

AI Starter Kit for Small Businesses

A plain-English guide for small shops, trades, and beginners

DRAFT v0.1 for review. Prepared October 2026.

Educational information only. This is not legal, HIPAA, privacy, tax, or compliance advice. Vendor terms and prices change often; verify everything with the vendor before you buy or rely on it. For your specific situation, talk to a qualified attorney or compliance professional.

What's in this kit

1. How to use this kit
 2. The 5-step beginner path
 3. Green / Yellow / Red data rules
 4. Medical and other sensitive data (BAAs)
 5. What it really costs (prices checked Oct 2026)
 6. Checklists
 7. Prompt templates you can copy
 8. One-page AI policy template
 9. Pilot tracking worksheet
 10. When to call a professional
 11. Sources
-

1. How to use this kit

This kit is for owners of small businesses (a plumbing outfit, a machine shop, a cleaning service, an electrician, a small retail store, a two-person office) who want to try AI tools without wasting money or putting customer information at risk.

You don't need to be technical. You'll do three things:

- **Pick a small job for AI to help with.** Something you already do every week.
- **Use the AI you may already pay for.** If you use Microsoft 365 or Google Workspace for email, start there.
- **Try it carefully for a few weeks, then decide.** Keep it only if it clearly saves time.

Read Sections 2 and 3 first. Everything else is reference material you can come back to.

2. The 5-step beginner path

Step 1: Pick 1 to 3 routine text tasks

Good first tasks happen every week, are mostly writing or reading, and won't cause real harm if the AI gets something wrong (because a person checks it first). Ideas:

- **Email and follow-ups:** replying to customers, following up on quotes, confirming appointments.
- **Customer questions:** drafting answers to the questions you get over and over (hours, service area, "do you work on X?"). A person approves every answer at first.
- **Quotes and job write-ups:** turning your rough notes into a clean, polite quote or job summary.
- **Bookkeeping help:** drafting friendly invoice reminders or explaining a report in plain words. Your bookkeeper or accountant still signs off.
- **Summaries:** shortening long PDFs, manuals, supplier terms, or meeting notes.
- **Shop documents:** turning "how we do it" notes into a step-by-step procedure (SOP) or checklist.
- **Marketing:** website text, product or service descriptions, social posts.

Write your tasks here:

- 1.
 - 2.
 - 3.
-

Step 2: Use the AI built into the tools you already have

Before buying anything new, check what's already included:

- **Microsoft 365:** Copilot Chat comes at no extra cost with eligible Microsoft 365 plans.
- **Google Workspace:** Gemini in Gmail is included in Google Workspace plans, including Business Starter.

Using built-in tools means one less account, one less bill, and your data stays under the business account you already manage. Don't build custom tools or connect lots of apps yet.

Step 3: Run a small pilot (1 to 2 people, a few weeks)

- Pick **one or two people** who are curious and careful.
- Run it for **2 to 4 weeks**.
- Use **Green data only** during the pilot (see Section 3).
- Have a person review everything before it goes to a customer.

Step 4: Measure the time saved

Use the worksheet in Section 9. For each task, write down:

- About how many minutes the task took before, and how many with AI (including checking time).
- How often the AI's draft needed big fixes.
- Whether customers got answers faster.

Keep the tool only if it clearly pays for itself. If it doesn't, stop. That's a fine result too.

Step 5: Write a one-page policy before everyone uses it

Use the template in Section 8. Review it every few months, since tools and prices change.

Want a deeper framework later? The free [NIST AI Risk Management Framework](#) is a good reference, but it's heavy reading for a beginner.

3. Green / Yellow / Red data rules

Before you paste anything into an AI tool, ask: "**What color is this?**" When in doubt, treat it as Red.

