

Assignment 1 — AI Foundations

Goal: Get ready for the quarter!

Due: Forms by Friday 11:59 PM week 1, remaining parts during tutorial in Week 2

Hi everyone! And welcome to CS 193T. We are so excited to have you join us in this exploration of AI and the process of establishing your own personal boundaries around the roles you assign to AI in your work.

Tutorial:

- **We won't have a formal tutorial this week.** Instead, you're welcome to drop in either **Thursday from 3-4:20** or **Friday from 9-1** (both in CODA B80) for help setting up the AI software tools you'll need this quarter on your laptops. We'll have a bunch of TAs floating around and helping you, so please stop by if you'd like help/are having any trouble!
- If you are not able to make it to the drop-in session, you will be fine using just the web-based [Stanford AI Playground](#) for the first two weeks. *But for the sake of your future busy Week 3 self, we do highly recommend you get the tools installation taken care of this week.*

Assignment outline:

- **First, complete two forms:** a [welcome survey](#), and a [survey of tutorial time preferences](#).

Throughout the quarter, your homework for the week will be split into two parts:

- **AI tool work:** a demonstration of your work with an AI tool.
- **Reflection:** a reflection about your experience using AI tools that week, or issues around AI use.

You'll use both of these deliverables as the starting point for the conversation you'll have with your TA next tutorial.

Part 1: Complete required forms

Tutorial preferences: <https://forms.gle/pvWGiNhZQJ7LLdiD8>

Welcome survey: <https://forms.gle/TXmdJ4JfQXe2tXeG6>

Part 2: AI Tool Work

Go to the [Stanford AI Playground](#), choose your favorite chatbot (ChatGPT, Claude, etc), and start a brand new chat. Write an opening prompt telling to thread the needle of helping you with your homework—but not too much!—and also never hallucinating wrong information about the homework topic. Do your best to make it a prompt you think it will adhere to (i.e., make it emphatic, specific, authoritative, etc, as you see fit to achieve the goal of making it stick).

After that opening prompt, continue the conversation and try to stress-test the system's adherence to your instructions. Ask yourself:

- How does it do?
- After asking it not to help too much, does it resist your pleas for excessive help or give in when you push?
- Is everything it says factual?
- What strategies did you use for both your original prompt and your attempts to push it to give in?
- As an extra exercise, re-run the experiment using different strength models from the same vendor (e.g., Haiku vs Sonnet vs Opus) and/or other vendors' models. Compare how each performs relative to the others.

Turn-in procedure:

- Save your full chat transcript(s) to PDF (or screenshot) and upload to [Gradescope](#). Regardless of whether you're in the AI playground or the ChatGPT/Claude/Gemini/etc UI, you can either copy and paste your responses or save it as a PDF (command + p on a mac). You may also share especially interesting snippets with your classmates on [Ed](#), if you want!

Part 3: Reflection

Answer AT LEAST ONE of the questions below and get ready to talk about it in tutorial as an icebreaker!

1. Write down what you think the AI portion of the Honor Code policy for this course should be. A few situations to consider (no need to answer them all):
 - a. What if I ask you to journal your experiences using AI to study a topic, reflecting on whether that use impacted your learning positively or negatively, and turn in your journal entry?
 - b. AI scans your journal entry for typos?
 - c. AI writes the entry from an outline of your ideas?
 - d. AI writes it entirely?
 - e. Should the answers change for ESL students, or students with writing disabilities (e.g., dyslexia)?
 - f. What is a reasonable way to detect violations of the policy? What is a reasonable consequence? Should there be warning(s) before consequences?
2. What is one skill you currently have, which you plan to use AI to increase productivity in, and that you want to keep sharp?
 - a. What mechanisms could you put in place to monitor, like a smoke detector, when that skill may be slowly, subtly dulling?

Be ready to discuss with your TA: N/A for this week.

Technology Setup:

This part of the assignment involves requesting access to premium Gemini/Claude/ChatGPT versions (free to Stanford students, staff, and faculty via Stanford enterprise subscriptions), as well as setting up your coding agent of choice.

Claude for Education

There is a higher tier available for a fee, but you will not need that version in this class.

