How to Use ChatGPT as Your Teacher

Analysis by Dr. Joseph Mercola | January 11, 2024

STORY AT-A-GLANCE

> As large language models (LLMs) like ChatGPT are taking the world by storm, it's important to understand their strengths and drawbacks

> ChatGPT answers can be significantly improved by entering custom instructions and learning to create better prompts to discourage fabrications and hallucinations

> According to one large-scale study, ChatGPT "shows a significant and systemic left-wing bias ... favoring the Labour Party and President Joe Biden's Democrats"

> Never share confidential information with ChatGPT or any other LLM. Never use it to organize or analyze such information, and never type in your name, address, email, phone number or any other personal identifiers in the chat box

> All conversations with ChatGPT are stored on open servers, shared with other LLMs, and used as an AI training tool, which means your information can end up being included in responses to other people's questions

It's been just a short 14 months since ChatGPT and the other large language models (LLMs) which are the progenitors of artificial general intelligence (AGI) have been available to us. I suspect many of you have explored their use. It's a fascinating technology that has enormous potential to serve as patient teachers to help you understand a wide range of concepts that you might find confusing.

One of the challenges of writing this newsletter is that it is virtually impossible to simplify certain medical concepts because there's such a wide range of medical

knowledge among the readers.

I regularly use ChatGPT to answer certain biological questions or concepts that I am unclear about. For example, I recently did a deep dive on the mechanisms of how carbon dioxide (CO_2) might work as one of the most effective and simple interventions to improve health and prevent disease.

I was really impressed with how quickly it would explain complex physiology that could help me understand the topic better. It occurred to me that my readers could use this tool to help them understand areas of medical science that they don't yet fully understand.

A classic example of this would be mitochondrial cellular energy production and the electron transport chain function. It is clearly a very complex topic but you can continuously ask ChatGPT as many questions as you want, and repeat your questions until you understand it.

This is a great example to use because it is a topic that many don't fully understand, yet it's not controversial — it doesn't violate any medical narrative that is radically influenced by the pharmaceutical paradigm. As long as you restrict your use of this tool to basic science topics you should be OK, and I would encourage you to do this on a regular basis. You can use the video above to help you refine your search strategies.

You just want to be very, very careful and avoid ever asking any questions that relate to treatment options, because you can be virtually certain it will be biased toward the conventional narrative and give you incorrect information. It will even warn you that something you know to be both effective and harmless is dangerous.

For example, the last thing you would want to ask the program is how to treat heart disease, diabetes or obesity. It will merely regurgitate what the drug companies want you to hear and give you serious warnings about the dangers of any strategy that conflicts with these recommendations.

Consider Using ChatGPT to Help You Update Your Health Knowledge

The integration of AI tools like ChatGPT in learning basic foundational health concepts represents a significant shift in education. Traditionally, learning about health and medicine has been confined to structured environments like classrooms or textbooks.

However, many find themselves lacking essential health knowledge that they were not taught in school, which limits their ability to successfully navigate the enormous amount of information that is currently available to them. This is where ChatGPT can step in to fill the gap.

ChatGPT, with its vast database and learning capabilities, offers an interactive and personalized learning experience. One of its most valuable attributes is its nearly infinite patience.

Unlike human teachers who might be constrained by time, energy, or resources, ChatGPT is available 24/7, ready to answer questions, clarify doubts and provide explanations about foundational health basics as many times as needed. This feature is especially crucial when seeking to understand complex concepts and terminology that is vital to make an important decision about your own health.

Moreover, the ability of ChatGPT to answer continuous questions and refine the understanding of answers is a game-changer. In traditional learning settings, students might hesitate to ask questions for fear of being judged or disrupting the flow of the class. ChatGPT eliminates this barrier. Learners can ask follow-up questions until they grasp the concept thoroughly, ensuring a deeper and more personalized learning experience.

