Microsoft 365 Azure Information Protection User Guide

Contents

Introduction to Azure Information Protection (AIP) 2

User Guide 2

Support 3

Data Protection Champion & Deputies 3

1. Documents 5

Example - Creating a Confidential Document Classified Automatically 5

Example - Creating a Highly Confidential Document Classified Manually 7

Example - Downgrading a Document 9

2. Emails 11

Example - Send Email with Highly Confidential Sensitivity Applied Automatically 11

Example - Send Email with Confidential Sensitivity Applied Manually 12

Example – Sending a Highly Confidential Email to External Recipient 13

Introduction to Azure Information Protection (AIP)

AIP is a cloud-based solution that helps an organisation to classify and protect its documents. After a document or email is classified (e.g. Highly Confidential, Confidential etc.) it can be tracked, and data flows can be analysed to detect risky behaviours and take corrective measures.

Documents and emails can be classified (labelled) automatically or manually when certain phrases are detected, such as Strictly Confidential, TMC Confidential or private information such as Credit Card and Passport numbers.

The below table gives an overview of each label including what it does and what triggers automatic labelling (classification).

User Guide

The following pages aim to give you some example screen shots showing you what you will see with documents and emails once you are AIP enabled.
The guide is divided into 2 sections:

- Documents
- Emails

Label	Description	What it does	How it's triggered
Public	Business data that is specifically prepared and approved for public consumption	No Restrictions Protection removed, no header or watermark	Manual selection only
General	Business data that is not intended for public consumption. However, this can be shared with external partners, as required	No Restrictions **Default label,** Manual selection No Protection, header or watermark	**Default label**, or manual selection
Confidential	Sensitive business data that could cause damage to the business if shared with unauthorised people	Encrypted, permissions changed to authenticated users (Users that have logged in) header, no watermark	TMC Confidential, driving license, passport No, credit card, NI No. Manual selection
Highly Confidential External	Very sensitive business data that could cause damage to the business if shared with unauthorised people	Encrypted, permissions changed to authenticated users, TMC header and watermark	Highly confidential, strictly confidential, strictly private and confidential Manual selection
Highly Confidential Internal	Very sensitive business data that could cause damage to the business if shared with unauthorised people	Encrypted, permissions changed Midcounties Colleagues, TMC header and watermark	Highly confidential, strictly confidential, strictly private and confidential Manual Selection

Support

If you have any issues with AIP, then please speak to your Data Protection Champion or their Deputy in the first instance. They will be able to help you or get the relevant support for you.

Data Protection Champion & Deputies

Business Unit	DPC Name, Job Title & Contact Details	Deputy DPC Name, Job Title & Contact Details
Healthcare	Phil Wilkes Pharmacist Manager, Healthcare Phil.Wilkes@midcounties.coop	Raj Patel Area Manager, Healthcare raj.patel@midcounties.coop
Childcare	Sue Hunt Quality Support Manager, Childcare sue.hunt@thecooperativechildcare.coop	Holly Sawyers Central Operations Manager, Childcare Holly.sawyers@thecooperativechildcare.coop
Travel	Richard Simpson Governance and Compliance Manager, Travel Rich.Simpson@cooptravel.coop	Bonnie Barber Marketing Communications Officer, Travel Bonnie.barber@cooptravel.coop
Funeral	Gill Moore Funeral Support Manager gillian.moore@midcounties.coop	Andrew Williams Masonry Manager, Funeral Andrew.williams@midcounties.coop
Food	Ann Hudson Retail Compliance Manager, Food Retail Operations ann.hudson@midcounties.coop	Louise Edgar-Kerrigan Regional Administrator, Convenience Louise.Edgar-Kerrigan@midcounties.coop
Post Office	Sue Spicer Area Manager, Post Office sue.spicer@midcounties.coop	Sue Berry Compliance Manager, Post Office susan.berry@midcounties.coop
Utilities (Flex Bens, Phone Co-op & Energy)	Dally Purewal Head of Commercial Sales and Partnerships Dally.purewal@midcounties.coop	Mark Redgrave Customer Service Advisor, Flexible Benefits mark.redgrave@midcounties.coop Sam Read Service Manager, Phone Coop Sam.Read@thephone.coop
Colleague & Co-operative Services	Pete Lockey Head of CCS Communications peter.lockey@midcounties.coop	Lee Franklin Membership Benefits Manager lee.franklin2@midcounties.coop
Membership	Lee Franklin Membership Benefits Manager lee.franklin2@midcounties.coop	Pete Lockey Head of CCS Communications peter.lockey@midcounties.coop

Business Unit	DPC Name, Job Title & Contact Details	Deputy DPC Name, Job Title & Contact Details
PSG	Nick Porter Head of Colleague Relations nick.porter@midcounties.coop	Rani Jandu Transactional Services Manager rani.jandu@midcounties.coop
Finance	Peter Kelly Group Financial Controller peter.kelly@midcounties.coop	Anne Penfold Transactional Finance Manager anne.penfold@midcounties.coop
Information Services	Aaron Clayton Deputy Chief Information Officer aaron.clayton@midcounties.coop	Avinash Kaur Babra Risk & Compliance Analyst, IT avinash.kaurbabra@midcounties.coop
Marketing / CRM	Suzanne Clucas CRM Manager Suzanne.clucas@midcounties.coop	Melody Aguero Head of Brand Strategy and Insights Melody.Aguero@midcounties.coop Hayley Small Brand and CRM Lead hayley.small@midcounties.coop
Specialist Services	Caroline Nichols Head of Insurance & Compliance caroline.nichols@midcounties.coop	Jayde Labron Insurance and Risk Advisor jayde.labron@midcounties.coop

1. Documents

Documents will be automatically classified as Confidential when any of the following text is contained but please note it must be in the format highlighted for auto classification as Confidential:

- Passport Number 791234567
- National Insurance Number Ab 12 34 45 c
- Driving Licence Number MORGA753116SM9IJ
- Credit Card 4111 1111 1111 1111