Color	What it covers	Rule
GREEN	Public info, marketing copy, generic how-to questions, your published prices, your own rough notes with no customer details	OK in any AI tool your business has approved
YELLOW	Internal documents, customer names and emails, job addresses, financial summaries, supplier contracts	Only in an approved business-tier account (not a personal or free account), with training on your data turned off. Remove or replace details you don't need first
RED	Medical/health information (PHI), Social Security numbers, full card or bank numbers, passwords or access codes, legal matters, HR or disciplinary files, trade secrets	Never , unless the tool has a signed agreement that covers this data (for example, a BAA for health info) and the owner has approved that specific use in writing

Simple habits that keep you safe

- **Business accounts only.** No business data in personal or free consumer accounts. Consumer accounts don't give you admin controls, and their privacy settings differ by vendor, so check them.
- **Give it only what it needs.** "Write a reply to a customer upset about a late install" works fine without the customer's name or address.
- **Swap details for placeholders.** Replace names and numbers with [Customer A], [Job #], [Address] before pasting. Put the real details back in afterward.
- **One login per person.** No shared passwords. Turn on two-step login (2FA) or single sign-on.
- **Remove access the day someone leaves.**
- **Limit connections.** If you connect the AI to your email or files, connect only the folders it actually needs.
- **Check training settings.** Look in each tool's settings to confirm whether your chats can be used to train the vendor's models, and turn that off if you can. Defaults have changed before, so re-check from time to time.

4. Medical and other sensitive data (BAAs)

Skip this section if you never handle health information. Read it carefully if you're a clinic, dentist, therapist, chiropractor, medical billing service, or you do work for one.

What's a BAA?

Under HIPAA, if a healthcare provider, health plan, or a business that works for one (a "business associate") puts protected health information (PHI) into a vendor's service, it needs a **Business Associate Agreement (BAA)** with that vendor. See [HHS: Business Associates](#).

A BAA alone does not make you compliant. Every vendor says the customer still has to set the service up correctly and follow HIPAA's other rules. Never describe your setup as "HIPAA compliant" based on this kit. Review it with a compliance professional.

Which plans offer a BAA? (checked Oct 2026)

Vendor	No BAA (don't use for PHI)	Where a BAA is available	Source
OpenAI (ChatGPT)	Free, Plus, Pro, and ChatGPT Business	ChatGPT Enterprise with Regulated Workspace and ChatGPT for Healthcare (through sales); ChatGPT for Clinicians (has its own in-product BAA flow for individual clinicians); the API with Modified Retention. The API BAA is self-serve only if you have an established history of API usage ; otherwise email baa@openai.com	HIPAA-eligible products, API BAA, Business billing
Anthropic (Claude)	Free, Pro, Max, and Claude Team	Claude Enterprise (20-seat minimum): the Primary Owner turns on HIPAA with "Accept and enable HIPAA" (this can't be undone). HIPAA doesn't automatically cover Claude Code or Cowork. A BAA is also available for Anthropic's own API	HIPAA-ready Enterprise, BAA for commercial customers, Enterprise
Microsoft 365	Consumer (personal) Copilot	The BAA is included by default in Microsoft's Data Protection Addendum for covered entities and business associates. Microsoft Copilot and Copilot Chat are listed as in scope	Microsoft HIPAA/HITECH
Google Workspace	Personal Gmail and personal Gemini	A Workspace admin must accept the BAA in the Admin console. Gemini features such as "Help me write," smart replies, and the side panel are listed as included. Third-party add-ons are not covered	Workspace HIPAA

In short: ChatGPT Business and Claude Team do **not** offer a BAA. Microsoft 365, Google Workspace, and the enterprise/healthcare offerings from OpenAI and Anthropic do, but you still have to configure them correctly.

A practical note for very small health offices: if you already use Microsoft 365 or Google Workspace, the AI built into that account (with the BAA in place and settings checked by someone qualified) may be the simplest path to explore. Enterprise plans with seat minimums or sales-quoted pricing can be a lot for a 3-person office. *This is a general observation, not a recommendation for your office. Confirm with your compliance advisor.*

California privacy (CCPA/CPRA)

California's privacy law applies to for-profit businesses that do business in California and meet certain thresholds (based on revenue or how much personal information they buy, sell, or share).

Many very small businesses fall below them, but your customers or contracts may still require privacy protections. Check the current thresholds with the [CA Attorney General](#) and the [California Privacy Protection Agency](#). If you want to use AI for **hiring, credit, or housing decisions**, talk to a lawyer first; California has rules on automated decision-making.

5. What it really costs (prices checked Oct 2026)

US list prices, checked against the vendor pages linked below in October 2026. Prices, promos, and plan names change often; confirm on the vendor page before you buy. Taxes not included.

