

Lock Down Your AI Projects

Maximum-security setup for Claude Projects, ChatGPT Projects, and Gemini Gems — keep files, instructions, and chats visible only to you and out of model training.

THE HONEST BOTTOM LINE

Projects, Custom GPTs-style folders, and Gems all work the same underlying way: they add a private workspace of files and instructions on top of the same account you already have. None of the three companies documents a separate “this project is never used for training” switch — a project's privacy and training status is governed by (1) whether you keep it un-shared, and (2) the account-wide training toggle you already set using the companion guide. This document shows you exactly where those two controls live for Projects/Gems specifically, plus the sharing traps that quietly expose a “private” project to other people.

1. Claude Projects — Maximum Security Setup

If you're on a Free, Pro, or Max plan, your projects are already private by default — there is no organization to share them with, so only you can ever see one unless you're on a Team or Enterprise plan. If you are on Team or Enterprise, follow every step below.

Step 1 — Create the project

1. Go to claude.ai/projects (or hover over your account menu and select “Projects”).
2. Click “+ New Project.”
3. Give it a name and description.

Step 2 — Lock visibility to “Only invited members” (Team/Enterprise only)

On Team and Enterprise plans, a project can be set to organization-wide visibility — meaning everyone at your company could open it. For maximum security, keep it restricted to you alone.

1. Open the project and click “Share” next to the project name.
2. Under “General access,” check whether it says “Everyone at [your organization].”
3. If it does, click it and switch to “Only people invited.”
4. Look through the member list and remove anyone besides yourself by clicking their role and selecting “Remove access.”

If you're on Free, Pro, or Max, there's no “Share” step to worry about — just don't use a future Team/Enterprise upgrade to invite anyone to this project if you want it to stay solo.

Step 3 — Be careful what you put in the knowledge base

Anything you upload to a project's knowledge base (documents, text, code) becomes visible to anyone you ever grant “Can view” or “Can edit” access to. Before uploading a file, ask: would I be comfortable with every future collaborator on this project seeing this exact document?

Step 4 — Turn off model training at the account level

There is no separate “don't train on this project” switch — projects follow the same account-wide setting as your regular chats. Go to Settings → Privacy → “Help Improve our AI models” and confirm it's OFF. (Full walkthrough in the companion guide, “Lock Down Your AI Privacy.”)

Step 5 — Know the limits

- ☐ Anthropic can still review project content flagged for safety or Usage Policy violations, regardless of your settings.
- ☐ If your project is ever shared — even briefly — anyone who had “Can view” access could have already seen the knowledge base and chats.
- ☐ Removing someone's access stops future viewing; it does not undo anything they already saw or downloaded.

2. ChatGPT Projects — Maximum Security Setup

Every ChatGPT Project is private the moment you create it — only you can see its chats and files until you actively choose to share it. Your job is simply: don't share it, and confirm the account-wide training setting is off.

Step 1 — Create the project

1. In ChatGPT, click “Projects” in the sidebar.
2. Click “+ New project.”
3. Name it, and optionally add custom instructions specific to this project.
4. Upload any files you want ChatGPT to reference inside this project.

Step 2 — Leave it unshared (the default is already the most secure state)

Do not click “Share” on the project unless you specifically intend to give someone else access. If you have shared a project in the past, check who still has it:

1. Open the project and click “Share” next to its name.
2. Review the list of people, workspace groups, or shareable links currently granted access.
3. Remove anyone you no longer want to have access, and delete any active share link.

Step 3 — Turn off model training at the account level

For Free, Plus, and Pro plans, project data can be used for model training if “Improve the model for everyone” is turned on — projects don't have their own separate switch.

1. Go to Settings → Data Controls.
2. Toggle OFF “Improve the model for everyone.”

If you're on a Business, Enterprise, or Edu plan, project data is excluded from training by default and this step is typically already handled by your organization's admin settings.

Step 4 — Know the limits

- ☐ If a project is shared, training only stays off for everyone if every single contributor also has the training toggle off — one collaborator with it on can pull shared content into training.
- ☐ OpenAI can still review flagged project content to monitor for abuse or policy violations, regardless of your setting.
- ☐ Deleting a project removes it from your view; check OpenAI's data-deletion timelines in the companion privacy guide for how long backend copies persist.

3. Gemini Gems — Maximum Security Setup

Gemini doesn't call its equivalent feature “Projects” — the closest match is Gems: a custom assistant you build with your own instructions and knowledge files. Like the other two, a Gem is private to you by default until you actively share it.