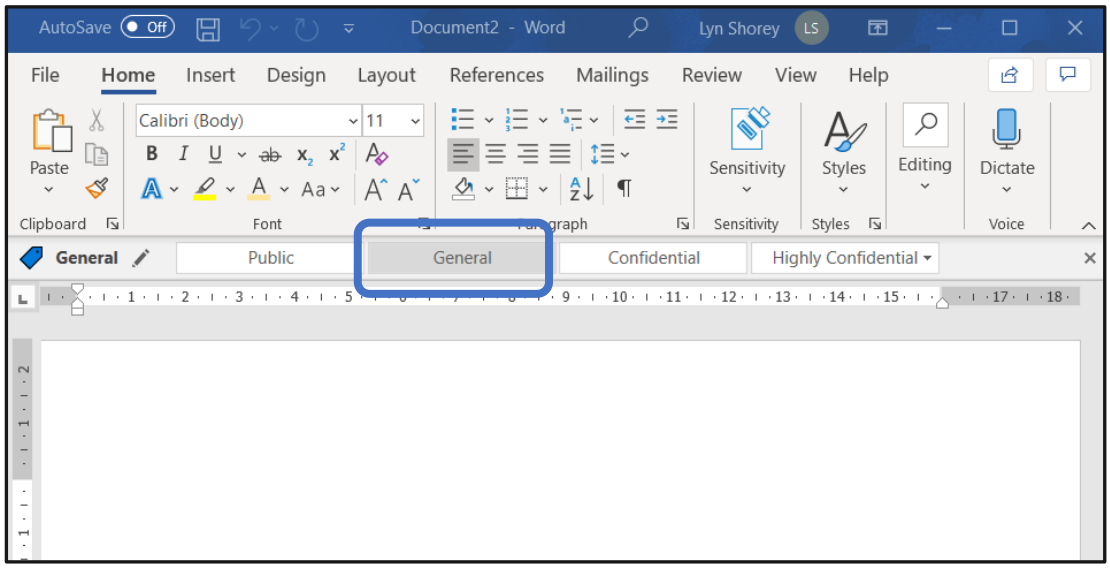
Documents will be automatically classified as Highly Confidential when any of the following text is contained in a document:

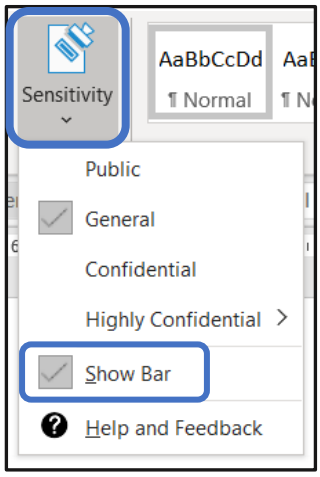
- Highly Confidential
- Strictly Confidential
- Strictly Private and Confidential

NB. Highly Confidential sensitivity is split into Internal (the default) and External.

Example - Creating a Confidential Document Classified Automatically

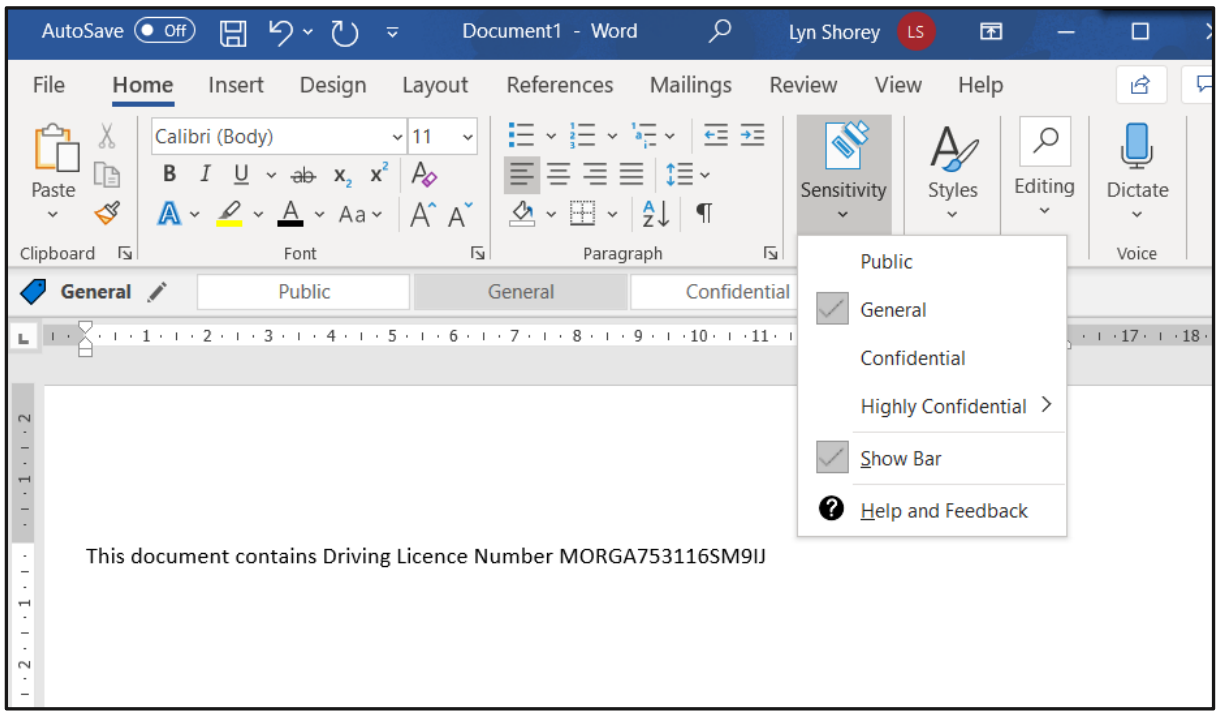
1. Create a new blank word document
2. The label shows the currently applied classification greyed out - **General** is the default



