BUILD PROJECTS · BUILDER · 20 MIN READ

Project: build an AI FAQ helper

Add an AI helper that answers only from a business's real FAQ, admits when it doesn't know, keeps the key on the server and passes a test set.

Pass the check (4 of 5) online to earn the “AI Feature Builder” badge:
https://digitalbuilders757.com/university/study/project-ai-faq-helper

What you'll build

A small chat box on a website (a gym, a salon, a club) that answers visitors' questions from the business's own FAQ and opening hours, and says 'I'm not sure, here's how to contact us' when the answer isn't there. It's the most common AI feature businesses ask for, and it teaches the habits that keep AI features honest, safe and affordable.

Step 1: Gather the knowledge and the tests

Collect the real FAQ, hours, prices and policies into one document (the knowledge base). Then write 15 test questions with the answer you expect, including three it should refuse, such as a price that isn't listed. These become your eval: the way you'll know it works before anyone else tries it.

Step 2: Build it with the key on the server

Prompt your builder: 'Add a chat box labelled AI helper. Send questions to a server route, never from the browser, using the AI provider's API with the key from an environment variable. The system prompt: answer only from this FAQ; if the answer isn't in it, say you're not sure and give the contact details; never invent prices or policies; keep answers under 80 words.' Paste the FAQ where the system prompt can use it.

Step 3: Test it, limit it, ship it

- Run your 15-question eval. Aim for at least 13 right, with every refusal correct. Fix the prompt or FAQ, not just the one answer.
- Add a rate limit (for example, a few questions per minute per visitor) and set a monthly spending limit with the AI provider.
- Label it clearly as an AI helper, add a 'talk to a person' option, and don't ask visitors for personal details in the chat.
- Deploy, ask the business owner to try to break it, and re-run the eval whenever the FAQ changes.

Key terms

Knowledge base
Documents an AI agent can look up, like your FAQ, policies or price list.

API key
A secret code that identifies your app to a service and is often tied to billing.

Eval
A set of real examples with expected answers, run to measure an AI feature's quality.

Hallucination
A confident AI answer that is false or made up.

System prompt
Hidden standing instructions that shape every answer an AI app gives.

Environment variable
A setting or secret the app reads at run time, kept outside the code.

Rate limit
The most requests or tokens a key may use in a period, such as per minute.

Server
A computer (usually in the cloud) that runs your app's back end and answers requests.

Try it: Build it for a real business

1. Pick a local business or club and gather its FAQ, hours and policies into one document.
2. Write 15 test questions with expected answers, including three it should refuse.
3. Build the helper with the Step 2 prompt and the key in an environment variable.
4. Run the eval, fix the prompt until it passes, then mark the AI FAQ helper Build Challenge as built.

KNOWLEDGE CHECK

Project: build an AI FAQ helper

5 questions. Circle one answer for each; 4 or more correct passes. Answers are at the back.

1. Where should the AI provider's API key live?

A. In the browser code, so answers come back faster
B. In the FAQ document
C. In a public GitHub repo
D. On the server, in an environment variable

2. A visitor asks for a price that isn't in the FAQ. What should the helper do?

A. Say it isn't sure and share contact details
B. Guess a fair price based on similar businesses nearby
C. Offer a small discount to keep the visitor happy and engaged
D. Ignore the question

3. What's an eval for this project?

A. A review on an app store
B. A set of test questions with expected answers you run to check the helper
C. The AI provider's invoice
D. A survey of visitors

4. Why add a rate limit and a spending limit?

A. To make answers more accurate by giving the AI more time
B. Because the law requires it for every website that uses AI
C. So no one can run up a huge bill or overload it
D. To hide the AI from search engines so competitors can't copy it

5. The FAQ changes next month. What then?

A. Nothing, the AI will notice the change and update its answers by itself
B. Delete the helper
C. Ask visitors to tell the AI the new rules
D. Update the knowledge base and re-run the eval

Official sites

OpenAI API docs: https://developers.openai.com/api/docs
Anthropic docs: Prompt engineering overview:
https://docs.claude.com/en/docs/build-with-claude/prompt-engineering/overview

Last reviewed 2026-11-25. AI tools change fast; check each tool's own site for current features, plans and prices.

ANSWER KEY

Project: build an AI FAQ helper

1. D: On the server, in an environment variable
Anything in the browser can be read by visitors. Keys stay on the server.

2. A: Say it isn't sure and share contact details
A grounded helper admits what it doesn't know instead of inventing policies.

3. B: A set of test questions with expected answers you run to check the helper
Evals show whether a prompt change made things better or worse, before users notice.

4. C: So no one can run up a huge bill or overload it
Every AI request costs money; limits protect the business from abuse and surprises.

5. D: Update the knowledge base and re-run the eval
The helper only knows what you give it. Update it, then test again.