Free and included options

- **ChatGPT Free, Claude Free, and consumer Gemini or Copilot apps:** \$0. **Green data only.** These use consumer terms and have no admin controls.
- **Microsoft Copilot Chat:** no extra cost with eligible Microsoft 365 plans. ([Microsoft](#))
- **Gemini in Gmail:** included in Google Workspace plans, including Business Starter. ([Google](#))

Paid plans

Plan	Price (per user, per month)	Good to know	BAA?	Source
Google Workspace Business Starter (Gemini in Gmail included)	\$7 on an annual plan, or \$8.40 on the monthly Flexible plan	New-customer promo seen at check time: \$4.90 for 3 months	Yes, admin accepts in Admin console	Business editions, Flexible plan, Pricing
Google Workspace Business Standard	\$14 annual, or \$16.80 Flexible	Includes appointment booking pages. Promo seen at check time: \$9.80 for 3 months, new customers	Yes, admin accepts in Admin console	Same as above
Google Workspace Business Plus	\$22 annual, or \$26.40 Flexible		Yes, admin accepts in Admin console	Same as above
Microsoft 365 Business Standard with Copilot	\$23.50, paid yearly	Business Premium with Copilot is \$32.00, paid yearly	Yes, in the Data Protection Addendum	Microsoft
ChatGPT Business (Standard seat)	\$25 billed monthly, or \$20 billed annually	2-seat minimum. Premium seats \$125 monthly / \$100 annual	No	OpenAI
Claude Team (Standard seat)	\$25 billed monthly, or \$20 billed annually	2-member minimum. Premium seats \$125 / \$100	No	Anthropic
Claude Enterprise	\$20 per seat, billed annually, plus usage at API rates	20-seat minimum, annual commitment	Yes (HIPAA-ready option)	Anthropic
ChatGPT Enterprise / Healthcare	Quoted by sales		Yes, for HIPAA-eligible offerings	OpenAI

Example monthly budgets

Simple arithmetic from the list prices above. Your bill depends on your plan, billing choice, and taxes.

Situation	Approximate monthly cost
1 person, Green data only, free tools	\$0
3 people on Google Workspace Business Starter	\$21 (annual plan) or \$25.20 (Flexible)
3 people on Google Workspace Business Standard	\$42 (annual plan) or \$50.40 (Flexible)
3 people on Microsoft 365 Business Standard with Copilot	about \$70.50 (paid yearly)
3 people adding ChatGPT Business or Claude Team on top of existing email tools	\$60 (annual billing) to \$75 (monthly billing)
A health office that needs to use PHI	Get quotes. Compare enterprise options against the BAA path in your existing Microsoft 365 or Google Workspace account, with a compliance advisor

Tip: If you already pay for Microsoft 365 or Google Workspace, compare your current bill to the plan above before adding a separate AI subscription.

6. Checklists

6.1 Getting-started checklist

- ☐ I picked 1 to 3 routine text tasks (Section 2, Step 1).
- ☐ I checked whether Copilot Chat or Gemini is already included in what I pay for.
- ☐ I'm using a **business** account, not a personal one.
- ☐ Each person has their own login, with 2FA turned on.
- ☐ I checked the tool's settings for training on our data and turned it off if possible.
- ☐ My pilot team (1 to 2 people) knows the Green / Yellow / Red rules.
- ☐ We're using Green data only during the pilot.
- ☐ A person reviews every AI draft before it goes out.
- ☐ I set a start and end date for the pilot: _____ to _____.
- ☐ I printed the tracking worksheet (Section 9).

6.2 Vendor checklist (answer yes or no before you pay)

- ☐ Is there a business or team plan with an admin console?
- ☐ Is training on our data off by default, and is that in the terms?
- ☐ How long is data kept, and can we delete it?
- ☐ If we handle health information: will they sign a BAA, and does it cover the specific features we'll use?
- ☐ Two-step login (2FA) or single sign-on? Separate accounts per person? Activity or audit logs?
- ☐ Do they offer a security report (such as SOC 2 or ISO 27001)?
- ☐ Where is data stored, and which other companies (subprocessors) handle it?
- ☐ Monthly cost, seat minimums, and how to cancel.