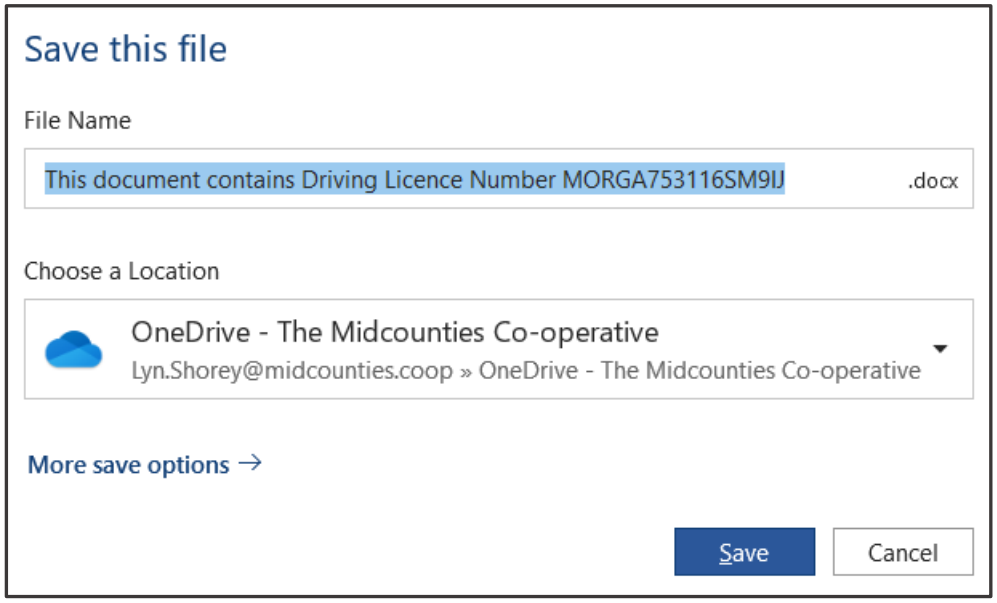


If the Sensitivity bar is not shown, then select Home tab, click on the Sensitivity button and select Show Bar from the dropdown.

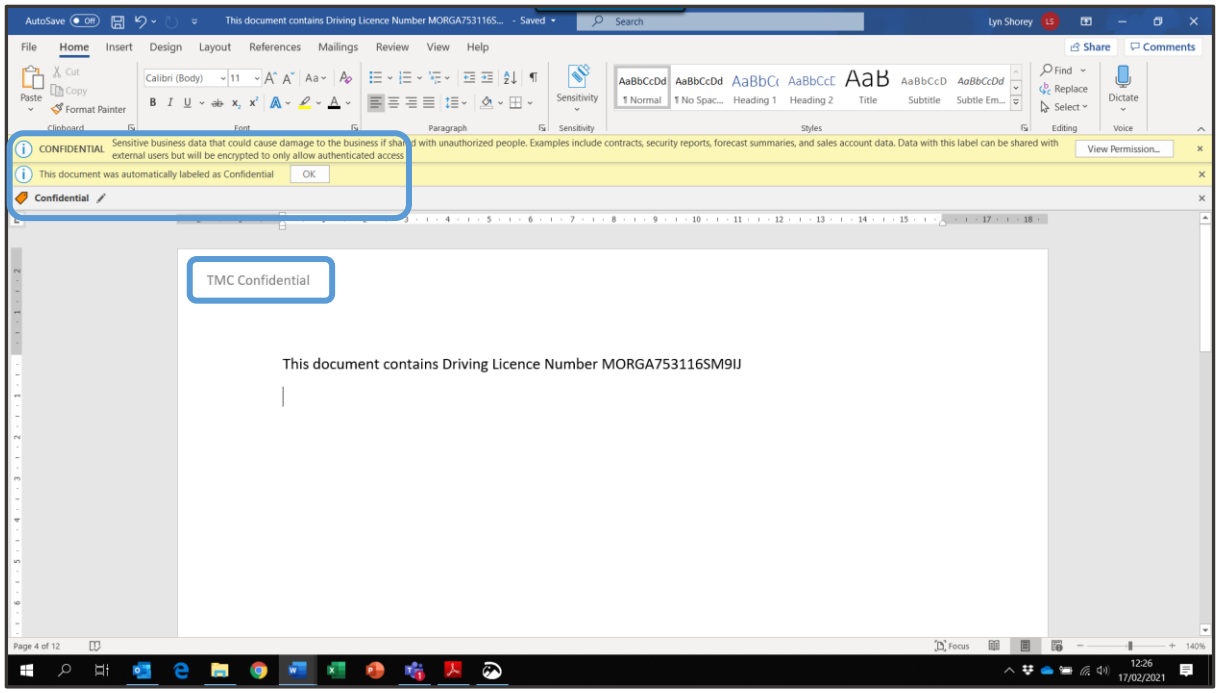
3. Next type a line in the document containing:
   Driving Licence Number MORGA753116SM9IJ



4. Save this file
5. You will see the message on the next page



6. Choose a location to save the document to and select Save
7. Now the document is saved it is labelled automatically as **Confidential** (shown below)

