



Product Policy Document: Microsoft 365 Copilot (the add-in, suite-wide)

Product and vendor: Microsoft 365 Copilot and Microsoft 365 Copilot Chat, Microsoft.

Way of working: The add-in, at suite scale. Copilot is an AI layer inside Word, Outlook, Teams, Excel, and the rest of the firm's Microsoft 365 subscription, plus a chat surface of its own.

Status: Ready to adopt, subject to the signup-time confirmations in Section 3 and with web grounding treated as a separate, unapproved data path. Adopting it is still adding one more cloud vendor that holds client data; the setup steps exist to make that true on paper and in settings, not just in marketing.

Implements: Model Firm AI Use Policy (42/02). Exhibits: 08 (Microsoft enterprise data protection page, dated 2026-05-29, retrieved 2026-08-07); 11 (Wave 1 exhibits pass memo).

Document date: 2026-08-07.

1. What this is

Copilot is the AI feature set inside the Microsoft 365 subscription most firms already have. It reads the open document, the mailbox, and, through Microsoft Graph, whatever else the signed-in user can reach in the firm's tenant (the firm's own partition of Microsoft's cloud), and it drafts, summarizes, and answers against that material.

Be clear-eyed about what adopting it means. The firm is not "staying inside its own walls"; the tenant is Microsoft's cloud, and enabling Copilot deepens the firm's dependence on one vendor that now holds the files, the email, the credentials, and the AI layer over all of it. Microsoft's enterprise data protection (EDP) commitments are real and contractual: prompts and responses are covered by the Data Protection Addendum and Product Terms, with Microsoft as a data processor, under the same terms as Exchange email and SharePoint files, and they are not used to train foundation models (Exhibit 08). Microsoft can also be breached, subpoenaed, or wrong, like any other vendor. The policy's answer is the same as for every tool: a row, a configuration, and the duties unchanged.

Two structural facts drive the setup steps. First, **Microsoft picks the models.** The customer does not choose or pin what serves a Copilot request, and the set has already changed once: Anthropic models now serve some Copilot features (Exhibit 08, footnote 3). Second, **web queries leave the envelope.** When Copilot grounds a response with web search, those queries go to Bing, which "operates separately from Microsoft 365," under the consumer-grade Microsoft Services Agreement, with Microsoft acting as an independent data controller rather than the firm's processor (Exhibit 08). A checkbox changes the legal envelope mid-session.

2. The Approved Tool List row (implements Section 3)

Microsoft 365 Copilot (suite). Tier / account type: Firm's M365 commercial subscription with EDP; Copilot licenses per seat | **Training disabled:** Not used to train foundation models (Exhibit 08) | **Memory off / scoped:** [confirm current Copilot memory and personalization controls at signup; see Section 3, step 4] | **Retention terms:** Firm-controlled: Copilot interactions follow the firm's own M365 retention policies and support audit (Exhibit 08) | **Permitted input tier:** Tier 2, with web grounding off | **Agentic capabilities:** Agents exist in Copilot and are off or admin-restricted; each agent carries its own privacy terms (Exhibit 08) | **Approved date:** [date of adoption] | **Notes:** Web queries to Bing are outside the DPA envelope; Microsoft picks and changes the models

3. Required setup (implements Sections 3 and 4)

Steps 1 through 6 are the Administrator's (with the firm's IT support); steps 7 and 8 are every user's.

1. **Confirm the subscription layer.** EDP applies to commercial M365 subscriptions under the DPA and Product Terms; the specific controls vary by plan (Exhibit 08, footnote 1). Identify the firm's plan, confirm Copilot on that plan carries EDP, and file the confirmation. Consumer Copilot (personal Microsoft accounts) is prohibited for client work.
2. **Disable web grounding for client work.** This is the single most important switch in this document. Locate the tenant control for Copilot web search, turn it off (or restrict it to users who do only Tier 1 work), and record the setting path and date. If the firm wants web grounding for public research, that is a Tier 1 activity on its own terms; it must not run in sessions that touch client material.
3. **Fix permissions before turning Copilot on.** Copilot respects the firm's existing identity model and permissions (Exhibit 08), which means it also inherits every permissions mistake: an overshared SharePoint folder that nobody browsed is now one prompt away from any user who technically has access. Before enablement, review site and folder permissions against matters, and confirm ethical walls are real in SharePoint, OneDrive, and Teams, not just in the case management system. This is the policy's memory and cross-matter rule (Section 4) applied to a tenant.
4. **Set memory, personalization, and agent controls.** Confirm what Copilot currently retains across sessions for personalization, and disable or scope it per the policy's memory rule [Exhibit 08 does not document these controls; record what the admin center shows at signup]. Agents are off or restricted to vetted ones; Microsoft itself says each agent carries its own privacy terms (Exhibit 08), which makes an agent an unvetted tool by default under Section 3.
5. **Turn on the audit trail.** Copilot supports audit of interactions and follows the firm's retention policies (Exhibit 08). Configure both deliberately: retention per the firm's records schedule, audit on. This is a place where the suite genuinely beats a chatbox: the firm can hold its own record.
6. **Harden the credential layer.** The tenant now gates the files, the mail, and the AI over both. MFA for every account, no shared logins, offboarding same day. A phished credential here is not one inbox anymore; it is a natural-language search interface over everything that account could see.
7. **Users: Copilot's reach is your reach.** Anything you can open, Copilot can read into a session. Work in the matter you are in; do not use Copilot as a firm-wide search tool for curiosity.
8. **Users: complete training** on this document before first client use, including the web-grounding rule and the tracked-changes rule in Section 5.