Another significant advantage of ChatGPT is its up-to-date knowledge base. The field of health and medicine is constantly evolving, with new discoveries and updates. ChatGPT, being an AI model that continuously learns, can provide the most current information, which is crucial for understanding contemporary health issues.

Understand the Limits of Using ChatGPT

However, it's essential to recognize the limitations of AI in health education. While ChatGPT can offer general information and guidance, it cannot replace professional medical advice. It's always recommended to consult healthcare professionals for personal health concerns.

That said, this is also a challenge, because many healthcare professionals know less about health than you do, so you need to identify a competent clinician. Once you understand your specific situation better with the help of ChatGPT, it will be far easier to work with your clinician.

Just keep in mind that while ChatGPT and similar AI tools can be invaluable teaching tools, there are significant dangers and concerns associated with their use, particularly in the realm of health. These concerns primarily revolve around potential biases programmed into the system, privacy issues, and the risk of hallucinations or misinformation, which I'll review below.

Bias and Conflict of Interest Creates a Dual Edged Sword

One of the critical issues is the potential for built-in biases, which may reflect the perspectives or interests of their developers and funding sources. This is particularly concerning in the context of health information, where it is highly likely that there will be a serious conflict of interest, especially regarding natural health approaches versus the pharmaceutical paradigm.

One needs to understand that there is a serious conflict of interest in ChatGPT's programming, as it is heavily influenced by pharmaceutical interests. This leads to bias when addressing health conditions that skew their responses towards pharmaceutical and surgical solutions, overshadowing natural health alternatives that address the fundamental cause of the problem.

This bias impacts the range and objectivity of health information provided and radically limits your access to a diverse spectrum of health care perspectives. It's crucial for you to know this before you engage with these powerful tools.

The bias toward conventional narratives emerge primarily as a result of the information the LLM was trained on. In this case, it was trained on data available online AFTER Big Tech began its purge of alternative voices, hence it's extremely one-sided.

Indeed, according to one large-scale study, ChatGPT "shows a significant and systemic left-wing bias ... favoring the Labor Party and President Joe Biden's Democrats."[1] That's because opposing views have been censored, so ChatGPT doesn't have that knowledge to draw from.

When only one side of a given story is allowed to exist, and that's the view ChatGPT predominantly ingests, bias is inevitable. The prompts used in inquiries can also inject bias into its responses.

AI Can Be Harnessed for Good, but Great Care Is Required

To be clear, a bias isn't necessarily harmful per se. It all depends on what the bias is promoting. We in the natural health field, for example, are biased toward things like whole foods and toxin-free products and against things like pharmaceutical drugs for lifestyle-induced ailments.

Mike Adams, founder of Natural News and Brighteon, is currently working on a free, open source LLM that is being trained on holistic and natural health material, permaculture and nutrition,[2] so this LLM will undoubtedly be biased as well, just in the opposite direction of most others.

Adams expects to release the first version of it around March 2024, with regular updates thereafter. Contrary to ChatGPT, you'll be able to download this program and use it offline in complete privacy. This effort is just one example of how we can harness the power of AI to help humanity achieve better health.

How to Navigate the Challenges

To navigate these challenges, you should approach AI-provided health information with a critical and informed perspective. Firstly, it's essential to recognize these tools should not replace professional medical advice.

They are best used as a supplementary source of information. It is important to always cross-reference information they provide with reliable sources and, if in doubt, consult a trusted healthcare professional.

A cautious, well-informed approach, coupled with cross-verification from reliable sources and consultation with healthcare professionals, can enable users to benefit from AI in health education will minimize the potential risks. With that said, let's take a look at how you can get the most out of ChatGPT, flaws and all.

How to Optimize Your Use of ChatGPT

In her video, YouTuber Leila Gharani reviews how to unlock the full potential of ChatGPT. To start, she suggests entering custom instructions, things like your location, job title, hobbies, topics of interest and personal goals. "This way, you won't have to repeat your preferences in every single conversation ... and you'll get answers that are more relevant ..." Gharani says.