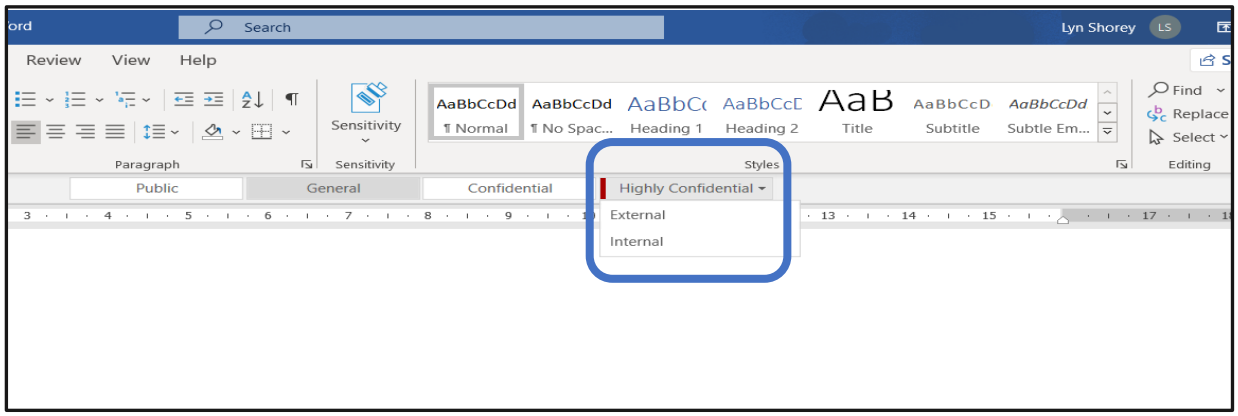


Example - Creating a Highly Confidential Document Classified Manually

1. Create a new blank word document

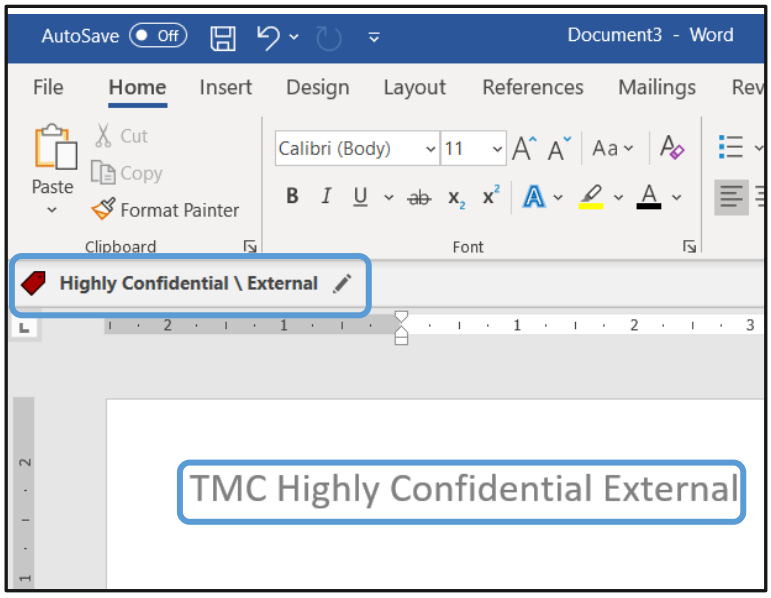
It will be classified as General by default.

2. Click on the Sensitivity button and select Highly Confidential choosing either External or Internal from the dropdown or click on the Highly Confidential tab and make your selection as per the example below.

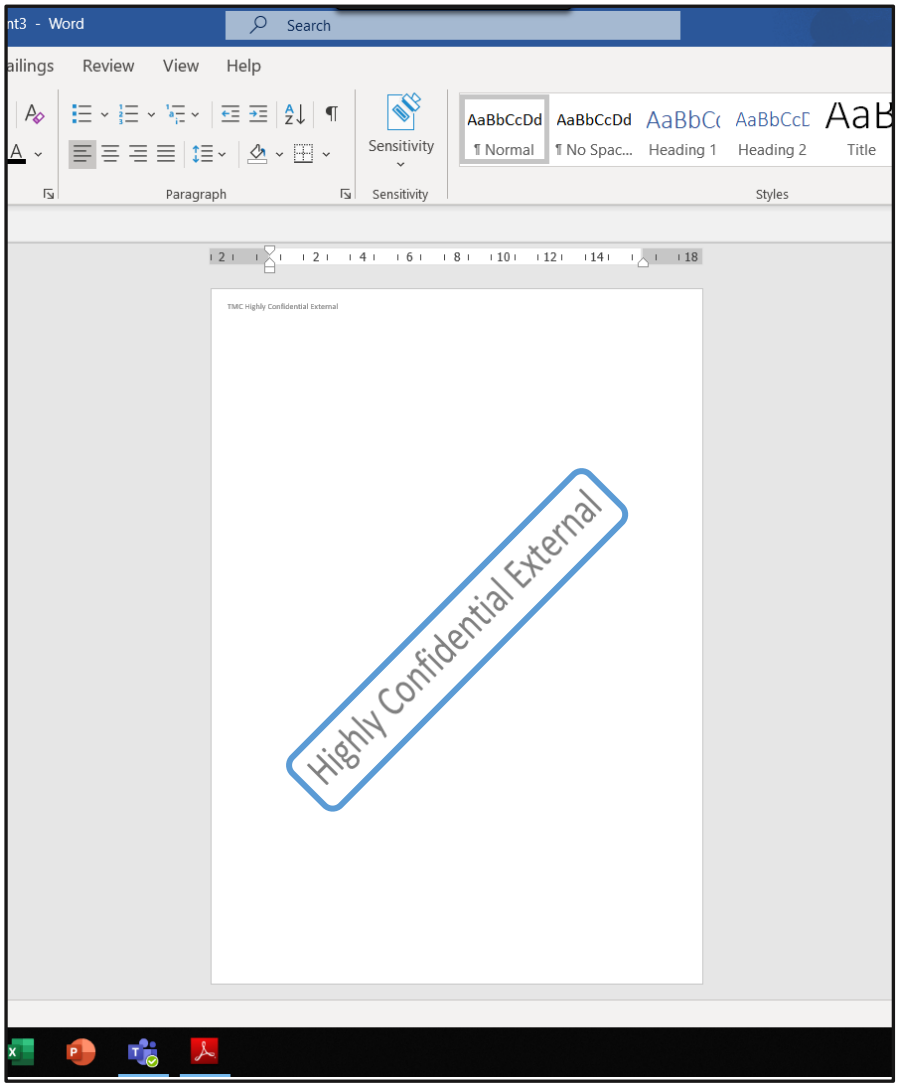


3. Save the document
   The document is labelled as **Highly Confidential \ External** or **Highly Confidential \ Internal** depending on your choice above.

   Each page will automatically include the header **TMC Highly Confidential External** or **Internal** (shown below).