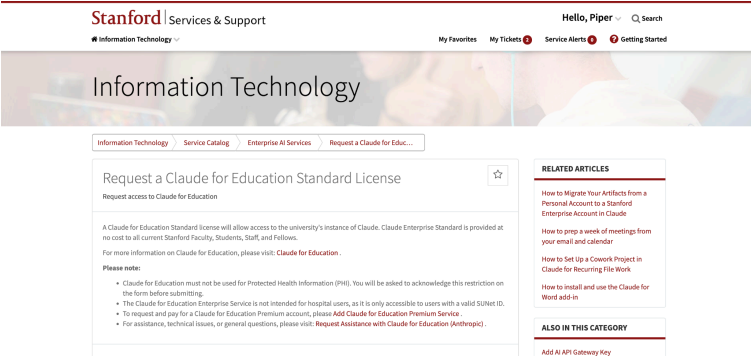
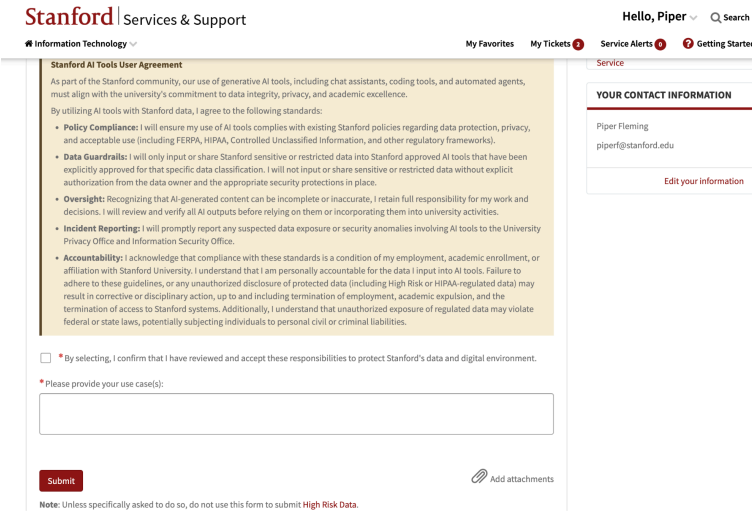
If you are a student:

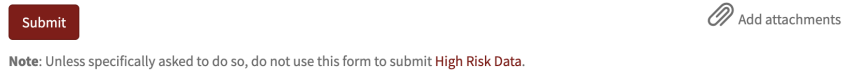
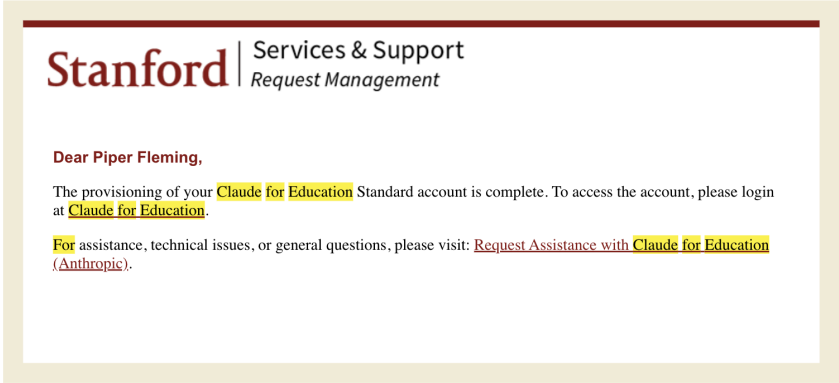
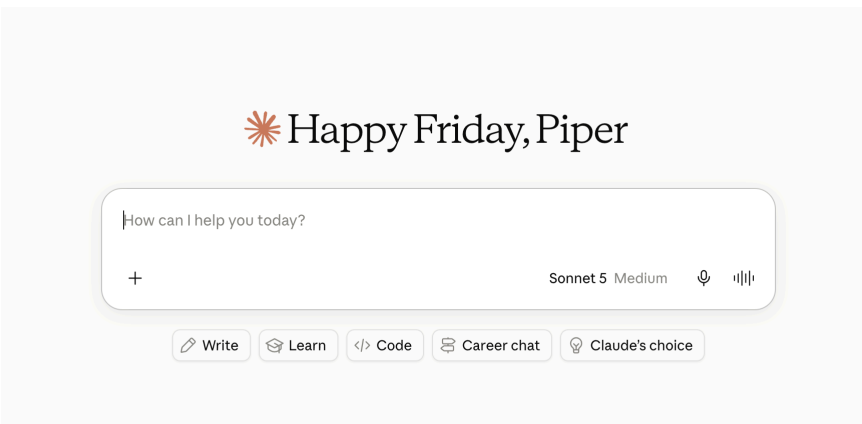
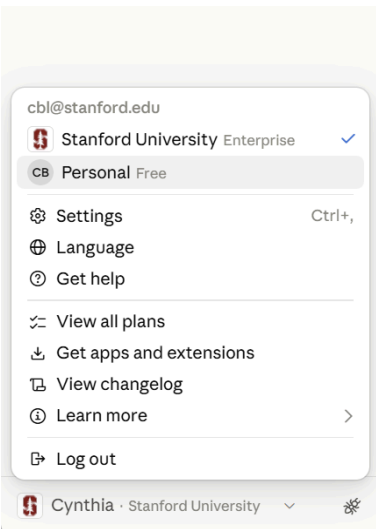
1. Click on this link.	https://stanford.service-now.com/it_services/en/request-a-claude-for-education-standard-license?id=sc_cat_item&sys_id=d0605d9c2b558b10ee36fd3fc891bfe2
------------------------	---

