



IT&T



Microsoft 365

itt.com.au



IT&T Guide to Microsoft Purview

Cyber security that helps protect it.

Sensitivity labels and sharing information safely. A practical guide for your team. No technical background is required.

**One Provider.
One Call.
One Bill.**



In short: your organisation is turning on Microsoft's standard data protection features in Microsoft 365. **Sensitivity labels** will appear in Word, Excel, PowerPoint and Outlook, and data loss prevention (DLP) rules will stop confidential files and emails from being shared with people outside your organisation.

For the first 30 days, nothing will be blocked. IT&T will be monitoring while everyone gets used to the new labels. After 30 days, the sharing rules switch on.

Two optional controls may also be turned on: seven-year email retention and Microsoft 365 Copilot restrictions on Highly Confidential files.

The rollout in three phases

Nothing is blocked until Day 30. Until then, everything works as it does today.

ROLLOUT DAY · LABELS ARRIVE

You see a new Sensitivity button

A **Sensitivity** button appears in Word, Excel, PowerPoint and Outlook. New emails default to **General**. New documents default to **Confidential — All Employees**. **Nothing is blocked.**

DAYS 1–30 · QUIET MONITORING

IT&T monitors, you keep working

IT&T records what *would* have been blocked. **You still won't be blocked from anything**, and you won't see pop-ups or policy tips.

DAY 30 ONWARDS · SHARING RULES ON

Sharing rules switch on

Outlook, SharePoint and OneDrive show a policy tip when an action is going to be blocked. Sharing inside your organisation works as normal.



The four sensitivity labels

A Sensitivity button or menu appears at the top of Word, Excel, PowerPoint and Outlook. You can choose from these labels.

● Public

NO PROTECTION

Use for marketing material and public media releases.
Nothing is added. It is for information only.

● General — Anyone (unrestricted)

NO PROTECTION

Use for routine internal emails and documents that can also go to external partners.

Nothing is added. It is for information only.

Default for new emails

● Confidential — All Employees

FOOTER MARKING

Use for internal-only contracts, plans and customer data.

Adds a "Classified as Confidential" footer once visual marking is turned on. **Blocks external sharing after Day 30.**

Default for new documents

● Highly Confidential — All Employees

ENCRYPTED

Use for source code, unannounced financial results, customer personal information and payroll.

Encrypts the file so only people in your organisation can open it. Adds a "HIGHLY CONFIDENTIAL" watermark once visual marking is turned on. **Blocks external sharing after Day 30.**

In the Sensitivity menu, **General** and **Confidential** are categories you expand to reach the label itself, for example *General > Anyone (unrestricted)*. In this guide we use the short names *General* and *Confidential*.

What it looks like in your apps

A preview of what you'll see in Word, Outlook, Excel and SharePoint. The exact appearance varies between app versions.

Word · New document

Home | Insert | Layout | ...

 **Sensitivity: Confidential — All Employees** ▼

Select the button to change the label. New documents start as Confidential — All Employees.

Classified as Confidential (once visual marking is turned on)

Outlook · Writing an email

To: **someone@partner.com**
Subject: **Q4 board pack**

 **Policy tip:** This message contains content that conflicts with a policy in your organisation.

The banner appears under the To/Cc line **before** you click Send. If you send anyway, the email is stopped.

Excel · Highly Confidential workbook

 **Sensitivity: Highly Confidential — All Employees** ▼

HIGHLY CONFIDENTIAL

Encrypted. Only people in your organisation can open this file. If it ends up on a USB stick or in a forwarded email, it cannot be opened.

SharePoint · Share window

Share **budget-2026.xlsx**
To: **guest@external.com**

 **This file contains content that conflicts with a policy in your organisation.**

Share

The Share button is greyed out for external recipients. Sharing the same file with a colleague works as normal.

Choosing or changing a label

— What if I don't choose a label?