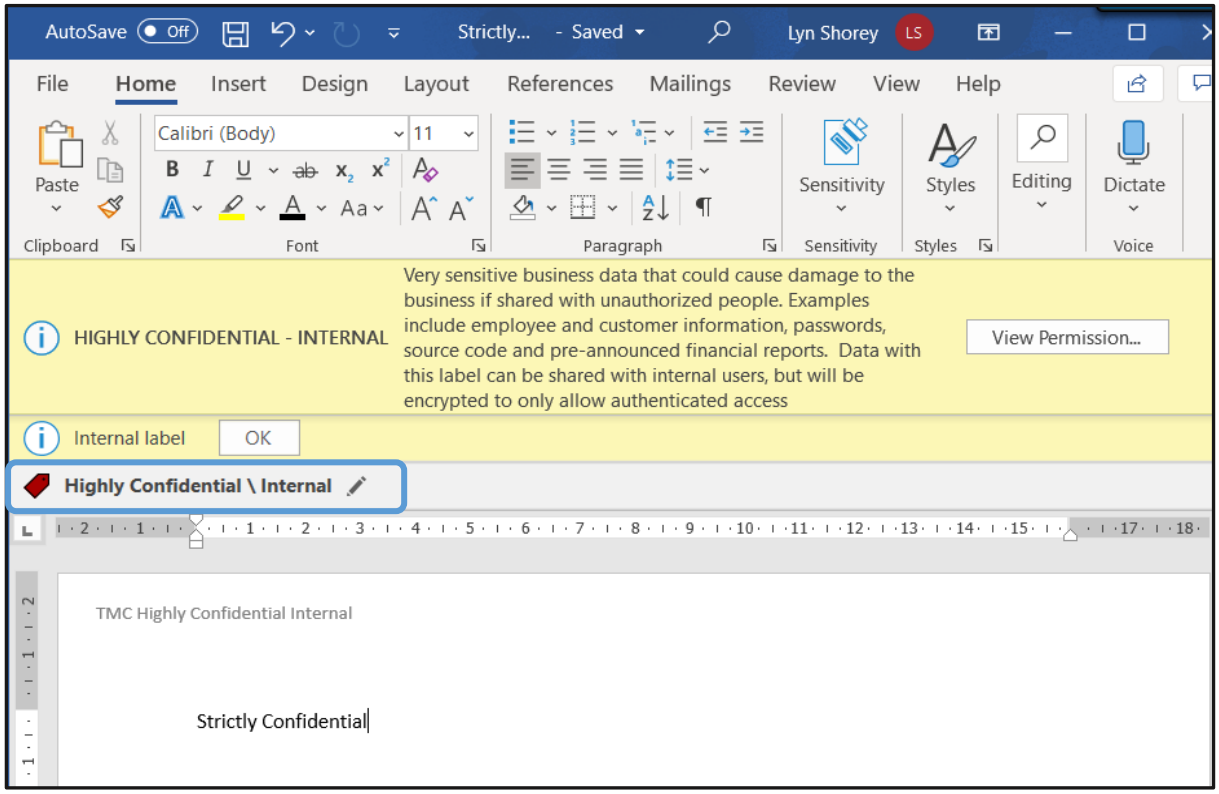
The watermark shows Highly Confidential External or Internal.



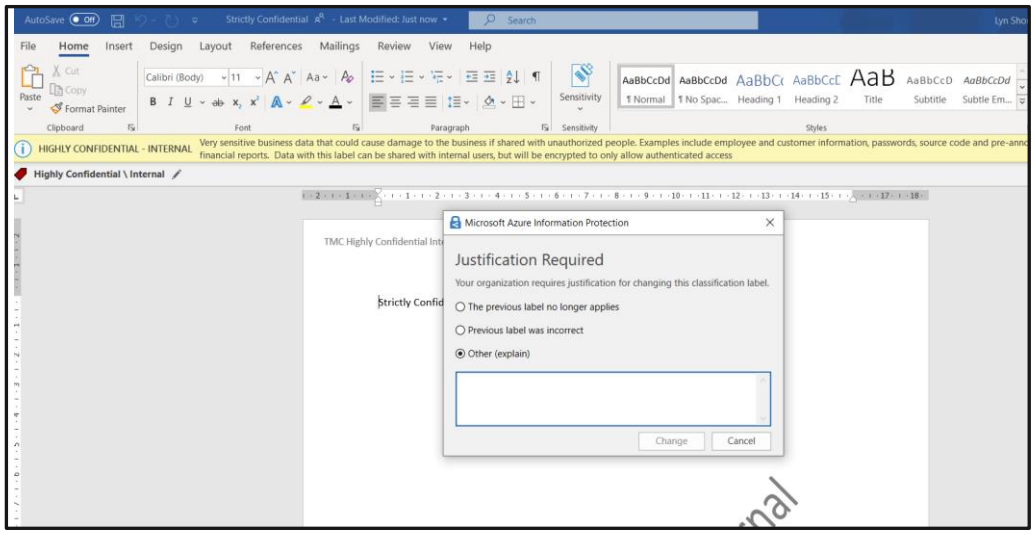
Example - Downgrading a Document

1. Create a word document adding the text Strictly Confidential and save

The document will be labelled as Highly Confidential – Internal.

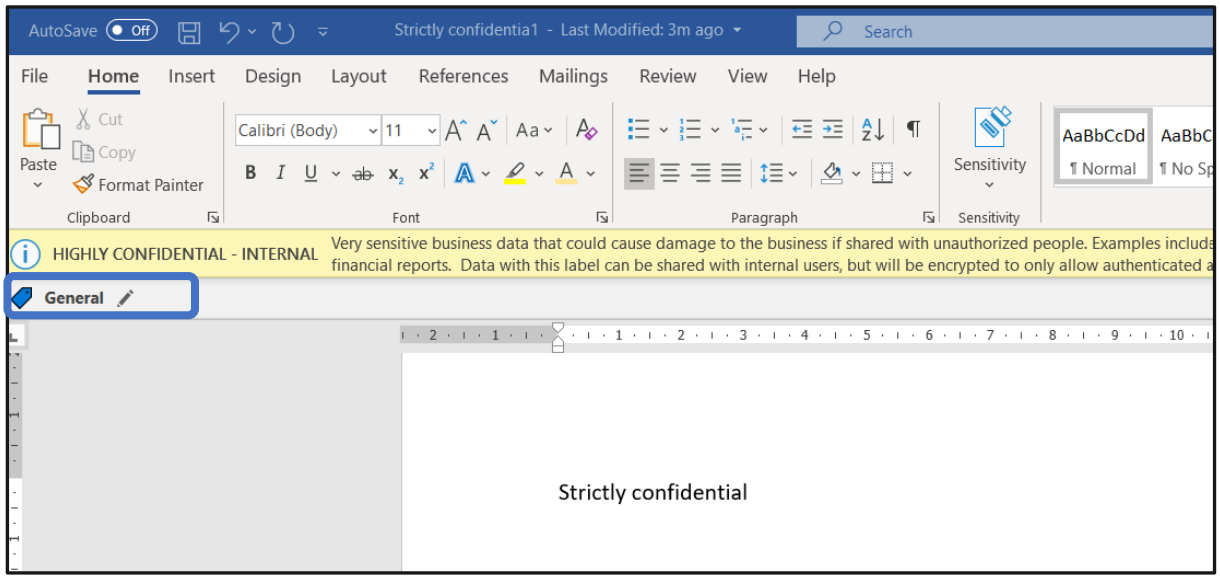


2. The watermark will show as **Highly Confidential Internal**
3. Close the document then re-open and select **General** from the Sensitivity dropdown
4. Pop-up is shown requesting justification for the downgrade



