Before you switch on Copilot: 10 Microsoft 365 readiness checks

A working checklist for IT and security leaders, with a pilot test you can run in an afternoon

Copilot can surface content your employees already have permission to open. It does not create new access. The risk is access you did not mean to grant. Work through these ten checks before rollout, and again after any big change.

	#	Check	What to verify	What to do if it fails
SHARING				
☐	1	**"Everyone except external users"**	Sites, libraries, folders or files granted to "Everyone except external users" or "Everyone". Anyone in the company, and Copilot, can find this content.	Replace it with a named group or specific people. Start with HR, finance and client sites.
☐	2	**Public team sites**	Microsoft 365 group-connected team sites set to Public. Anyone in the company can find their content.	Make the site private, or restrict content discovery while you review it.
☐	3	**"People in your organization" links**	Company-wide links on files with personal or financial data. Anyone who opens the link gains access, and Copilot can then use the file for them.	Replace with specific-people links, and make specific people the default link type.
☐	4	**"Anyone" links**	Anonymous links, especially with no expiry. A risk in their own right: no sign-in, no audit trail.	Set an expiry, remove unneeded links, or turn Anyone links off.
☐	5	**External sharing links older than 12 months**	Links to guests and outside parties created more than a year ago.	Confirm each one is still needed. Remove the rest.
OWNERSHIP				
☐	6	**Sites or libraries without an active owner**	Owners who have left, or groups with no owner at all.	Assign an owner who can approve and remove access.
☐	7	**Files owned by former employees**	OneDrive content and shared files left behind by people who have gone.	Transfer ownership, then review who still has access.
☐	8	**Inactive sites**	No activity for 12 months or more. Old content can surface as if it were current.	Archive, restrict or delete in line with your retention schedule.
SENSITIVE DATA				
☐	9	**Sensitive data behind broad access**	Social Security numbers, bank details, health or HR records in the places found in checks 1 to 5.	Restrict or move those files first. This needs a scan of file contents, not settings.
☐	10	**Pilot-user test**	Test Copilot with a few typical, non-admin accounts before wide rollout.	Fix any unexpected access at the source, then test again. Steps on page 2.

How to run the pilot-user test

1. **Pick three to five people with typical access:** someone in operations, someone client-facing, a manager. Not IT administrators.
2. **With their agreement, ask Copilot what an employee should not be able to answer.** For example: "What is [colleague]'s salary?", "List client Social Security numbers", "Summarize the latest board pack", "What has HR written about [name]?"
3. **Record anything that comes back that should not, and where it came from.**
4. **Fix the access at the source** using checks 1 to 9, not just the answer Copilot gave.
5. **Ask the same questions again** before you widen the rollout.

Tell HR and the people taking part what you are doing before you start, and use test questions that fit your business.

Related Microsoft 365 check: mail forwarding

Mailboxes that forward automatically to outside addresses can send sensitive attachments out of the business. It is a different control with a different failure mode, and worth checking in the same review.

Where Priivacy fits alongside Microsoft

Microsoft 365 gives you sharing reports and oversharing assessments, and Purview can classify content once it is configured. Priivacy adds a different view: it reads the files themselves for 60 types of personal data, and flags a risky setting where real personal data sits behind it. That turns a long list of settings into a short list of fixes. It runs inside your environment and covers file servers and laptops in the same pass.



Illustrative example. Seven of Priivacy's 35 Microsoft 365 posture tests flag a setting only where personal data sits behind it.

Run the checks on your own tenant, free

USC Data will scan up to 20,000 files and run the Microsoft 365 posture tests inside your environment, then walk you through the findings in 30 minutes.

Get the free 20,000-file scan

Sources: Microsoft Learn, How shareable links work in OneDrive and SharePoint; Microsoft Learn, Microsoft 365 Copilot best practices with SharePoint. General guidance, not a substitute for your own security review. Feature availability depends on your Microsoft 365 licenses.