If you are a visiting scholar, affiliate, fellow, or other:

1. Click on this link	https://stanford.service-now.com/it_services/en/add-claude-for-education-standard-monthly?id=sc_cat_item&sys_id=e1d03e6787068310c5ea52073cbb35c5
-----------------------	---

For everyone:

2. After you sign in, the page should look like this.	 The screenshot shows the 'Request a Claude for Education Standard License' page on the Stanford Services & Support portal. The page includes a header with the user's name 'Hello, Piper' and a search bar. Below the header, there's a navigation bar with 'Information Technology' and other links. The main content area has a title 'Request a Claude for Education Standard License' and a sub-header 'Request access to Claude for Education'. It contains a paragraph explaining the license and a 'Please note' section with bullet points. On the right, there's a 'RELATED ARTICLES' section with links to 'How to Migrate Your Artifacts from a Personal Account to a Stanford Enterprise Account to Claude', 'How to prep a week of meetings from your email and calendar', 'How to Set Up a Cowork Project in Claude for Recurring File Work', and 'How to install and use the Claude for Word add-in'. At the bottom, there's an 'ALSO IN THIS CATEGORY' section with a link to 'Add AI API Gateway Key'.
3. Acknowledge the requirements and then write “For CS193T” or something similar in the “reason for requesting.”	 The screenshot shows the 'Stanford AI Tools User Agreement' page. It starts with a heading 'Stanford AI Tools User Agreement' and a paragraph explaining the university's commitment to data integrity, privacy, and academic excellence. Below this, there's a section 'By utilizing AI tools with Stanford data, I agree to the following standards:' followed by four bullet points: 'Policy Compliance', 'Data Guardrails', 'Oversight', and 'Incident Reporting'. The 'Policy Compliance' bullet point states that the user will ensure their use of AI tools complies with existing Stanford policies regarding data protection, privacy, and acceptable use. The 'Data Guardrails' bullet point states that the user will only input or share Stanford sensitive or restricted data into Stanford approved AI tools that have been explicitly approved for that specific data classification. The 'Oversight' bullet point states that the user will review and verify all AI outputs before relying on them or incorporating them into university activities. The 'Incident Reporting' bullet point states that the user will promptly report any suspected data exposure or security anomalies involving AI tools to the University Privacy Office and Information Security Office. Below the bullet points, there's a section 'Accountability' stating that the user acknowledges that compliance with these standards is a condition of their employment, academic enrollment, or affiliation with Stanford University. At the bottom, there's a checkbox for 'By selecting, I confirm that I have reviewed and accept these responsibilities to protect Stanford's data and digital environment.' and a text area for 'Please provide your use case(s):'. There's a 'Submit' button and a link to 'Add attachments'.

