Doing it safely: a short checklist

From the CA Craft Beer Summit talk, November 11. Good habits for setting AI up at a brewery, and where to read each vendor's own rules. For anything sensitive, bring in whoever handles IT for you, and read the vendor's page for the plan you're on.

How to use it: go down the list before you connect anything, and again each time you add a file or a system.

---

1. Use a business account

- [ ] **Sign up on the tool's business or team plan,** in the brewery's name. A personal account's settings belong to one person, and the rules often differ by plan.
- [ ] **Read the data settings before you connect anything:** whether your chats and files can be used to train the vendor's models, how long they're kept, and who on the account can see them. Turn off what you don't want, and write down what you chose.
- [ ] **Everyone signs in as themselves.** Then you can see who set up what, and take someone off cleanly when they leave.

2. Give it only the access it needs

- [ ] **Read-only wherever the tool offers it.** It can read the sales file without being able to change it.
- [ ] **One job at a time.** Connect the files behind the one report you picked first, and add the next system once that one has earned its spot. In the talk, step 3 started with two: the step 1 file in a shared folder, and the calendar.
- [ ] **A folder made for it.** Drop the exports it needs into one shared folder, and keep everything else somewhere it can't see.
- [ ] **The same permissions people have today.** If someone can't open a file now, their AI shouldn't be able to open it either.
- [ ] **A short list of what's connected,** who connected it, and what it's for. Take a connection off once nothing uses it.

3. A person checks what goes out

- [ ] **It drafts and recommends; a person sends.** Anything a distributor, an account, a customer or the whole team will see gets read by someone first.
- [ ] **Check it against a number you trust** before anyone reads an insight (habit 2 from the talk).

- [ ] **Make it show its sources,** and say so when one didn't come in, instead of filling the gap.
- [ ] **Start with work where a mistake is easy to spot and cheap to fix.**

4. Agree on what goes in

- [ ] **Write one short rule for the team** on what can go into AI and what stays out. A starting point: passwords, bank and card numbers, and personal details about your staff or your customers stay out of any tool the brewery hasn't approved.
- [ ] **Say who to ask** when someone isn't sure: _____

Where to read each vendor's own rules

Each of the big AI vendors has a page on how it handles data on its business plans. Read the one for the tool you use, on the plan you're on.

- **Claude (Anthropic):** Is my data used for model training? Anthropic's privacy center says that by default it doesn't use inputs or outputs from its commercial products, Claude for Work among them, to train its models.
- **ChatGPT (OpenAI):** Business data privacy, security, and compliance. OpenAI says it doesn't train its models on your organization's data by default, and lists the admin and access controls on each business plan.
- **Microsoft Copilot:** Copilot Chat privacy and protections. Microsoft says Copilot Chat's prompts and responses aren't used to train the underlying foundation models.
- **Gemini in Google Workspace:** Generative AI in Google Workspace Privacy Hub. Google says Workspace doesn't use customer data to train models without the customer's permission, and that Gemini only retrieves content the user already has access to.

Links checked October 24, 2026. Vendors update these pages, so read the current version before you connect anything.

Jeremy Carney · Central Coast Analytics · jeremy@centralcoast-analytics.com