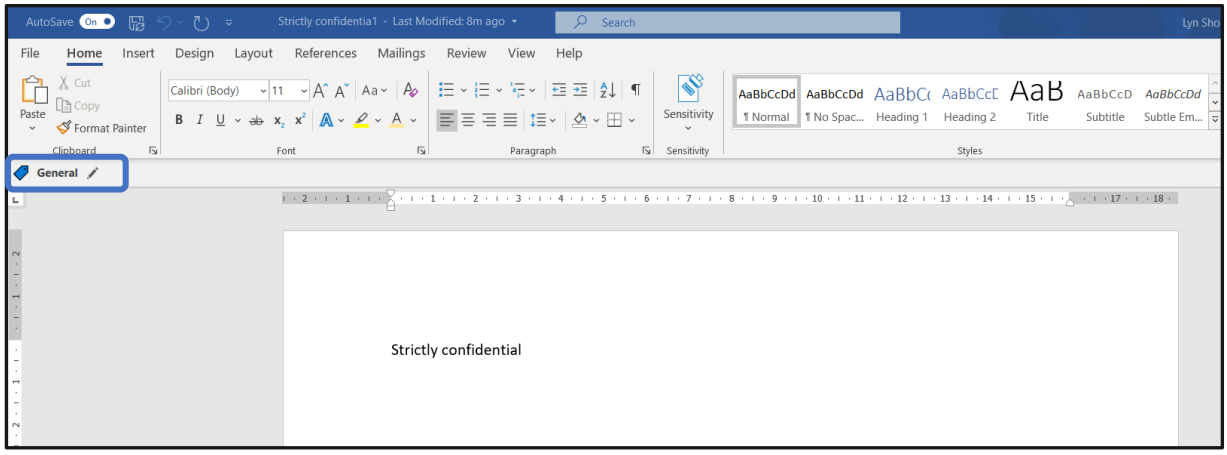
5. Click on Other (explain) option
6. Enter text justifying the downgrade
7. Click on Change to submit the justification reason

The document label will now show as **General** (shown below).



8. Save and close the document
9. Open the document and check that the sensitivity is set to **General**

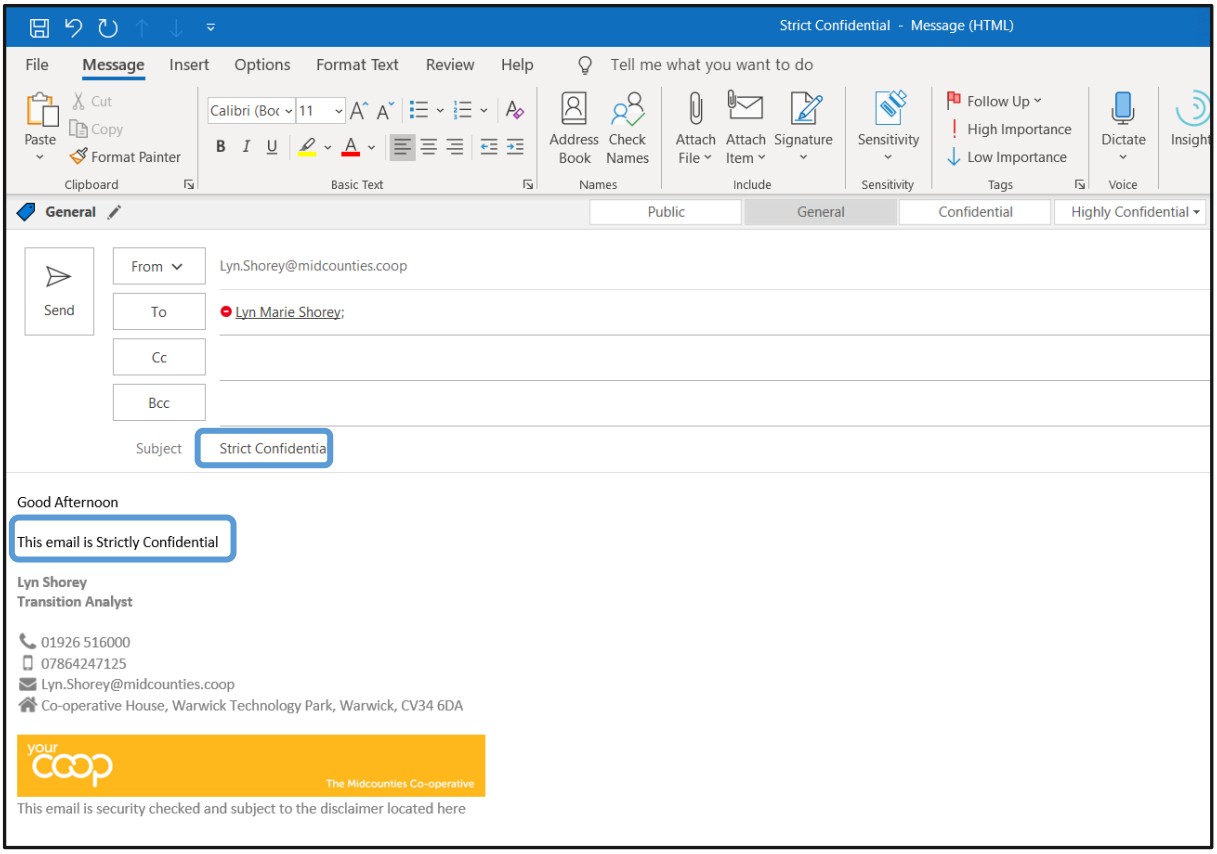
The **Highly Confidential** Banner has now been removed - this only happens when the document has been saved, closed and reopened.