New emails automatically get General — Anyone (unrestricted). This is fine for routine emails. New documents automatically get Confidential — All Employees. This is a safe default. It only matters if you intend to share the document externally: in that case, change the label to General or Public before you send it.

Existing files and emails are not relabelled. Default labels apply only to new content.

Attaching a labelled file to an email? If the attachment has a more sensitive label than the email, Outlook automatically raises the email's label to match. You don't need to change it yourself.

— If you need to choose a lower label

- 1 Select **Sensitivity** and choose the lower label, for example *General* or *Public*.
- 2 Office asks you for a short reason. Type a sentence such as *"This document has been approved for external release."*
- 3 Select **OK**. The reason is recorded for audit purposes. It is not sent to anyone for approval, and you can continue straight away.

Good to know. Old documents and emails are *not* relabelled automatically. The default only applies to **new** content.

Encryption: Highly Confidential only

When you apply Highly Confidential — All Employees to a document:

- The file is encrypted. Anyone outside your organisation who receives it, whether through a forwarded email, a USB stick or a leak, cannot open it.
- Everyone in your organisation can open, view, edit, save, reply, reply all and forward it.
- Copying, printing and macros are allowed for this label, so co-authoring and search work normally in Office. Other encrypted labels added later may work differently. Contact IT&T support if something you expect to work is blocked.
- If you open the file offline, you have 30 days before it needs to check in with the server. Open it once while online within those 30 days to reset the clock.

What gets blocked after Day 30, and what doesn't

Only sharing of Confidential or Highly Confidential content with people outside your organisation is blocked. Everything else works as normal.

❌ BLOCKED

Outlook · Send an email labelled *Confidential* or *Highly Confidential* to an external address

A yellow banner appears before you click Send. If you send anyway, the email is stopped. You, the file owner, the person who last modified the file and the site administrator are notified.

✅ ALLOWED

Outlook · Send the same email to a colleague in your organisation

Internal email is sent as normal.

❌ BLOCKED

SharePoint / OneDrive · Share a *Confidential* or *Highly Confidential* file with someone outside your organisation

Includes anonymous links and guest invitations. The share window shows a policy message and the Share button is greyed out for external recipients.

✅ ALLOWED

SharePoint / OneDrive · Share the same file with a colleague in your organisation

Internal sharing works as normal.

❌ BLOCKED

Anyone outside your organisation who receives a *Highly Confidential* file

The file is encrypted and cannot be opened outside your organisation.

✅ ALLOWED

Anything labelled *General* or *Public*

Routine email and public material are sent and shared as normal.

Can I override a block? No. There is no self-service override. To share blocked content, contact IT&T support and explain the business need. IT&T can adjust the rule or share the file through an approved channel.

Only if enabled for your organisation

Email retention

If the optional seven-year retention policy is turned on:

- Emails older than seven years are automatically deleted from your mailbox.
- This applies to your whole mailbox, including Inbox, Sent Items and Deleted Items. Emails you delete are kept for seven years before they are permanently removed.
- You don't need to do anything. There is no setting for you to change, no warning when emails are deleted and no way to recover them after seven years.

Need to keep something longer? Records such as partnership agreements or correspondence about intellectual property should be moved out of your mailbox: save the file to a SharePoint document library, or save the email as a **.msg** or **.pdf** file elsewhere. You can also ask IT&T about a longer retention policy for your team.



Only if AI controls are enabled

Microsoft 365 Copilot

If the optional AI governance policy is turned on:

Copilot ignores Highly Confidential files when it answers questions, summarises content or looks for information. For example, if you ask Copilot to "summarise our Q4 board pack" and the board pack is labelled Highly Confidential, Copilot responds as if it can't access the file. This is intentional.

What you can do: if you need Copilot to use the file and its content allows it, change the label to Confidential — All Employees. Otherwise, open the file yourself.

Quick reference

The day-to-day essentials in one place.