4. What may go in (implements Section 4)

- **Tier 1:** permitted on any properly licensed seat.
- **Tier 2 (client documents and matter facts):** permitted once the Section 3 steps are complete, because with web grounding off, prompts, responses, and Graph data sit under the DPA envelope (Exhibit 08). Opening a client document in a Copilot-enabled session is a Tier 2 input of the whole document, exactly as the policy's Section 5 states for add-ins.
- **Tier 3:** prohibited absent informed client consent and Administrator approval, as everywhere.

This product's specific hazards are scope and the envelope switch. Scope: the unit of exposure is not the paste but the tenant; a prompt can pull from anything the user's permissions reach, so the permissions work in Section 3, step 3 is a confidentiality control, not an IT nicety. The envelope switch: with web grounding on, parts of the session leave the DPA envelope for consumer-grade terms; that is why the switch is off, and why its state is recorded on the row.

5. Verification (implements Section 5)

Unchanged: the ladder, the statute check, the no-delegation rule. Product notes: Copilot edits inside Word must run as tracked changes or as saved before-and-after versions compared before acceptance; silent in-place editing is prohibited (policy Section 5, verbatim duty). Copilot's strength is drafting against the firm's own material; its citations to law are not grounded in a legal corpus and get the full ladder every time.

6. The record (implements Sections 8 and 10)

Better than the chatbox, if configured: Copilot interactions can be audited and are subject to the firm's own retention policies (Exhibit 08), so the firm can hold a record without a per-session export habit. The matter file still gets the material record for any session that shaped work product (Section 10); the audit log locates sessions, it does not narrate them.

Billing: Copilot seats are subscription overhead under Section 8. No pass-through.

7. Vendor facts and evidence grades

Prompts, responses, and Graph data covered by the DPA and Product Terms; Microsoft as processor. Source: Exhibit 08 | **Grade:** Published, pointing at contract instruments (the firm's M365 agreement incorporates them; read at adoption) | **Date:** Page dated 2026-05-29

Not used to train foundation models. Source: Exhibit 08 | **Grade:** Published | **Date:** Same

Copilot inherits permissions, sensitivity labels, retention policies; supports audit. Source: Exhibit 08 | **Grade:** Published | **Date:** Same

Web queries go to Bing outside M365, Microsoft as independent controller, consumer-grade terms; no HIPAA/BAA coverage for them. Source: Exhibit 08 | **Grade:** Published | **Date:** Same

Anthropic models now serve some Copilot features (model set changed after launch, without customer action). Source: Exhibit 08, footnote 3 | **Grade:** Published | **Date:** Same

Agents carry their own privacy terms; Microsoft directs customers to check each one. Source: Exhibit 08 | **Grade:** Published | **Date:** Same

Not established: the firm's specific plan's control set (footnote 1's variability); the current memory/personalization controls; the exact admin paths for the web-grounding switch. All are sign-up-day items. **The ask for the vendor (or the firm's Microsoft partner):** the current admin documentation for disabling Copilot web search tenant-wide, the Copilot personalization/memory control documentation, and written confirmation of which Copilot features on the firm's plan route to which model providers.

8. Re-vetting triggers (implements Section 12)

1. **Model routing changes.** It already happened once (Anthropic added). Re-check Exhibit 08's source page at every annual review and on any Microsoft announcement about Copilot models.
2. **Web grounding defaults or control granularity change.**
3. **Agents become default-on,** or an agent gets embedded in a workflow the firm uses.
4. **DPA or Product Terms changes** at renewal.
5. **New Copilot surfaces** (a new app in the suite gets a Copilot): each new surface inherits this row only if it stays inside the EDP envelope; confirm before use.
6. **A Microsoft security incident touching the tenant layer:** re-run the credential and permissions review, and reassess the single-vendor concentration this document opens with.