

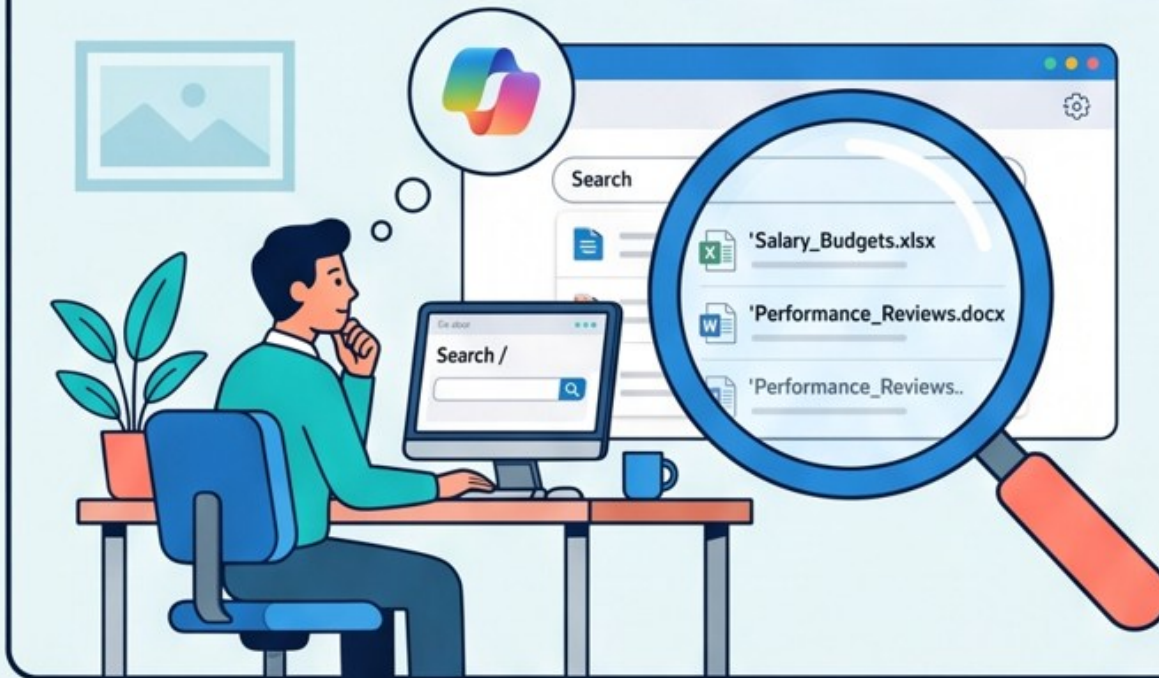
How to See & Fix Permissions in Microsoft 365

Ash Nathaniel and Keith Breazeale

Oct 13, 2026

WHY PERMISSIONS MATTER?

THE SEARCH & AI REVELATION



**If they have access,
they can find it.**

Modern M365 search and AI tools will surface any file a user has permission to see. If you leave a sensitive file open to **'Everyone in the Organization'**, it can easily appear in a colleague's search results or AI summaries.

[Search | M365 Copilot](#)

[Chat | M365 Copilot](#)

UNDERSTAND WHERE FILES LIVE

Know Your Workspace Boundaries

OneDrive (My Personal Sandbox)



You own it.
Share individual files only when needed.

Teams & SharePoint (The Team's Room)



A collaborative space. Anyone in the Team
generally has access to everything inside.

Knowing where files live is the first step to keeping them secure.



TEAMS VS SHAREPOINT

1 The Core Difference (Visual Metaphor)

Microsoft Teams:
The Active Office



Where the work happens day-to-day.
You discuss, meet, and collaborate on the fly.

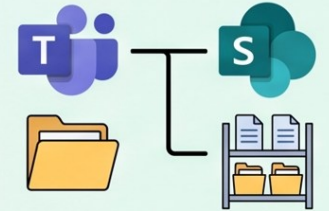
SharePoint:
The Filing Cabinet



The storage behind the scenes.
Where files are securely kept, structured, and archived.

