

25 FAQs about Copilot

In the 350+ organizations that my colleagues and I work with about Copilot, common questions and concerns are top of mind. This chapter summarizes what is seen and how some are proceeding.

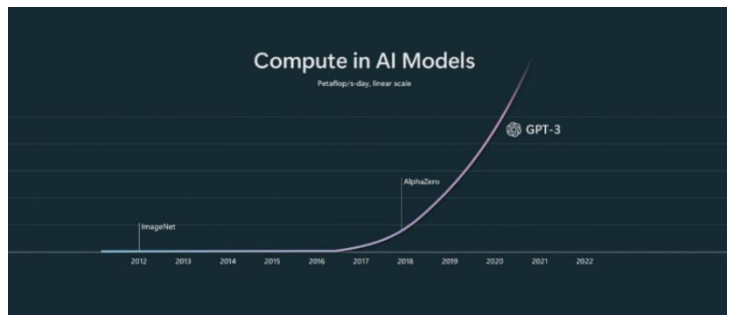
If your question isn't found here, it may not be frequent enough. Check the specific app chapters throughout the book for the topic you're pondering.

Why the licensing and Pay as You Go fees?

Yes, Microsoft 365 Copilot costs \$30/user/month. And yes, advanced features like agents and Cowork run on a metered, pay as you go basis. As a reference point, one could compare to ChatGPT Enterprise from Open AI, which lists for \$30/month, or at least to ChatGPT Business at \$20.

Why a fee? It's no secret that large languages model uses a lot of GPUs to search and

produce relevant content. Microsoft provided this visual aid at right, comparing current AI computing resources to past. Newer models use even more compute.



Will our Data Train the LLM?

No, partitions are in place to only allow your authorized users to access your SharePoint, OneDrive, Exchange, etc. The prompts and responses your Copilot users will not cross organizational boundaries, and won't be used to train the large language models.

Is my Organization's Confidential Data Secure?

From the LLMs, yes. But from overexposure internally, no. Minimizing permissions in SharePoint and protecting confidential data at the file level with Purview are recommended ways to limit this risk. See Chapter 17 on Securing Copilot.

Is Copilot safe? Will it hallucinate?

Microsoft has used the term “usefully wrong” instead, but there's been a lot of press about hallucinating. ChatGPT (and other models) have demonstrated an inability to reason over controversial or dangerous prompts, which has led to sometimes unpredictable results.

This is not unexpected, because models have no moral compass or filter. OpenAI's CEO Sam Altman has suggested to the US Congress that regulations be put in place.¹ Microsoft is working on safe and responsible AI² and Anthropic is widely known for acknowledging that LLMs continue to be a research initiative.

To reduce the risks of hallucination, people should be trained to make optimal prompts, and acknowledge that by using Copilot at work, they accept such risks and will do their part to limit any liability.

Does Data need to be in Microsoft 365?

Yes, *Copilot's full functionality* will apply to data in SharePoint, OneDrive, Teams, Exchange, etc.

However, if the data that the organization finds most valuable is not in Copilot, there are likely a few choices.

1. The manufacturer of the app where the vital data lives may provide a GenAI interface for their app. Many SaaS providers are building copilots.
2. Connectors or Model Context Protocol server can extend Copilot's capabilities into compatible data sources (see Chapter 22, Extending Copilot)
3. If you're using databases or other AI systems in Azure, then explore Foundry or other Azure AI services directly.

There are a growing number of Copilot Connectors and Model Context Protocol servers, which make it possible to connect external data sources. Connectors are APIs that connect to specific data sources. They pull data from the external source, transform it into a format that can be indexed and searched, and then push it to the Microsoft Search index. Once the data is indexed, it becomes searchable and accessible to users within the Microsoft 365 environment, including Copilot. That data is primarily used to help 'ground' Copilot. In other words, Copilot can add *context and insights* from the third-party source, before a prompt is sent to the LLM. You can read more about Connectors and MCP servers in Chapter 22.

How do I Keep up with the Rapid Changes?

It won't be easy! To help, this book is also available online, where it is frequently updated. See <https://stegh.info/Book%20Chapters.html> for the latest, and follow me on LinkedIn <https://www.linkedin.com/in/christianstegh/> for posts about updates and other news.

¹ <https://www.npr.org/2023/05/16/1176508612/a-leader-in-artificial-intelligence-is-urging-congress-to-regulate-it>

² <https://www.microsoft.com/en-us/ai/responsible-ai>