4. Click the submit button!	 Note: Unless specifically asked to do so, do not use this form to submit High Risk Data.
5. You will then get an email (probably in a few days) that looks like this. Click on the “Claude for Education” link.	
6. Follow the prompts to get your Claude account set up on the web version. Once it looks like this, you’re done.	
7. <i>If you already had a Claude personal account, you should be able to switch between your Stanford and personal versions by clicking in the lower left corner.</i>	

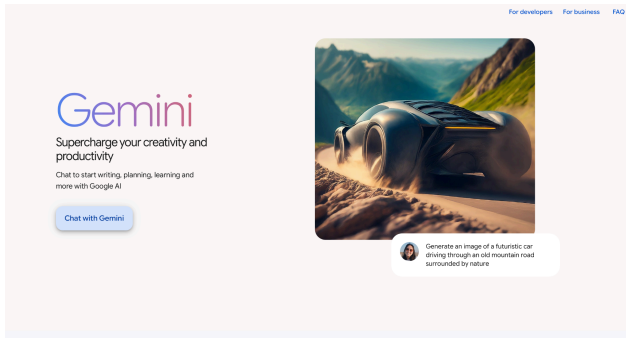
Google Gemini

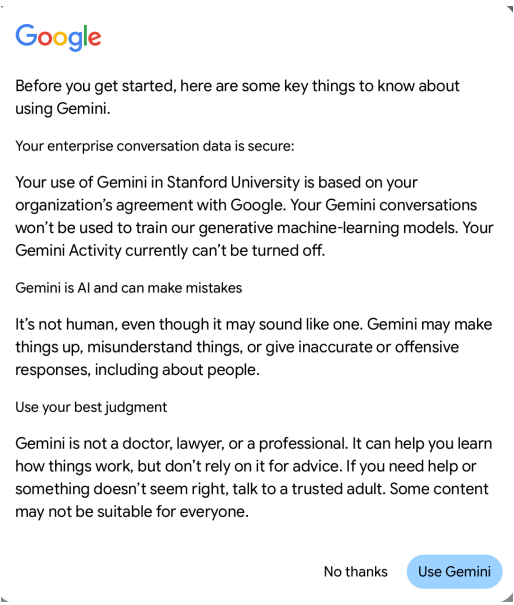
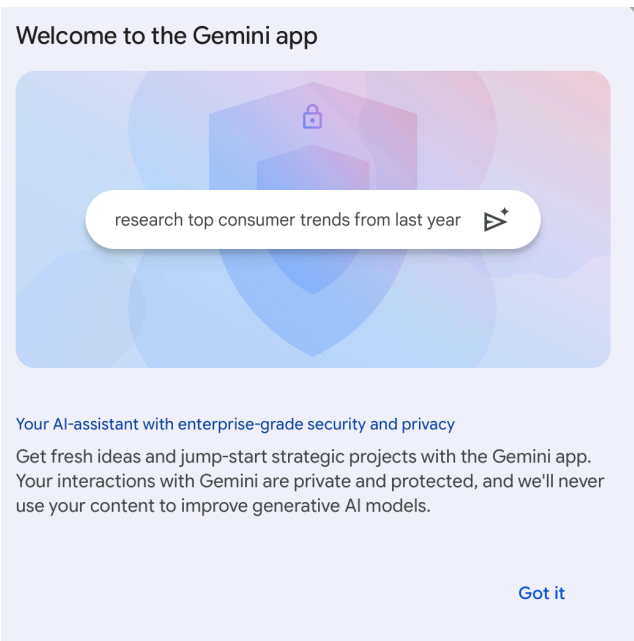
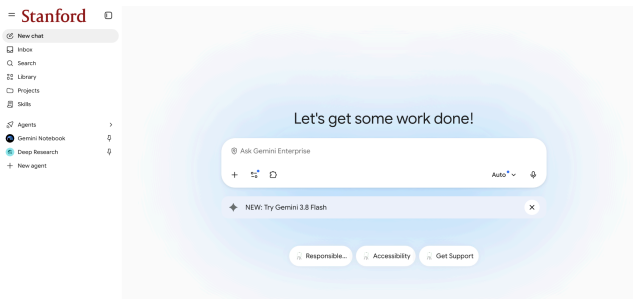
If you are a student, jump to the installation instructions below.

If you are a visiting scholar, affiliate, fellow, or other, you will need to go through a request process at the following link:

1. Click on this link.	https://stanford.service-now.com/it_services/en/add-gemini-standard-monthly?id=sc_cat_item&sys_id=d6d3e7b487d64f10c5ea52073cbb35c9
2. Follow the same process outlined for Claude and Chat to request access. Then, follow the steps below.	