2 Where do my files live?

Did you know? Every time you create a Microsoft Team, a **SharePoint site** is **automatically** created in the background to hold your files!



3 How to Manage Permissions (The Best Practices)

[Chat | Microsoft Teams](#)

TEAMS – WHERE DO YOUR TEAM FILES AND RECORDING ACTUALLY LIVE?

1. Uploading Files to a Channel



Saved automatically to...



SharePoint Site

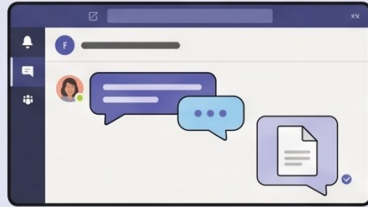
A team document library / filing cabinet

Every Team has its own SharePoint site behind the scenes. Files uploaded to standard channels **are stored here and are visible to everyone in the Team, including Guests.**



Private Channels: Have their own completely separate, locked SharePoint sites only for their specific members.

2. Sending Files in a Chat (1-on-1 or Group)



Stored in...



The Sender's OneDrive

The sender's personal OneDrive **"Microsoft Teams Chat Files"** folder.

Only chat participants are automatically granted access. If you leave the company or delete the file, other chat members may lose access!

3. Recording a Meeting



Saved based on meeting type...



Meetings in a Channel → SharePoint Site

Stored in that Team's SharePoint site. Everyone in the channel has access.



Regular Meetings (1-on-1, Group, or Scheduled)

→ **Organizer's OneDrive**
Stored in the Meeting Organizer's OneDrive ("Recordings" folder). Automatically shared with participants.

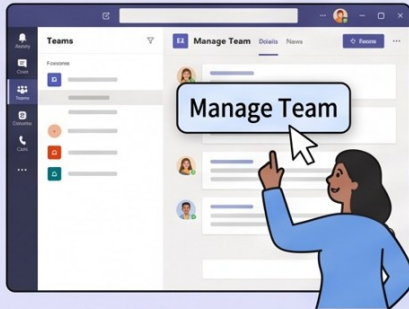


Key Takeaway: Teams is the doorway, but your files always rest in SharePoint (for teamwork) or OneDrive (for personal & 1-on-1 work).

TEAMS VS SHAREPOINT – WHERE TO MANAGE PERMISSIONS & FILES

Manage from TEAMS (Your Default)

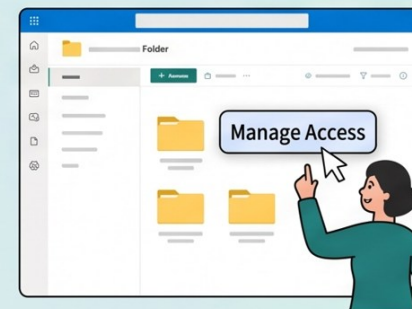
Use this for everyday teamwork



-  To add or remove people from the entire workspace
-  To invite guests or external partners to participate in conversations and files
-  **Best Practice:** Always adjust the team's membership first! It automatically syncs access to your files without manual hassle.

Manage from SHAREPOINT (Only When Needed)

Use this for specific, advanced needs



-  To grant access to someone who only needs a file, not the chats
-  To restrict sensitive **subfolders** inside a shared project
-  **Best Practice:** Avoid 'unique permissions' (breaking inheritance) on individual files unless absolutely necessary—it creates a digital maze!

 **Golden Rule:** Keep it simple! If everyone needs access, manage it in Teams. If only one person needs one file, use a sharing link in SharePoint.

ONE DRIVE – HOW TO MANAGE PERMISSIONS

1 The Core Rule:

OneDrive is Your Personal Sandbox

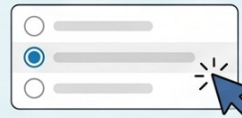


Everything in OneDrive is private to YOU by default. You are the digital “gatekeeper”—it is up to you to share safely.

Best Practice: Only share individual files when needed, never entire high-level folders.

2 The Best Practice Workflow (3 Key Steps to Share Safely)

1 Choose the Right Link Type (The Who)



Avoid “Anyone” or “People in your organization” unless strictly necessary.

