501CISO
501C CYBERSECURITY LEADERSHIP
Powered by ClearTone Consulting, LLC

AI / CHATGPT POLICY

What is ChatGPT?

ChatGPT is a generative AI language model developed by OpenAI, based on the GPT (Generative Pre-trained Transformer) architecture. It is a state-of-the-art language model that is capable of generating human-like text based on the input it receives.

ChatGPT is trained on a massive dataset of text from the internet, including books, articles, and websites, and it uses deep learning techniques to generate responses that are contextually relevant and grammatically correct. It can be used for a variety of natural language processing tasks, such as language translation, summarization, and conversation generation.

One of the most significant advantages of ChatGPT is its ability to generate natural-sounding responses that are often difficult to distinguish from human-generated text. This makes it an excellent tool for conversational applications, such as chatbots, customer service, and virtual assistants.

However, like all AI technologies, there are also concerns about the ethical implications of ChatGPT's use, particularly in areas such as bias, privacy, and the potential for misuse. As such, responsible use of ChatGPT, along with appropriate regulation and oversight, is essential to ensure that it is used for good and benefits society as a whole.

How might we use ChatGPT at work?

There are many ways a small business could use ChatGPT to improve their operations and engage with customers. Here are a few examples:

> Chatbot: A business could use ChatGPT to develop a chatbot that can answer common customer inquiries and provide basic support. ChatGPT can help the chatbot generate more natural-sounding responses and improve the overall user experience.
>
> Content creation: ChatGPT can help a business generate content for their website, social media channels, and marketing materials. This can save time and resources while still producing high-quality content that is engaging and informative.

Customer engagement: A business could use ChatGPT to engage with customers on social media platforms, such as Twitter or Facebook, by generating responses to customer inquiries or comments. This can help improve customer satisfaction and loyalty.

Language translation: If a business operates in multiple countries or serves customers who speak different languages, ChatGPT can be used to translate content quickly and accurately. This can help the business expand its reach and communicate effectively with a broader audience.

Research and analysis: ChatGPT can help a business analyze customer feedback or reviews to identify common themes or issues. This can help the business make data-driven decisions and improve its products or services.

It's important to note that while ChatGPT can be a valuable tool for small businesses, it's essential to use it responsibly and ethically. This includes ensuring that any AI-generated content is fact-checked and edited by humans, and that data privacy and security are prioritized.

ChatGPT Policy

Our business recognizes the potential benefits of using artificial intelligence (AI) to improve efficiency and productivity in the workplace. However, we also acknowledge the importance of using AI responsibly and ethically, particularly when it comes to generating content.

Our policy aims to provide guidelines for the responsible use of AI-generated content, emphasizing the need for proofing, editing, fact-checking, and using AI-generated content as a starting point, not the finished product.

Requirements for AI-generated content:

- Proofing: All AI-generated content must be proofread and checked for accuracy by a human before being published or shared. This includes checking for spelling errors, grammar mistakes, and factual inaccuracies.

- Editing: AI-generated content must be edited to ensure that it is well-written, coherent, and engaging. This includes ensuring that the content is structured in a logical manner and that it is appropriate for the intended audience.
- Fact-checking: AI-generated content must be fact-checked to ensure that all information is accurate and up-to-date. This includes verifying sources, checking statistics, and ensuring that any claims made in the content are supported by evidence.
- Starting point, not the finished product: AI-generated content should be viewed as a starting point, not the finished product. While AI can provide a valuable tool for generating content, it cannot replace the creativity and critical thinking skills of human writers and editors.

Guidelines for responsible use of AI-generated content:

- Transparency: All AI-generated content must be clearly labeled as such, and the use of AI in generating content should be transparent to employees and customers.
- Data privacy: We must ensure that any personal or sensitive data used to train AI models is handled with appropriate care and that any AI-generated content that contains such data is handled in compliance with data protection laws.
- Fairness: We must ensure that AI-generated content does not discriminate against any individual based on their protected characteristics, such as race, gender, age, or disability.
- Liability: Our company must take responsibility for any harm caused by AI-generated content, and we must have insurance coverage to protect against potential legal claims.