Step 1 — Create the Gem

1. Go to gemini.google.com and open the sidebar.
2. Select “Gems,” then click “New Gem.”
3. Give it a name and write your custom instructions.
4. Under “Knowledge,” click “Add files” to upload any documents you want it to reference.
5. Click “Save.”

Step 2 — Leave access set to “Private”

Gemini's sharing menu offers five levels: Private (only people with access can open it), Specific people, Anyone with the link, your organization, or fully Public. For maximum security, leave it on Private and never click “Share” unless you mean to.

1. If you've shared a Gem before, open it and click “Share” to review the current access level.
2. If it shows anything other than “Private,” change the access level back to “Private” or remove individual people/links.

IMPORTANT

Google's own documentation is explicit on this point: “Any Gem instructions and files that you have uploaded to the Gem can be viewed by any user with access to the Gem.” Sharing a Gem — even just with one person as a “Viewer” — hands them your uploaded knowledge files, not just the ability to chat with it.

Step 3 — Turn off model training at the account level

Gems don't have a separate training toggle in Google's documentation — they run on the same account-wide setting as every other Gemini conversation.

1. Go to myactivity.google.com/product/gemini.
2. Turn OFF “Keep Activity.”

With Keep Activity off, conversations inside a Gem are auto-deleted after 72 hours and are not used for training unless you separately submit feedback on a response.

Step 4 — Know the limits

- ☐ Google can still have chats reviewed by human reviewers for safety and terms enforcement, regardless of your Keep Activity setting.
- ☐ If you ever shared a Gem publicly or via link, treat its knowledge files as exposed even after you switch access back to Private — anyone who already opened the link may have saved a copy.

4. Side-by-Side Comparison

	Claude Projects	ChatGPT Projects	Gemini Gems
Private by default?	Yes on Free/Pro/Max (no one to share with). On Team/Enterprise, creator chooses.	Yes — only you can see it until you actively share it	Yes — only you can open it until you actively share it
How you'd accidentally expose it	Setting visibility to “Organization-wide” or inviting members on Team/Enterprise	Sharing the project with people, a workspace group, or a link	Sharing the Gem with people, your org, a link, or making it public
Does sharing expose your uploaded files?	Yes — anyone with “Can view” access sees the project’s knowledge files	Yes — anyone with access sees project files and chats	Yes — “Any Gem instructions and files you’ve uploaded can be viewed by any user with access”
Governed by which training toggle?	Account-wide “Help Improve our AI models” setting (Settings → Privacy)	Account-wide “Improve the model for everyone” setting (Settings → Data Controls)	Account-wide “Keep Activity” setting (myactivity.google.com/product/gemini)
Is there a project-specific training switch?	Not documented — projects follow the same account-wide setting as regular chats	Not documented — projects follow the same account-wide setting as regular chats	Not documented — Gems follow the same account-wide setting as regular chats

5. Bring It Back to the 5 Golden Rules

This connects to Golden Rule 5 from the AI Safety Essentials workshop: the best defense is preventing unwanted access in the first place. A Project or Gem is only as private as the access list behind it — the single highest-risk moment for all three tools is clicking “Share” without thinking through who ends up on that list.

TRY THIS THIS WEEK

If you already have any Projects (Claude/ChatGPT) or Gems (Gemini) set up, open each one's Share/access menu today and confirm exactly who's on the list. Remove anyone who shouldn't be there — it takes about a minute per project.

Sources

Source: *How can I create and manage projects?* — Claude Support <https://support.claude.com/en/articles/9519177-how-can-i-create-and-manage-projects>

Source: *Project visibility and sharing* — Claude Support <https://support.claude.com/en/articles/9519189-project-visibility-and-sharing>

Source: *Projects in ChatGPT FAQ* — OpenAI Help Center <https://help.openai.com/en/articles/10169521-projects-in-chatgpt-faq>

Source: *Data Controls FAQ* — OpenAI Help Center <https://help.openai.com/en/articles/7730893-data-controls-faq>

Source: *Get started with Gems in Gemini Apps* — Google Help <https://support.google.com/gemini/answer/15236321>

Source: *Use Gems in Gemini Apps* — Google Help <https://support.google.com/gemini/answer/15146780>

Source: *Share a Gem from Gemini Apps* — Google Help <https://support.google.com/gemini/answer/16504957>

Source: *Manage & delete your Gemini Apps activity* — Google Help <https://support.google.com/gemini/answer/13594961>

Note: Company settings, menu labels, and plan features change over time. If a step above doesn't match what you see, search the platform's own help center for “projects,” “gems,” or “sharing” to find the current version.