Best Practice: Choose “Specific People” (the gold standard) and enter their exact email. It prevents unwanted forwarding.



2 Set Access Limits (The What)

Viewing ☒
Blocking ☐

Decide on “Can View” or “Can Edit”.

Best Practice: If they only need to read it, use “Can View” and toggle on “Block Download” to prevent offline copies.



3 Add an Expiration Date (The When)



Set it to expire in 7 or 14 days for temporary collaboration.

Best Practice: Letting it auto-expire saves you from having to remember to revoke it later!

[My files - OneDrive](#)

CHOOSING THE RIGHT SHARING LINK

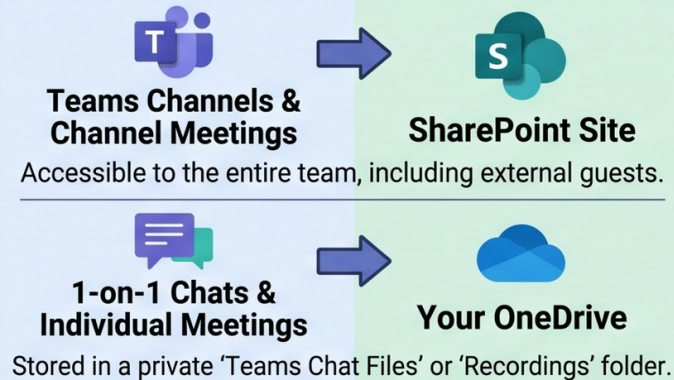
Link Option	What It Really Does	Recommendation
People you choose (Specific People)	Only users whose exact email address you enter can open the file. If forwarded, recipients cannot access it.	DEFAULT CHOICE
People in your org	Anyone with a company account who gets or searches for the link can view/edit. Discoverable via search and AI assistants.	COMPANY PUBLIC
Existing access	Creates a clean direct link without changing or expanding permissions. Safe for copy-pasting to teammates.	SAFE SHORTCUT
Anyone with the link	Anonymous link open to anyone across the entire internet without logging in. Usually blocked or disabled.	AVOID / RESTRICTED

The "Copilot & Search" Reality Check

Microsoft 365 search tools and AI assistants only display documents a person is permitted to view. If you leave a file shared with "People in your organization," your colleagues may see sensitive notes appear in their search results or recommendations. Always prefer "People you choose" when sharing sensitive data.

DEMO

1. Where Do Your Files & Recordings Actually Live?



2. Managing Permissions in Teams

1. Click the **three dots (...)** next to your Team.
2. Select **"Manage Team"**
3. Review, add, or remove members and guests.

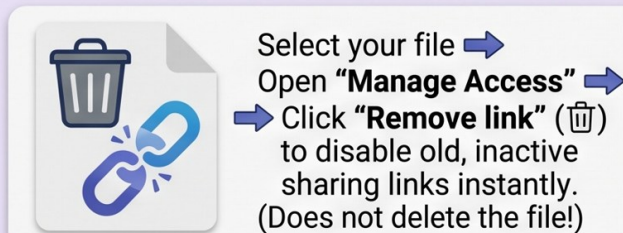


3. Why You Should Manage Permissions via Teams

The Gold Standard for Teamwork

- ✓ **Auto-Sync:** Adding someone to a Team automatically gives them access to its files—no manual SharePoint tweaking needed.
- ✓ **Offboarding:** Removing a member from the Team instantly revokes their access to everything inside.
- ✓ **Visibility:** Keeps all your project permissions clear, organized, and visible in one simple spot.

4. Removing Stale Links (The Cleanup)



5. Managing Permissions in OneDrive (Control Your Sandbox)

👉 Shared With Me

Files others have shared with you. To stop seeing them, click **"Remove from shared list"** to keep your inbox and interface tidy.



👉 Shared By You

The critical audit.

Click **"Shared"** in the left menu, then **"Shared by you"** to review who has access to your folders and files. Click **"Manage Access"** to revoke permission.



[My files - OneDrive](#)

Q&A



Thank You

Ash Nathaniel & Keith Breazeale