Do not share proprietary data with ChatGPT

As an AI language model, ChatGPT is designed to process and generate language based on the input it receives. While ChatGPT is a sophisticated tool that can provide

helpful insights and responses, it is not inherently equipped to handle sensitive information.

Since ChatGPT is a digital tool that can potentially be accessed by others, it may not be appropriate to share proprietary and confidential information with it. There is a risk that the information could be exposed or misused, either through a security breach or by unintended parties gaining access.

Additionally, ChatGPT is not a legal entity and is not bound by the same confidentiality agreements or legal protections as human employees or contractors. As such, it may not be able to guarantee the same level of discretion and confidentiality that a trusted human partner could provide.

In summary, businesses should exercise caution when sharing proprietary and confidential information with ChatGPT, as doing so could pose a security risk and potentially compromise sensitive data.

SIMPLE USAGE GUIDELINES

Acceptable AI Usage:

- Enhancing Productivity: Utilize LLMs to improve productivity in tasks such as drafting documents, drafting reports, or automating responses where appropriate.
- Verify Facts: If you use the LLM to gather information or generate content that includes facts or data, verify and cite the original sources when necessary. Never trust facts provided from an LLM without verification.
- Follow Legal and Ethical Guidelines: Use LLMs in a manner that adheres to applicable laws, ethical guidelines, and professional standards.
- Report Issues: Immediately report any security or privacy issues related to the use of LLMs to the IT department.

Unacceptable AI Usage

- Sharing Sensitive Information: Avoid sharing any personal or organizational sensitive data with the LLM, as this can lead to privacy breaches.
    - Avoid disclosing staff names, titles, or direct contact information without proper authorization.
    - Do not share financial information such as budgets, salaries, financial statements, or any confidential financial data.
    - Refrain from discussing details about human resource activities, including terminations, disciplinary actions, or new hires.
    - Do not reveal details about the organizational structure, internal processes, strategic plans, or any other information that could undermine the organization's operations.
- Use for Decision-Making Without Verification: Do not solely rely on LLM-generated information for critical decision-making without additional verification from credible sources.
- Bypass Security Protocols: Never use LLMs to attempt to bypass network security protocols, engage in unauthorized access, or decrypt secure data.
- Violate Copyrights: Avoid using LLMs to generate content that may infringe on copyrights or other intellectual property rights.
- Ignore Organizational Policies: Always adhere to organizational policies and guidelines specific to the use of technology and data handling.
- Don't Input Confidential or Sensitive Content:
    - Avoid inputting any information that you would not be comfortable seeing published on your organization's website.
    - Do not use LLMs to generate or handle content that could be sensitive, confidential, or potentially damaging if leaked.
- Don't Input Spreadsheet Data:
    - Avoid copying and pasting data directly from spreadsheets into LLM interfaces. This prevents the accidental sharing of sensitive or confidential information that might be contained within spreadsheet cells.

- Do not use LLMs to process spreadsheets containing proprietary data, personal information, or any other sensitive organizational details without ensuring that all such data has been properly anonymized or sanitized.
- Be cautious of metadata that may inadvertently be included when copying data from spreadsheets, as this can also contain sensitive information.

These guidelines aim to balance the innovative potential of LLMs with the need to mitigate risks associated with their use, ensuring that they contribute positively and safely to the organization's objectives.

501CISO is a cybersecurity consultancy supporting associations and mission-based nonprofits provided by ClearTone Consulting. We provide expert knowledge, strategy, implementation, leadership and risk assessment to improve your organization's risk position and minimize the likelihood of successful cyber-attacks.

Contact brianscott@cleartoneconsulting.com to learn more.