6.3 Human-review checklist (before anything AI-written goes out)

- ☐ **Facts:** numbers, prices, dates, names, part numbers, and measurements are correct.
- ☐ **Tone:** it sounds like us, and it's polite.
- ☐ **Privacy:** no Red data, and no other customer's details slipped in.
- ☐ **Promises:** no guarantees, warranties, legal claims, or deadlines we didn't agree to.
- ☐ **Safety:** any technical or safety instructions were checked by someone qualified.
- ☐ Logged in our AI-use log if it was customer-facing or financial.

6.4 When someone leaves the business

- ☐ Remove their AI tool account the same day.
 - ☐ Remove their access to connected email, drives, or folders.
 - ☐ Change any shared codes they knew (and stop sharing codes).
 - ☐ Reassign any saved prompts, files, or projects they owned.
-

7. Prompt templates you can copy

How to use these: copy the template, fill in the [brackets], and paste it into your approved AI tool. Use placeholders instead of real customer details. **Always review the result** with the checklist in 6.3.

Tip for better results: tell the AI who it is, who the reader is, what you want, and how long it should be. If the first answer isn't right, just say what to change ("shorter," "friendlier," "add a line about the warranty").

7.1 Follow up on a quote

You are helping a small [type of business, e.g., HVAC company] write to customers. Write a short, friendly follow-up email to [Customer A] about the quote we sent on [date] for [job description]. Remind them the quote is valid until [date], offer to answer questions, and invite them to book by replying or calling [phone]. Keep it under 120 words. No pressure tactics.

7.2 Reply to a customer question

Write a polite reply to this customer question: "[paste question, with names removed]". Here are the facts to use: [hours / service area / pricing policy / what we do and don't do]. If the facts above don't answer the question, say we'll check and get back to them. Don't make up any details. Keep it short and friendly.

7.3 Calm reply to an unhappy customer

A customer is upset because [what happened, no names or addresses]. Draft a calm, sincere reply that acknowledges the problem, explains what we'll do next: [your plan], and gives a way to reach us: [contact]. Don't admit legal fault, promise refunds, or offer anything not listed here. Under 150 words.

7.4 Turn rough notes into a job summary

Turn these rough job notes into a clean summary for the customer: [paste notes, with names and addresses removed]. Use these headings: Work completed, Parts used, Recommendations, Next steps. Plain language, no jargon. Don't add any work or parts that aren't in my notes.

7.5 Write a step-by-step procedure (SOP)

Turn the notes below into a simple step-by-step procedure for a new employee at a [type of shop]. Number the steps, put any safety warnings in a separate "Safety" section at the top, and list tools or materials needed. Flag anything in my notes that seems unclear or missing instead of guessing. Notes: [paste notes].

Have someone qualified check every safety step before using it.

7.6 Friendly invoice reminder

Write a friendly payment reminder for invoice [Invoice #] for [amount], which was due on [date]. Offer the ways to pay: [methods]. Polite but clear. Two short paragraphs. Don't mention late fees unless I list them here: [late fee policy or "none"].

7.7 Summarize a long document

Summarize the document below in plain English for a small business owner. Give me: (1) a 3-sentence summary, (2) a list of any dates, deadlines, prices, or obligations, and (3) anything that looks unusual or that I should ask about. Quote the exact wording for anything important. Document: [paste text, after removing Red data].

For contracts and legal documents, an AI summary is a starting point only. Have a lawyer review anything you're signing.

7.8 Website or social post

Write [3] short social media posts for a [type of business] in [city/area] about [topic, e.g., getting furnaces checked before winter]. Friendly, practical, no hype, no made-up statistics. Each under [50] words, with one simple call to action: [call/book online/visit].

7.9 Service or product description

Write a clear description of our [service/product] for our website. Facts: [what it is, who it's for, what's included, price or "call for quote"]. About [100] words. Plain language. Don't add claims, guarantees, or certifications I haven't listed.

7.10 Redaction helper (use with Green-level text only)

Here's a template with placeholders. Rewrite it so it reads naturally, but keep every placeholder in square brackets exactly as written: [paste text with placeholders].

Do the actual removal of names, numbers, and addresses yourself before pasting. Don't paste Red data into a tool to have it "clean" it.

8. One-page AI policy template

Fill this in, print it, and have everyone sign it. This is a starting template, not a legal document. Have a professional review it if you handle sensitive data.