For everyone:

1. Click on this link.	https://aiworkspace.stanford.edu/
2. You will be directed to this page. Click “chat with Gemini”.	

3. You will then be asked to review some permissions, agree to them	 The image shows the Google Gemini onboarding screen. At the top is the Google logo. Below it, text reads: "Before you get started, here are some key things to know about using Gemini." This is followed by a section titled "Your enterprise conversation data is secure:" which states that Gemini use in Stanford University is based on an agreement with Google and that conversations won't be used to train models. Another section says "Gemini is AI and can make mistakes" and "It's not human, even though it may sound like one." A final section titled "Use your best judgment" states that Gemini is not a professional and users should talk to a trusted adult if needed. At the bottom right are two buttons: "No thanks" and "Use Gemini".
4. You will then see this screen, say “got it”	 The image shows the "Welcome to the Gemini app" screen. It features a large blue and purple abstract background with a central white pill-shaped button containing the text "research top consumer trends from last year" and a search icon. Below this, text reads: "Your AI-assistant with enterprise-grade security and privacy" and "Get fresh ideas and jump-start strategic projects with the Gemini app. Your interactions with Gemini are private and protected, and we'll never use your content to improve generative AI models." A "Got it" button is in the bottom right corner.
5. If you see this screen, you're done!	 The image shows the Stanford Gemini interface. On the left is a sidebar menu with items: "New chat", "Inbox", "Search", "Library", "Projects", "Skills", "Agents", "Gemini Notebook", "Deep Research", and "New agent". The main area has a header "Stanford" and a "Let's get some work done!" prompt. Below this is a search bar with "Ask Gemini Enterprise" and a "NEW: Try Gemini 3.5 Flash" notification. At the bottom are links for "Responsible", "Accessibility", and "Get Support".

OpenAI ChatGPT Edu

There is a higher tier available for a fee, but you will not need that version in this class.

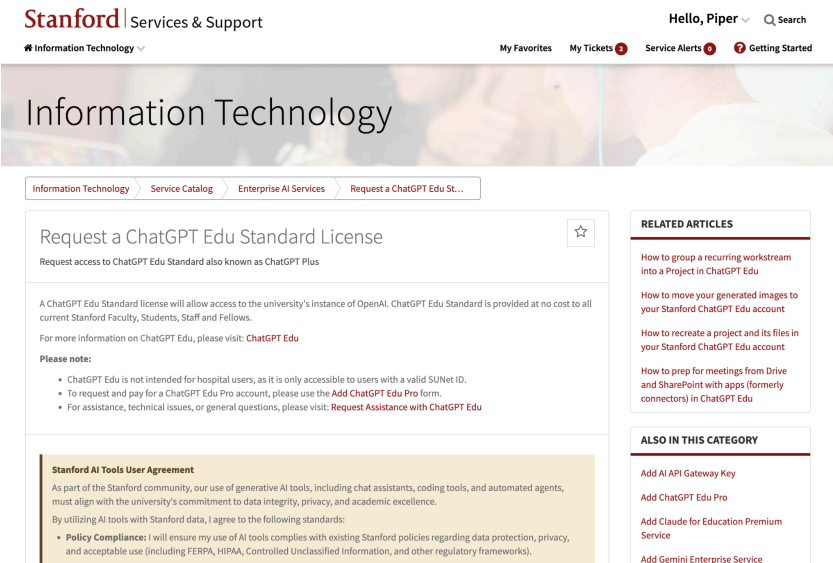
If you are a student:

1. Click on this link.	https://stanford.service-now.com/it_services/en/request-a-chatgpt-edu-standard-license?id=sc_cat_item&sys_id=0c3324ad2be5cf90ee36fd3fc891bf6f
------------------------	---

If you are a visiting scholar, affiliate, fellow, or other:

1. Click on this link	https://stanford.service-now.com/it_services/en/add-chatgpt-edu-standard-monthly?id=sc_cat_item&sys_id=d52e16ab87028310c5ea52073cbb35d4
-----------------------	---

For everyone:

2. After you sign in, the page should look like this.	 The screenshot shows the Stanford Services & Support portal. At the top, it says 'Stanford Services & Support' with a search bar and user profile 'Hello, Piper'. Below the header is a navigation bar with 'Information Technology' selected. The main content area is titled 'Information Technology' and contains a breadcrumb trail: 'Information Technology > Service Catalog > Enterprise AI Services > Request a ChatGPT Edu St...'. The primary card is 'Request a ChatGPT Edu Standard License', which includes a star icon, a description of the license, and a 'Please note' section with bullet points about user eligibility and request procedures. To the right, there are two sidebars: 'RELATED ARTICLES' with links to project setup and image management guides, and 'ALSO IN THIS CATEGORY' with links to API Gateway, ChatGPT Pro, Claude for Education, and Gemini Enterprise services.
---	---

3. Acknowledge the requirements and then write “For CS193T” or something similar in the “reason for requesting.”	
4. Click the submit button!	
5. You will then get an email (probably in a few days) that looks like this. Click on the “ChatGPT Edu” link.	
6. Follow the prompts to get your Chat account set up on the web version. Once it looks like this, (specifically, the little Stanford S in the bottom left corner) you’re done.	