However, don't include any confidential information or anything that might compromise your privacy. For example, don't include your actual address, just the general location.

Another custom instruction relates to how you want ChatGPT to respond. Here, you can instruct it to respond in a casual or formal tone, for example. You can also specify the approximate length of responses, how you want to be addressed, and whether ChatGPT should provide opinions on topics or remain neutral.

A sample instruction offered by Gharani is "When I ask for Excel formulas, just provide the most efficient formula without any explanation." She also suggests instructing

ChatGPT to always include the confidence level of its answers, and, to inform you any time its answer contains speculation or prediction.

You can also add instructions to always providing a source with a valid URL for facts given. Now, recall, I mentioned that ChatGPT can hallucinate. Always double-check the sources provided.

As you can see in the video below, a poorly worded prompt can easily trigger ChatGPT to veer straight into fantasyland, and if instructed to provide URLs, it will simply fabricate those too. Ultimately, to make ChatGPT useful, you must master the art of asking good questions and creating clear prompts.

How to Create Better Prompts

Next, Gharani reviews how to create better prompts. First, you can teach ChatGPT to imitate your style of writing by giving it some examples. Here's a sample instruction created by Gharani:

> *"I'd like you to help me write articles for my productivity blog. First I want you to understand my writing style based on examples that I give you. You'll save my writing style under LG_STYLE. After that, you'll ask me what the topic of my specific content is. You'll then write the article using LG_STYLE."*

Next, copy and paste in a couple of writing samples. Now, you're ready to give it a topic to write about. You can also instruct ChatGPT to review, critique and provide feedback on its answers. "This sounds funny, but it really works well," Gharani says. In the video, you can see how this process works. Other ways to improve ChatGPTs output include:

- **"Self-prompting"** — Instruct ChatGPT to ask you questions until it is sure it can create an optimal answer.
- **Set word limits** — To avoid unnecessary rambling, instruct it to limit its answer to a specific word count. (If you want this for all answers, you'd add it under custom instructions, as mentioned earlier). You can also ask it to reduce the word count of

an answer already given. A sample prompt for this could be, "Now say the same thing more concise and briefer using only 60% as many words."

- **Specify output format** — ChatGPT can provide answers in a variety of formats, not just plain. Examples include table format, HTML, comma-separated values (CSV), JSON, XML and Pandas data frame.

Protect Your Privacy

One key thing to remember whenever you interact with ChatGPT is that it stores every conversation you have with it on OpenAI's servers, and if you share confidential information, that gets stored too. These logs are shared with other AI companies and AI trainers.

As reported by Make Use Of,[3] Samsung employees inadvertently leaked confidential company data via ChatGPT, showing just how great a security risk it can be.

> *"... given that huge companies are using ChatGPT to process information every day, this could be the start of a data leak disaster,"* Make Use Of writes.

> *"Samsung's employees mistakenly leaked confidential information via ChatGPT on three separate occasions in the span of 20 days. This is just one example of how easy it is for companies to compromise private information ... Some countries have even banned ChatGPT[4] to protect their citizens until it improves its privacy ...*

> *Luckily, it seems that Samsung's customers are safe — for now, at least. The breached data pertains only to internal business practices, some proprietary code they were troubleshooting, and the minutes from a team meeting ...*

> *However, it would have been just as easy for the staff to leak consumers' personal information ... If this happens, we could expect to see a massive increase in phishing scams and identity theft.*

There's another layer of risk here, too. If employees use ChatGPT to look for bugs like they did with the Samsung leak, the code they type into the chat box will also be stored on OpenAI's servers.

This could lead to breaches that have a massive impact on companies troubleshooting unreleased products and programs. We may even end up seeing information like unreleased business plans, future releases, and prototypes leaked, resulting in huge revenue losses."