[Business name] AI Use Policy

1. **Approved tools.** We use only these AI tools for work: _____. No personal or free AI accounts for business information.
2. **Data colors.** Follow the Green / Yellow / Red rules. When in doubt, treat it as Red and ask [owner].
3. **People check AI work.** A person reviews everything AI-written before it reaches a customer, our books, a contract, or anyone outside the business.
4. **No professional advice.** We don't present AI output as legal, medical, tax, engineering, or safety advice.
5. **Report problems the same day.** If AI makes a serious mistake or someone pastes data they shouldn't have, tell [owner] the same day.
6. **Accounts.** One login per person, 2FA on, no shared passwords. Access is removed the day someone leaves.
7. **Review.** [Owner name] reviews this policy every [3] months.

Policy owner: _____ Date: _____

Employee signature: _____ Date: _____

9. Pilot tracking worksheet

Fill in one row each time you use AI for a pilot task. At the end of the pilot, compare the "before" and "with AI" columns.

Date	Tas k	Minutes before AI (typical)	Minutes with AI (incl. checking)	Needed big fixes? (Y/N)	Customer reply faster? (Y/N/NA)	Notes

End-of-pilot questions

- Total minutes saved per week (your own numbers): _____
 - Monthly tool cost: \$ _____
 - Did mistakes or rework cancel out the time saved? _____
 - Did anyone use Yellow or Red data by mistake? What will we change? _____
 - **Decision:** Keep / Change / Stop (circle one)
-

10. When to call a professional

Talk to a qualified attorney or compliance professional **before** you go further if:

- You handle **health information** (clinic, dental, therapy, medical billing, or work for them).
 - You're about to **sign a BAA or an enterprise contract**.
 - You want to use AI in **hiring, firing, credit, housing, or other big decisions** about people.
 - You may meet **California privacy law thresholds** or handle a lot of consumer personal data.
 - You've had a **data breach** or think customer data was exposed.
 - A customer contract requires specific privacy or security measures.
-

11. Sources

All vendor pages checked October 2026. Prices and terms change; confirm before buying.

- Google Workspace editions: <https://knowledge.workspace.google.com/admin/getting-started/editions/business-editions>
- Google Workspace Flexible plan: <https://knowledge.workspace.google.com/admin/billing/flexible-plan>
- Google Workspace pricing: <https://workspace.google.com/pricing>
- Google Workspace HIPAA: <https://knowledge.workspace.google.com/admin/compliance/hipaa-compliance-with-google-workspace-and-cloud-identity>
- Microsoft Copilot business pricing: <https://www.microsoft.com/en-us/copilot/pricing/business>
- Microsoft HIPAA/HITECH: <https://learn.microsoft.com/en-us/compliance/regulatory/offering-hipaa-hitech>
- OpenAI ChatGPT Business billing and seats: <https://help.openai.com/en/articles/8792536-managing-billing-and-seats-in-chatgpt-business>
- OpenAI HIPAA-eligible products: <https://help.openai.com/en/articles/20001069-hipaa-eligible-products-and-functionality>
- OpenAI API BAA: <https://help.openai.com/en/articles/8660679-getting-a-business-associate-agreement-for-the-openai-api>
- Anthropic Claude Team plan: <https://support.claude.com/en/articles/9266767-what-is-the-team-plan>
- Anthropic HIPAA-ready Enterprise: <https://support.claude.com/en/articles/13296973-hipaa-ready-enterprise-plans>
- Anthropic BAA for commercial customers: <https://support.claude.com/en/articles/8114513-business-associate-agreements-baa-for-commercial-customers>
- Anthropic Claude Enterprise: <https://claude.com/solutions/enterprise>
- HHS, Business Associates: <https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/business-associates/index.html>
- CA Attorney General, CCPA: <https://oag.ca.gov/privacy/ccpa>
- California Privacy Protection Agency: <https://cppa.ca.gov/>
- NIST AI Risk Management Framework: <https://www.nist.gov/itl/ai-risk-management-framework>

Disclaimer: This kit is educational information only. It is not legal, HIPAA, privacy, tax, or compliance advice, and using it does not make your business "compliant" with any law. Vendor terms, features, and prices change; verify with the vendor. Consult a qualified attorney or compliance professional for your situation.