Choosing a label

- Public material → **Public**
- Routine email, partners → **General**
- Contracts, plans, customer data → **Confidential**
- Payroll, source code, personal information → **Highly Confidential**



Lowering a label

- Select **Sensitivity**
- Choose the lower label
- Type a short reason
- Continue working



If you're blocked

- Read the banner: it explains why
- If the label is wrong, change it
- Otherwise, contact **IT&T support**
- Don't keep retrying: each attempt is recorded



Mobile, Mac and web

- Outlook mobile: supported
- Office for Mac and iPad: supported
- Office on the web: supported
- Other apps may not open encrypted files



Working from home

- Labels and sharing rules work anywhere: they're tied to your account, not the office network
- Open encrypted files online at least once every 30 days



Need help?

- "Should this be labelled higher?" → your manager or IT&T support
- Stuck on a block → IT&T support
- Problem with an encrypted file → IT&T support

What this guide doesn't cover

This guide covers sensitivity labels, sharing rules, and the optional email retention and Copilot controls. Your organisation may also have other security controls in place, such as Conditional Access, device compliance checks, multi-factor authentication, blocking of automatic email forwarding or expiry dates on external links. If something happens that isn't explained here, contact IT&T support.

Frequently asked questions

Will my old documents and emails be labelled automatically?

No. Only content created after the rollout receives a default label. You can label older content yourself if you want to.

Will I be unable to send any external email?

No. Only emails **labelled** Confidential or Highly Confidential are blocked from going outside your organisation. Routine General email is sent as normal.

I attached a Confidential file to a General email. Why did the email's label change?

This is expected. If an attachment has a more sensitive label than the email, Outlook automatically raises the email's label to match before it is sent. You don't need to do anything. It stops a sensitive attachment leaving under a less sensitive email label.

My document was automatically labelled Confidential, but I need to share it externally. What do I do?

Open the document, select **Sensitivity**, then **General** or **Public**. Type a short reason when asked, then share it as normal.

Do labels and sharing rules work away from the office or on my home laptop?

Yes. They are tied to your Microsoft 365 account, not to the office network.

Do labels work in Outlook on my phone?

Yes. Outlook for mobile (iOS and Android) lets you apply and view sensitivity labels.

Will a labelled file open on a Mac, iPad or in a web browser?

Yes, in Word, Excel, PowerPoint and Outlook on Mac, iOS, Android and the web. Apps from other providers may have trouble opening encrypted (Highly Confidential) files.

What happens if I email a labelled document to a personal Gmail or Hotmail account?

After Day 30, it is blocked. During the first 30 days, it is allowed but recorded.

I deleted an email that is less than seven years old. Is it really gone?

Not if a retention policy applies. Deleted emails are kept in a hidden recoverable area until they reach seven years, then permanently deleted.

How do labels affect Teams chats?

Files shared in a Teams chat are stored in OneDrive, so the same sharing rules apply as when you share directly from OneDrive. A Confidential file shared in a Teams chat with an external guest is blocked in the same way.

When I create a new Team, group or SharePoint site, I'm asked to choose a sensitivity. Which one?

You'll see three choices: General, Confidential — All Employees and Highly Confidential — All Employees. Choose the one that matches the most sensitive content you expect to keep there. Most everyday team sites are General. Use Confidential for sites with employee or customer personal information, financial information or contracts, and Highly Confidential for source code or regulated material. You can change it later.

I opened a Highly Confidential file after time offline and now it won't open. Why?

Encrypted files check your access every 30 days. If you have been offline for longer than that, the file stays locked until you reconnect. Sign in once on a connected device to open it again.

Who can I ask whether a file should have a higher or lower label?

Your manager or IT&T support. As a rule of thumb, if it contains employee or customer personal information, financial information, source code, contracts or anything regulated, use Confidential or higher.

Need help?

If sharing is blocked, a file won't open or you're unsure which label to use, contact IT&T support and explain what you need to do.

IT&T Support: **1300 482 638**

[Online version of this guide](#)