Never Enter Sensitive Information Into Your Prompts

The take-home here is, never share confidential information with ChatGPT or any other LLM. Never use it to organize or analyze such information, and never type in your name, address, email, phone number or any other personal identifiers in the chat box.

Remember, EVERYTHING you type into the chat box is stored on open servers, shared with other LLMs, and used as an AI training tool, which means your information can end up being included in responses to other people's questions.

So, lawyers, never use ChatGPT to review legal agreements unless completely anonymized; coders, never ask it to check proprietary code; company workers of all stripes, never enter sensitive customer data for analysis or organization, and so on. Think things through. If you wouldn't plaster the information on a public message board in the center of every town square in every country on earth, don't enter it into ChatGPT.

ChatGPT Data Collection Issues

As reported[5] by Uri Gal, a professor of business information systems at the University of Sydney, Australia, the LLM that underpins ChatGPT was trained on 300 billion words scraped from books, articles, websites and social media posts. Personal information was also swept up. Gal sees several problems with this data collection.

"First, none of us were asked whether OpenAI could use our data. This is a clear violation of privacy, especially when data are sensitive and can be used to identify us, our family members, or our location," Gal writes.

"Even when data are publicly available their use can breach what we call contextual integrity. This is a fundamental principle in legal discussions of privacy. It requires that individuals' information is not revealed outside of the context in which it was originally produced.

Also, OpenAI offers no procedures for individuals to check whether the company stores their personal information, or to request it be deleted. This is a guaranteed right in accordance with the European General Data Protection Regulation (GDPR) ...

This 'right to be forgotten' is particularly important in cases where the information is inaccurate or misleading, which seems to be a regular occurrence with ChatGPT.[6]

Moreover, the scraped data ChatGPT was trained on can be proprietary or copyrighted. For instance, when I prompted it, the tool produced the first few passages from Joseph Heller's book Catch-22 — a copyrighted text ...

Finally, OpenAI did not pay for the data it scraped from the internet. The individuals, website owners and companies that produced it were not compensated.

This is particularly noteworthy considering OpenAI was recently valued at US$29 billion, more than double its value in 2021 ... None of this would have been possible without data — our data — collected and used without our permission."

Also be aware that ChatGPT gathers things like your IP address, browser type and browser settings, your interactions with the site and your online browsing history, and that OpenAI may share all of this information with unspecified third parties.[7] You

consent to all that data gathering and sharing when you accept OpenAI's privacy policy,[8] which no one ever really reads.

Concluding Thoughts and Recommendations

Protecting your privacy is becoming all the more important in light of AI's growing role in warfare.[9] Since AI consumes data, data becomes a primary weapon, and "not having anything to hide" is no longer a valid reason to cast privacy aside. Any piece of information can be used against you personally, and in aggregate, even the most harmless data points can be weaponized.

Perhaps most importantly, AI is being taught to look for patterns and is no doubt employed in social engineering projects already. What this means is, everything you write and share online is being used, or will be used in the future, to devise the most effective strategies to manipulate and control us all.

That doesn't mean you can't or shouldn't use it, though. It just means you need to be mindful of the downsides, and use it in a way that optimizes your own benefit while minimizing the risks. It's a spy machine, yes, but if used with care, it can massively speed up your learning curve of things like basic biology and physiology.

Once it becomes available, also consider checking out Adams' natural health-focused LLM which, as mentioned, will also have additional privacy features. His AI is being trained to answer questions specifically relating to health, nutrition, holistic medicine practices from around the world, biodynamic and regenerative food production and much more, without the Big Pharma bias.

I am really interested to hear your thoughts on this topic and look forward to reading your comments.

Sources and References

- [1] Sky News August 17, 2023
- [2] Natural News December 6, 2023

- [3] Make Use Of April 17, 2023
- [4] Make Use Of April 1, 2023
- [5, 7] The Conversation February 7, 2023
- [6] Fast Company January 11, 2023
- [8] OpenAI Privacy Policy November 14, 2023
- [9] Brookings November 29, 2018