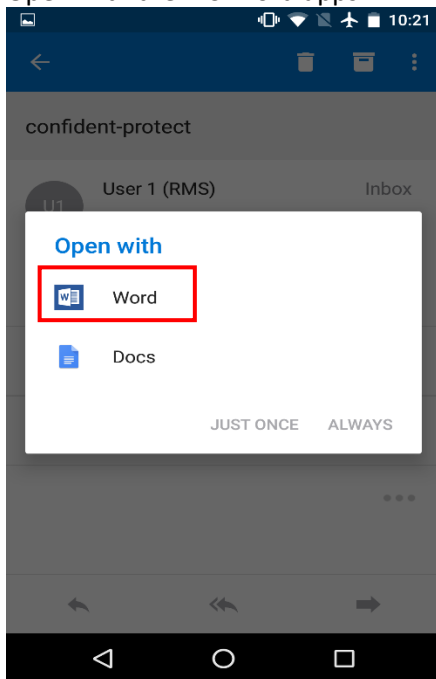


OR



**In Android OS:**

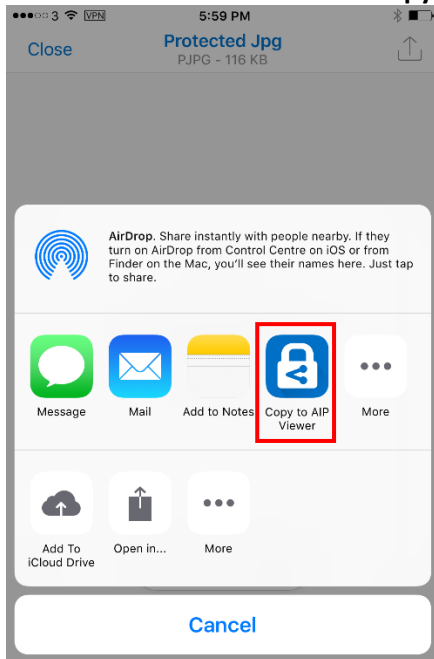
Open with the MS Word apps.



7. To open the protected JPG file (non-Office file), click on the file JPG attachment in the email.

**In iOS:**

Click on the  icon and click **Copy to AIP Viewer** to open it by AIP Viewer.




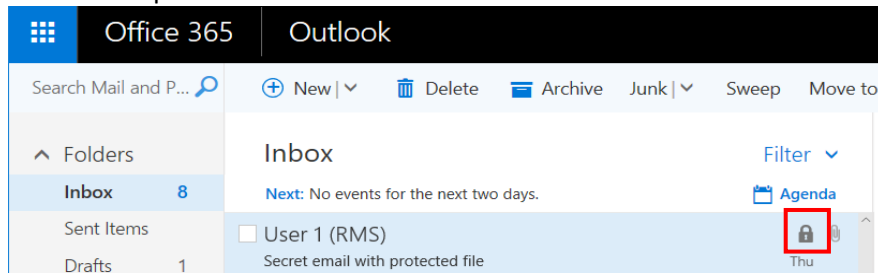
**In Android OS:**

It will call the AIP Viewer directly and open the file.

### 5.3.3. In Outlook Web Access (OWA)

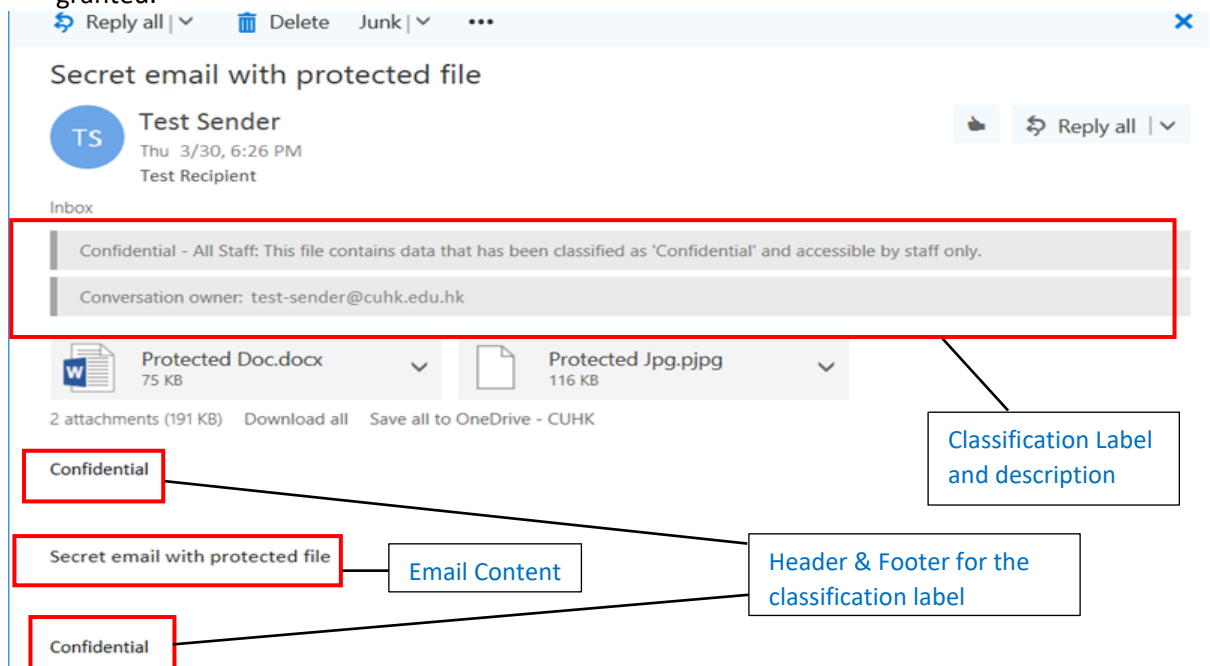
#### Steps:

1. Login O365 Mail, locate the protected email in your mailbox, there is a  icon indicating the email is protected

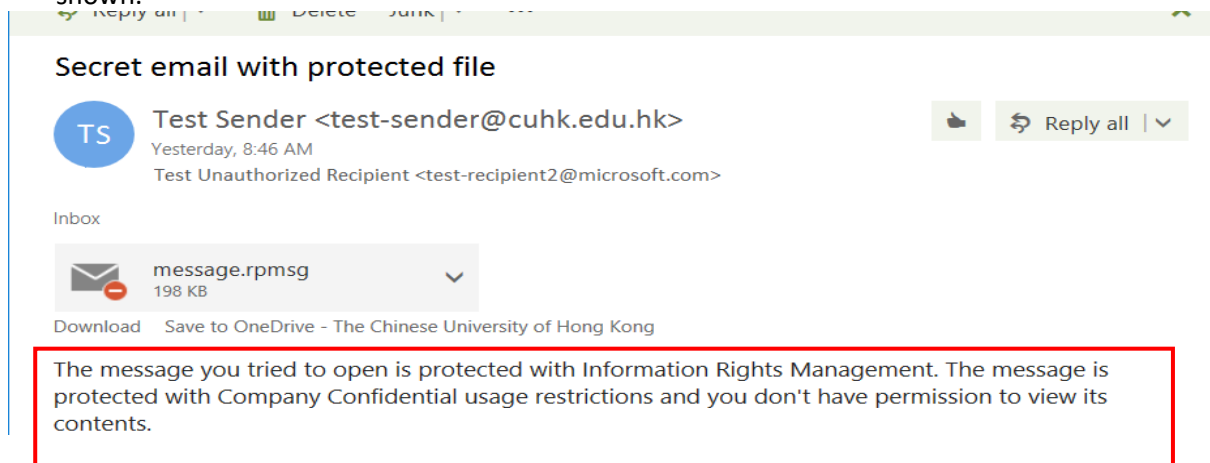


2. Open the protected email by double clicking the email subject.

Authorized recipient can access the email content & attachment according to the permission granted.



3. If you are unauthorized recipient, below message about the email is AIP protected would be shown.



## 6. File Protection in SharePoint Online & OneDrive

### 6.1. Create a Protected document in SharePoint Online & OneDrive

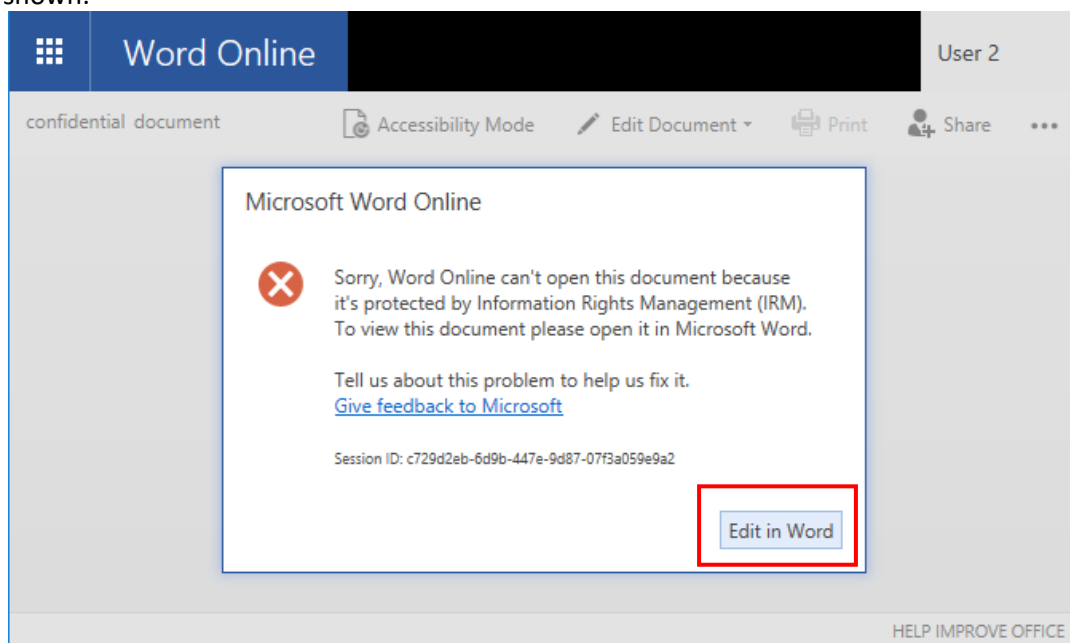
Currently, AIP is not integrated in MS SharePoint Online and OneDrive. However, you can upload a AIP protected file to these environment as usual, and the file should be protected in your local computer in advance. Detailed steps about File Protection can be found in Section 4.

### 6.2. Open a Protected document in SharePoint Online & OneDrive

Protected documents in SharePoint Online and OneDrive cannot be opened and edited 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 Word** to launch the MS Word in your local computer and access to the 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.