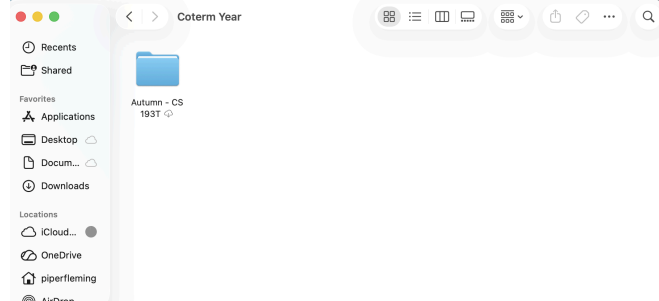
Coding Agents

Later on in this class, we'll be working with coding agents, and we will be supporting students doing agentic workflows. So you won't need these tools for several weeks, but if you would like to get a head start, here are some instructions for installation.

When we use them, we will be allowing students to choose which vendor they want to use (including Anthropic's Claude Code, OpenAI's Codex, and Gemini workflows).

You are welcome to choose whichever one you want, or all three! For Claude and Codex, you will need to have your coding agent of choice set up on your computer, **within the terminal**. If you are not familiar with working in the terminal, you may be more comfortable with Gemini workflows, which do not require terminal use. We've included instructions below, but if you run into bugs, you're welcome to paste your errors into your favorite LLM and try getting help that way! You're also welcome to come to the drop-in help hours (see top of assignment for times/location).

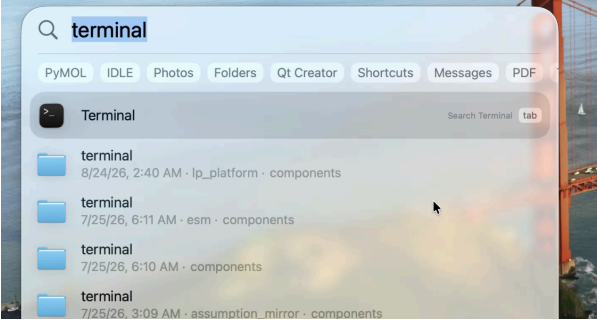
For everyone:

1. Make a new folder titled "CS193T" (the exact name doesn't matter) wherever you keep downloaded class materials on your laptop.	
---	---

Claude Code

For Mac users:

1. Open your terminal (go up to the little magnifying glass icon in the right corner of your screen and click that, then type "terminal").	
--	--

	
2. Paste this line into your terminal, and then press enter (make sure there are no leading spaces): This all needs to be one line, exactly as typed here! See my screenshot.	<pre>piperfleming@Pipers-MacBook-Pro-3 ~ % curl -fsSL https://claude.ai/install.sh bash</pre> <code>curl -fsSL https://claude.ai/install.sh bash</code>
Debugging tips: if you see “command not found” when you type in “claude”, try closing the terminal, and reinstalling. If the terminal says “run this line”, run it.	
3. Wait for this line to pop up again:	<pre>(base) piperfleming@Pipers-MacBook-Pro-3 ~ %</pre>

For Windows users (I have a mac so cannot provide screenshots of this but if anyone with a windows laptop would like to take screenshots and send to me I would appreciate it!):

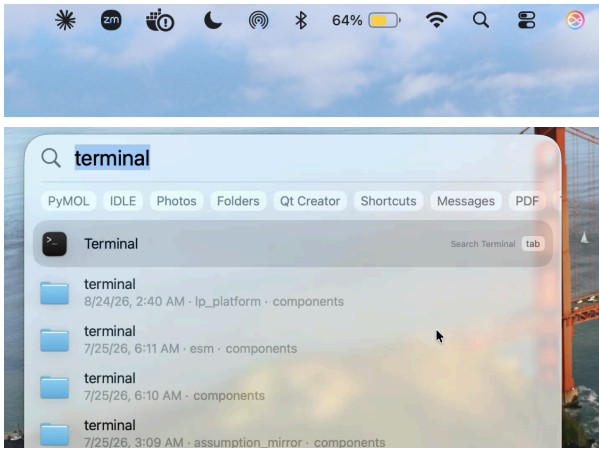
1. Open your application menu and search “terminal”	
2. Paste this line into your terminal:	<pre>irm https://claude.ai/install.ps1 iex</pre>
3. Wait for this line to pop up again:	<pre>(base) piperfleming@Pipers-MacBook-Pro-3 ~ %</pre>