2. Emails

Example - Send Email with Highly Confidential Sensitivity Applied Automatically

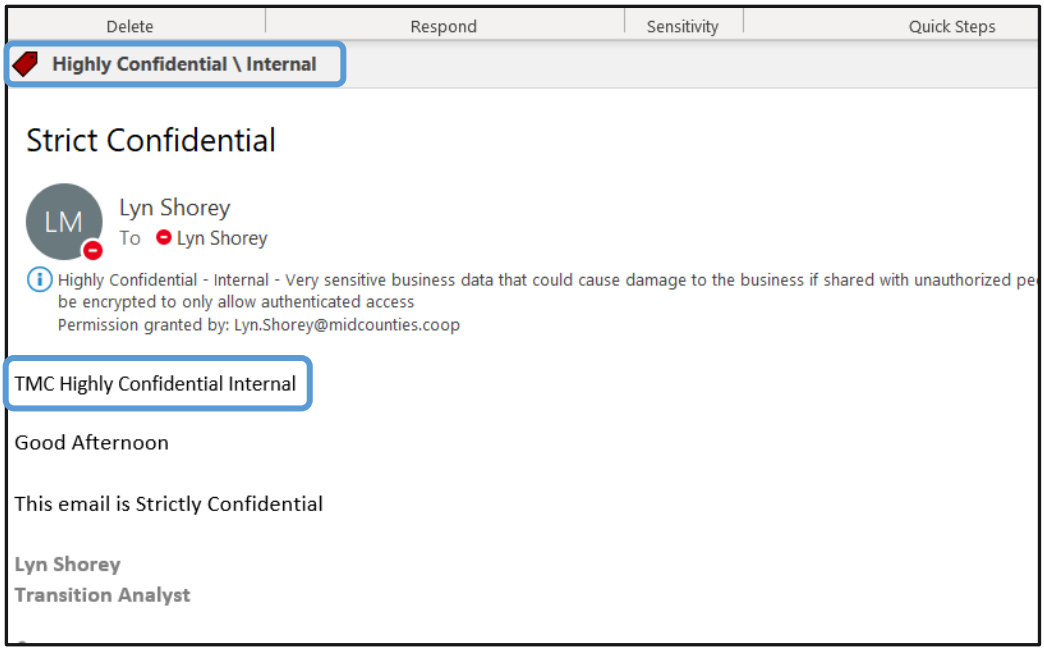
1. Open a new email
2. Select your internal recipient
3. Type 'Strictly Confidential' as the Subject (the Subject of the email is checked by AIP)
4. Type in body text which includes 'Strictly Confidential'



5. Click on Send

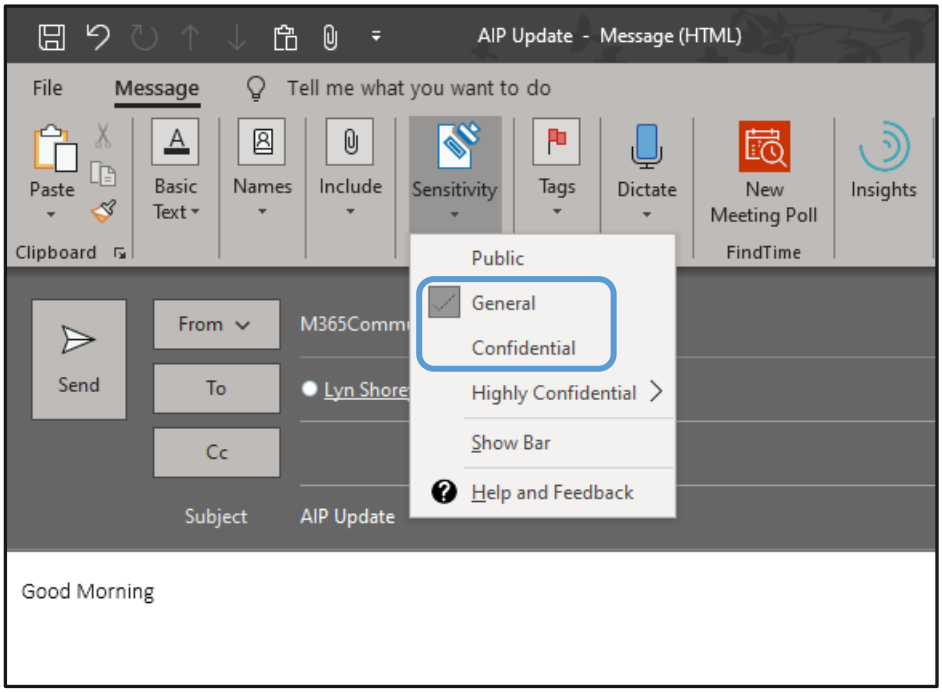
The recipient will see the email in their Inbox showing the padlock icon.

When the recipient opens the email, it is labelled **Highly Confidential Internal** (default).
The email now contains the header **TMC Highly Confidential Internal**.

