



COPILOT FAQs

ANSWER MICROSOFT COPILOT SECURITY CONCERNS WITH CONFIDENCE

Customers are excited about Microsoft Copilot, but many still have questions around security and readiness.

This guide is designed to help you answer common concerns across five key areas in a simple and reassuring way.

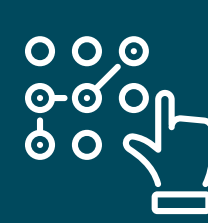
USE THESE FAQs AND THEIR SUGGESTED RESPONSES TO:



Build trust in AI conversations



Position security as an enabler, not a blocker



Guide customers towards a practical next step

DATA AND PRIVACY

Does Copilot access all our company data?

No. Copilot only accesses information users already have permission to see within Microsoft 365.

Could sensitive information be exposed?

Without the right data governance controls, oversharing risks can already exist within organisations. Reviewing permissions, protecting sensitive data, and applying policies through solutions like Microsoft Purview can help create a safer foundation for AI adoption.

SECURITY AND COMPLIANCE

Does Copilot support compliance requirements like GDPR?

Microsoft provides security, compliance, and governance capabilities designed to help organisations support regulatory and compliance requirements.

How can we protect sensitive business data?

Solutions like Microsoft Purview can help you classify, protect, and govern sensitive information through tools like Information Protection and Data Loss Prevention.

READINESS AND CONTROL

Do we need to prepare our environment before using Copilot?

Yes. A readiness assessment identifies security gaps and shortfalls that need to be addressed before wider AI adoption. This enables confidence in your roll out and helps you achieve maximum productivity from your tools.

What are the biggest risks to AI readiness?

Weak identity controls, unprotected data, fragmented security tools, and limited governance are some of the most common barriers to secure AI adoption. A readiness assessment can help strengthen your foundations for Copilot use.

USER EXPERIENCE AND RISK

Will Copilot replace human decision-making?

No. Copilot is designed to support employees by helping reduce repetitive work, summarise information, and improve productivity – not replace human judgement.

Will AI make security risks worse?

AI can increase the visibility of existing security and governance gaps. That is why organisations should strengthen protection across identities, devices, and data with a security-first approach using solutions like Microsoft Defender, Entra, and Purview.

GETTING STARTED

What is the first step to adopting Copilot securely?

Start with a readiness assessment to understand your current environment, identify risks, and build a roadmap for secure AI adoption.

Do we need to deploy everything at once?

No. Most organisations start with small pilots, focused use cases or targeted security improvements before scaling further. Through our workshops, we can help you identify potential use cases for your business.

TURNING CUSTOMER QUESTIONS INTO OPPORTUNITIES

Copilot delivers significant productivity gains for your customers when supported by the right security foundations.

At Westcoast Cloud, we can help you navigate customer questions, supporting you with assessments, recommendations, and guidance that keep conversations moving.

GET IN TOUCH TO DISCUSS YOUR NEXT OPPORTUNITY