For everyone:

1. Type “claude”, and press enter. If a new window pops up, follow the prompts. It should look like this when you’re done.	 Claude Code v2.1.252 Opus 5 with medium effort · Claude Team /Users/piperfleming ⚠ 1 MCP server needs authentication · run /mcp Using Opus 5 (from .claude/settings.json) · /model
--	--

Codex

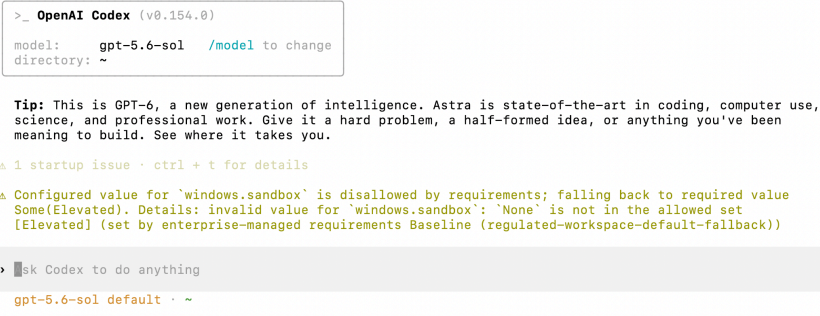
For Mac users:

1. Open your terminal (go up to the little magnifying glass icon in the right corner of your screen and click that, then type “terminal”).	
2. Paste this line into your terminal: This all needs to be one line, exactly as typed here! Debugging tips: if you see “command not found” when you type in “codex”, try closing the terminal, and reinstalling. If the terminal says “run this line”, run it.	<pre>(base) piperfleming@Pipers-MacBook-Pro-3 ~ % curl -fsSL https://chatgpt.com/codex/install.sh sh</pre> curl -fsSL https://chatgpt.com/codex/install.sh sh
3. Wait for this line to pop up again:	<pre>(base) piperfleming@Pipers-MacBook-Pro-3 ~ %</pre>

For Windows users (note I have a mac so cannot provide screenshots of this but if anyone with a windows laptop would like to take screenshots and send to me I would appreciate it!):

1. Open your application menu and search “terminal”	
2. Paste this line into your terminal: This needs to be one line, not two!	<code>powershell -ExecutionPolicy ByPass -c "irm https://chatgpt.com/codex/install.ps1 iex"</code>
3. Wait for this line to pop up again:	<code>(base) piperfleming@Pipers-MacBook-Pro-3 ~ %</code>

For everyone:

4. Type “codex”, and press enter. If a new window pops up, follow the prompts. It should look like this when you’re done.	 <pre> >_ OpenAI Codex (v0.154.0) model: gpt-5.6-sol /model to change directory: ~ Tip: This is GPT-6, a new generation of intelligence. Astra is state-of-the-art in coding, computer use, science, and professional work. Give it a hard problem, a half-formed idea, or anything you've been meaning to build. See where it takes you. ^ 1 startup issue · ctrl + t for details ^ Configured value for 'windows.sandbox' is disallowed by requirements; falling back to required value Some(Elevated). Details: invalid value for 'windows.sandbox': 'None' is not in the allowed set [Elevated] (set by enterprise-managed requirements Baseline (regulated-workspace-default-fallback)) > sk Codex to do anything gpt-5.6-sol default · ~ </pre>
---	--

Once you’ve seen either of those screens, a good starting prompt might be “Tell me what I can do with you as a tool!”. This will allow you to both get a feel for the UI but start getting a hang of using the tool itself.

OTHER RESOURCES

- If you’ve never used a terminal before:
 - a. Claude Code: <https://code.claude.com/docs/en/terminal-guide>
- Setup guide:
 - a. Claude Code: <https://code.claude.com/docs/en/quickstart>
 - b. Codex: <https://learn.chatgpt.com/docs/codex/cli#getting-started>