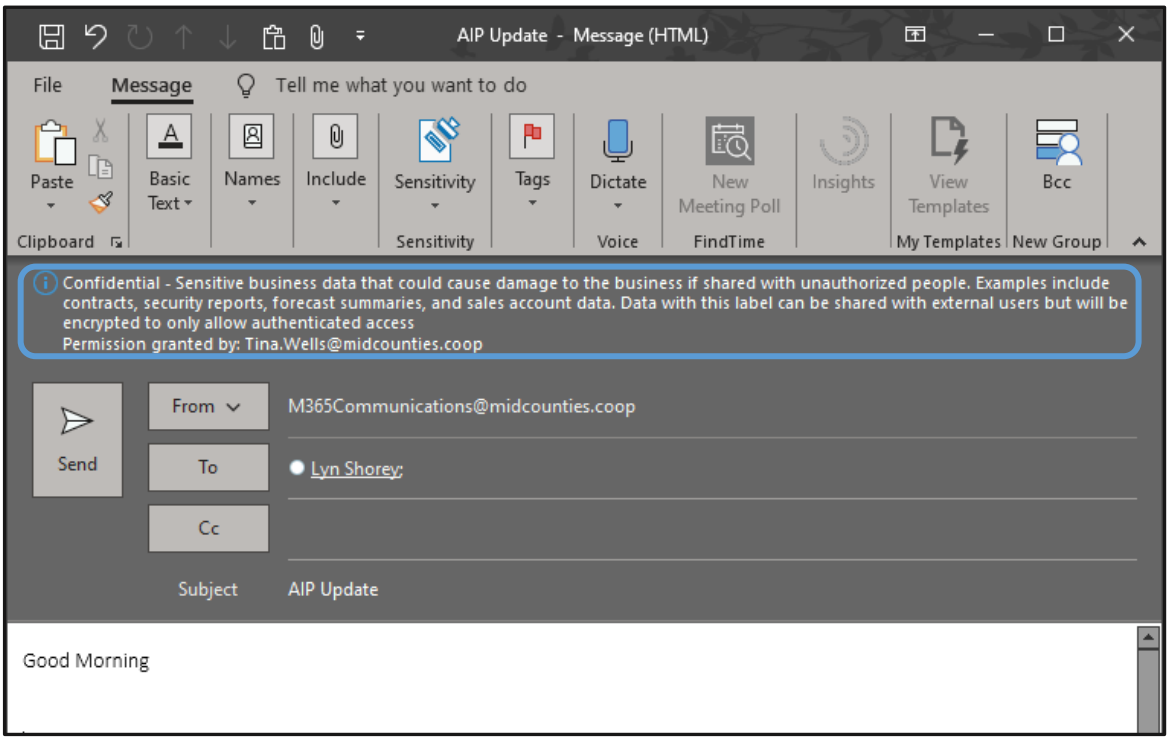


Example - Send Email with Confidential Sensitivity Applied Manually

1. Open a new email and select your internal recipient
2. Enter Subject, but do not include any sensitive text
3. The email will automatically be labelled as General
4. Click on the Sensitivity button and select Confidential from the dropdown



The email has now been manually labelled as **Confidential.**

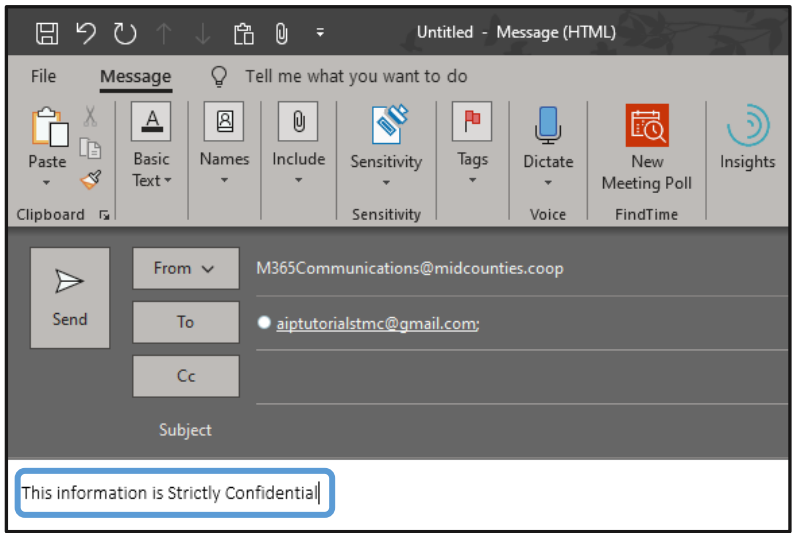
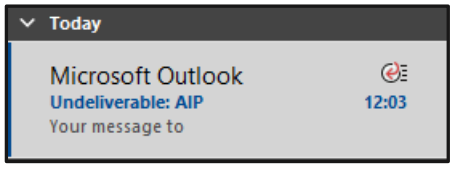
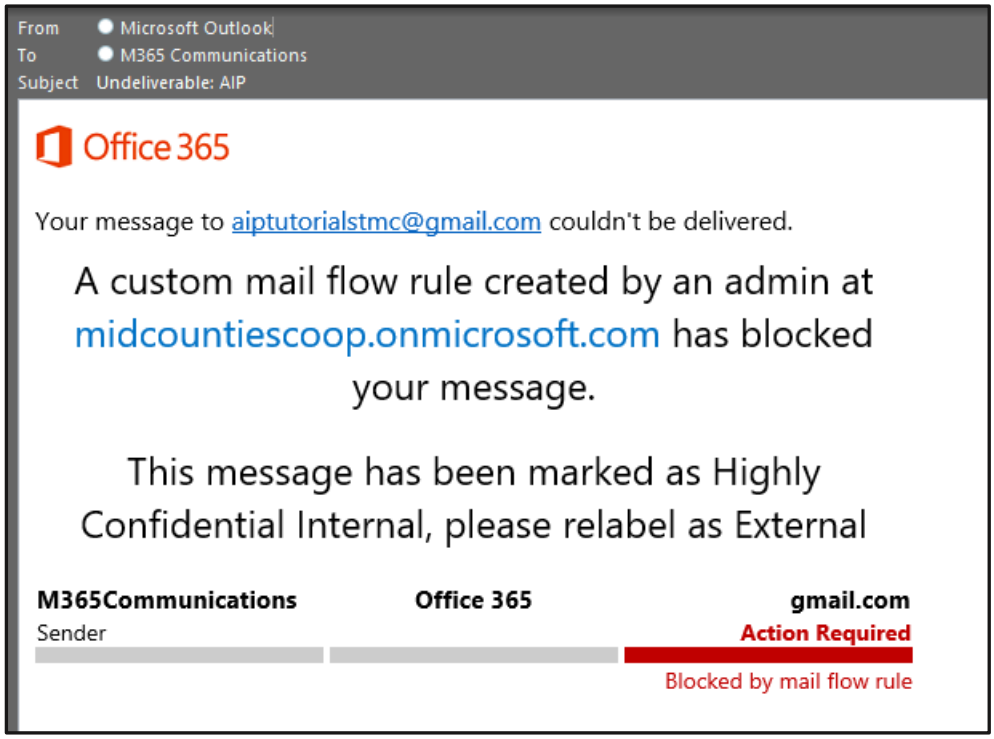


5. Add text to the email then send it

Recipient will see the email listed with the padlock shown.

Example – Sending a Highly Confidential Email to External Recipient

1. Open a new email and enter an external email address
2. Enter text in body of email **Strictly Confidential**



3. Send the email
4. The intended recipient will not receive the email
5. The sender will receive the following undeliverable email in their In Box