

READINESS GUIDE

AI for Small Business

Practical ways to use AI, what to weigh before adopting, and how to build a realistic roadmap.

1**Why AI matters for small business now**

The conversation has shifted

A few years ago, AI was a topic for large enterprises with dedicated data teams. That changed. Tools built on large language models are now accessible through software your team likely already uses: Microsoft 365, your CRM, your accounting platform. The question for small businesses is no longer whether AI will affect how you work. It is whether you will adopt it thoughtfully or reactively.

The short version

AI can save real time on routine work, but only with the right data hygiene, security, and guardrails in place. The businesses that benefit most are not the ones that rush in. They are the ones that start small, pick one measurable use case, and build from there.

The opportunity for small businesses is genuine. AI tools are good at repetitive, language-based tasks: drafting, summarizing, sorting, routing, and extracting. These are exactly the tasks that consume disproportionate time in a small office. A five-person team that saves two hours per week per person reclaims the equivalent of a part-time role.

But the risks are also real. Consumer AI tools learn from what you feed them. An employee who pastes a client contract, a patient record, or financial data into a public chatbot may be violating confidentiality obligations they do not even know they have. Without a clear policy and basic security guardrails, the efficiency gains are not worth the exposure.

2

Where AI actually helps SMBs

Focus on problems you already have, not problems AI might solve in theory. The use cases below are practical, proven, and appropriate for businesses with 5 to 75 employees. None require a dedicated data team.

Customer support and chat. AI-assisted chat tools can handle common questions, qualify leads after hours, and route inquiries to the right person. Most integrate with your website or Microsoft Teams. The key is keeping a human in the loop for anything sensitive or complex.

Drafting and editing content. Email responses, proposals, job postings, policy documents, and marketing copy all benefit from AI-assisted drafting. Treat the output as a first draft that a person reviews and edits, not a finished product.

Summarizing documents and meetings. Microsoft 365 Copilot can summarize long email threads, meeting recordings, and Word documents in seconds. This is one of the highest-value, lowest-risk starting points for most small businesses already on Microsoft 365.

Data entry and extraction. AI tools can pull structured data from invoices, forms, and scanned documents and route it into your systems. This works well for accounts payable, onboarding forms, and intake processes. Accuracy still needs human spot-checks.

Scheduling and admin automation. AI scheduling assistants can propose meeting times, send reminders, and manage calendar conflicts without back-and-forth email. These tools connect to Microsoft 365 or Google Workspace and require minimal setup.

Sales follow-up. CRM platforms with AI features can flag deals that have gone quiet, suggest next-step actions, and draft follow-up emails in your voice. This keeps pipeline hygiene from depending entirely on a salesperson's memory.

Basic analytics and forecasting. Tools built into Microsoft 365 can identify trends in your sales, cash flow, or inventory data and surface them in plain English. These features are most useful when your underlying data is clean and consistently entered.

IT and security monitoring. AI-driven anomaly detection is already built into many security platforms. It flags unusual login locations, suspicious file access, and behavioral outliers that rule-based tools miss. Your managed IT provider should already be running this layer.

A useful filter: Before adopting any AI tool, ask: Is this task currently eating real time? Is the output something a person will review before it affects a customer or a record? If yes to both, it is a reasonable candidate. If the output goes directly to a customer or into a system of record without review, add more structure first.

3

What to consider before adopting AI

Moving too fast on AI without addressing these factors first is how small businesses create problems they did not anticipate. Work through this list before your first pilot.

Data in public AI tools

Never paste client data, protected health information, financial records, employee records, or anything subject to a confidentiality agreement into a consumer AI chatbot. These tools may use submitted content to improve their models or store it in ways you cannot audit. This is not theoretical: regulators in healthcare, finance, and legal services have already begun citing AI-related data handling as a compliance risk. If your team uses AI tools without a written policy, assume they are making these mistakes today.

- **Data privacy and confidentiality.** Know what data classifications your business handles and which AI tools are approved for each. Microsoft 365 Copilot, deployed within your Microsoft tenant, is a different risk profile than a public consumer tool. Establish the boundary in writing.
- **Security and access controls.** AI tools are only as secure as the accounts and data they connect to. Before enabling AI features, verify that your Microsoft 365 environment has multi-factor authentication enforced, that inactive accounts are removed, and that permissions follow least-privilege principles.
- **Accuracy and human review.** AI output is plausible, not reliable. It will sometimes be confidently wrong. Any process that feeds AI output directly into customer-facing communications, financial records, or compliance documentation without human review is a risk waiting to surface.
- **Vendor lock-in and cost creep.** AI features are often bundled into subscription tiers. Before enabling them, understand what you are committing to and whether the cost is justified by measurable time savings. Costs tend to grow as usage scales.
- **Employee training and change management.** Tools your team does not understand or trust will either be ignored or misused. Budget time for training, address the job-security anxiety directly, and designate someone to own AI tool policies internally.
- **Regulatory and compliance exposure.** If your business operates under HIPAA, financial regulations, or legal confidentiality rules, any AI tool that touches regulated data must be evaluated against those requirements before use. When in doubt, get written guidance from your compliance advisor.

Before you enable any AI add-on: Check whether the tool processes data inside your existing secure environment (such as your Microsoft 365 tenant) or sends it to an external service. The distinction matters for compliance, data residency, and your ability to audit what was shared.

4

An AI readiness self-assessment

Work through this checklist before committing to any AI tool or investment. It takes about ten minutes and gives you a realistic picture of where you stand.

Do you have a written policy on what data can be entered into AI tools?

Is your Microsoft 365 environment secured with multi-factor authentication on all accounts?

Are inactive and former-employee accounts removed promptly from your systems?

Do you have clean, consistently entered data to work from in the area where you want to use AI?

Have you identified one specific, measurable use case to start with?

Is someone on your team accountable for reviewing AI output before it affects customers or records?

Do your employees know which AI tools are approved and which are off-limits for work use?

Have you evaluated the AI tool against any compliance or regulatory obligations your business has?

Do you have a way to monitor and measure whether the AI tool is actually saving time?

Is your managed IT provider aware of the AI tools you are considering, and have they reviewed the security implications?

Reading your score

- **8 to 10 checked:** You have a strong foundation. A focused pilot is a reasonable next step.
- **5 to 7 checked:** You are partially ready. Address the unchecked items before expanding AI use beyond low-stakes tasks.
- **Fewer than 5 checked:** Start with the foundation: policy, access controls, and data hygiene. A premature AI rollout without these creates more risk than it solves.

5

Building a realistic AI roadmap

The businesses that get lasting value from AI are not the ones that adopt every new tool as it appears. They are the ones that pick a deliberate path, measure honestly, and build incrementally. The four phases below apply to businesses of almost any size.

Phase 1: Secure the foundation and set an AI use policy. Before any AI tool goes live, confirm that your Microsoft 365 environment has MFA enforced, that permissions are current, and that you have removed former-employee accounts. Then write a short AI use policy: which tools are approved, what data categories may and may not be used with each, and who is responsible for reviewing AI output. This does not need to be long. One page is enough to start.

Phase 2: Pick one high-value, low-risk pilot and measure it. Choose a single, well-defined task that currently takes real time and produces reviewable output. Meeting summarization, first-draft emails, and invoice data extraction are good candidates. Define success before you start: how many hours per week should this save? Run the pilot for 30 to 60 days, track the numbers honestly, and decide whether to expand based on what you actually measured, not how the tool felt.

Phase 3: Train your team and document what works. Once a use case is proven, write a brief internal guide: what the tool does, how to use it correctly, what to watch for, and how to flag problems. Hold a short team session. Address the questions employees actually have rather than assuming the tool is self-explanatory. Document which prompts and workflows produced good results so the knowledge stays with the organization, not just one person.

Phase 4: Expand deliberately and review quarterly. Add one use case at a time. Each new tool or feature should go through the same evaluation: what problem does it solve, what are the data and security implications, how will we measure success, and who owns the review process. Set a calendar reminder to review all active AI tools quarterly: are they still saving time, are costs still justified, and have any new compliance considerations emerged?

One principle worth keeping: Measure every AI pilot against a simple question: did this free up meaningful time for work that requires a human? If the answer is not clearly yes after 60 days, move on. Not every use case will work for every business, and that is fine.

Not sure where to start with AI?

We can walk through your current environment and help you identify one practical, low-risk pilot that fits your business. No obligation, no jargon, just a clear conversation.

Talk to PTS

hello@phantomts.com
phantomts.com
Indiana & Michigan, since 2010

This guide is provided for general informational purposes by Phantom Technology Solutions and does not constitute legal, regulatory, or professional advice. Every organization is different. Use it as a starting point, not a substitute for a tailored assessment. Copyright Phantom Technology Solutions. You may share this document freely in its original, unmodified form.