

Generative Artificial Intelligence (AI) Tools

GUIDANCE DOCUMENT



UNIONCOUNTY
INFORMATION TECHNOLOGY

ChatGPT / Artificial Intelligence Tools and Union County

With the advent of OpenAI's ChatGPT, generative artificial intelligence (AI) and Large Language Models (LLM) are becoming more popular and enticing to the general public. Using Artificial Intelligence, Learning Language Modules learn from huge volumes of data gathered across repositories such as the internet. The success of a Learning Language Module is the size of its data that it is trained to use, in most cases this includes everything that has been written and stored on the internet. While ChatGPT and similar Large Language Model (LLM) tools such as Microsoft's Bing and Google's Bard may ease the burden of writing comprehensive documents, it is important to use such tools with caution.

When staff enter prompts, questions or provide documents to these tools for recommended improvements, the county may be exposed to unintended risks. Risks to using AI tools may include but are not limited to the violation of data privacy laws such as Health Information Portability and Accountability Act (HIPAA); increased cybersecurity threats and even copyright infringement.

This guidance applies to all Union County employees and those assigned county network credentials.

Data Privacy Risk

Users must exercise caution when inputting data into ChatGPT/Bard/Bing. The AI tool will consume information and process data to generate a response on your behalf. This and similar tools may retain all the information provided to facilitate responding to any future requests and to improve their own AI model and its responses. It is important to recognize the sensitivity of data that you are entering and that it will easily become publicly available. For example, inputting data that includes Personally Identifiable Information (PII), Public Health Information (PHI) or other sensitive information may violate regulations such as PCI, DSS or HIPAA that could expose the county to reputational or legal risks including significant fines. Before providing a document to ChatGPT as input, carefully look at all pages to ensure sensitive information is not included.

In the state of North Carolina, N.C. General Statutes – Chapter 14, Article 19C, Identity Theft, 14- 113.20 classifies the following as Personally identifiable information (PII):

- (1) Social security or employer taxpayer identification numbers.
- (2) Driver's license, State identification card, or passport numbers.
- (3) Checking account numbers.
- (4) Savings account numbers.
- (5) Credit card numbers.
- (6) Debit card numbers.
- (7) Personal Identification (PIN) Code as defined in G.S. 14-113.8(6).
- (8) Electronic identification numbers, electronic mail names or addresses, Internet account numbers, or Internet identification names.
- (9) Digital signatures.
- (10) Any other numbers or information that can be used to access a person's financial resources.
- (11) Biometric data.

- (12) Fingerprints.
- (13) Passwords.
- (14) Parent's legal surname prior to marriage.

Increased Email Phishing Threats

Phishing emails designed to deceive people into clicking bad links, opening malicious attachments, or giving their usernames and passwords to cyber criminals is the most common cyber security threat. Cyber criminals and bad actors are already using tools like ChatGPT to write proper business letters, email, etc. The greater the clarity sophistication of the content, the greater the likelihood that phishing emails are less detectable and less likely blocked by email filters and human review.

Copyright Infringement

Due to the processing engine of AI tools like ChatGPT, it may provide information or content that is reserved by an existing copyright. AI tool responses consist of data gathered by others with no clear way of knowing the true source. If your documentation mistakenly includes copyright or proprietary intellectual property, such information could find its way into a response to another user's question. Anyone using ChatGPT/Bing/Bard and incorporating responses into a work that is distributed should ensure that the information produced does not infringe upon copyrighted material. Please check with the county's Legal department if in doubt.

Inaccurate Information

While AI Large Language Models (LLM) like ChatGPT can yield results that are impressive, it is important to remember that it may not be accurate. Items of concern:

- This may come in the form of human error as the AI can only generate information based on its comprehension of the user inputting the question or request.
- The validity of the information that the AI produces may also be questionable or incorrect depending on its original source.
- ChatGPT/Bing/Bard may be inherently faulty by design. OpenAI, the founding organization behind ChatGPT, has identified that there are possible inaccuracies that are being worked on and addressed.

County Acceptable Use Guidance

Used appropriately and with data security in mind, ChatGPT and similar tools can be a good starting point to explore a topic and assist with document creation. However, it must only be used to provide input to county work efforts and not a standalone final product. As the warnings advise on ChatGPT and other AI LLM websites, what is proposed could be wrong or biased. Final copy of any work product should be your own.

Any information that is entered or provided to ChatGPT or other LLMs are assumed to be publicly available. Therefore, employee information, software code, or any other proprietary data owned by Union County may not be input to products like ChatGPT.

There are multiple AI/LLM tools like ChatGPT available now not only for general writing but video, computer programming, presentations and more coming available. At this time, these tools are available through the county network and internet connection; however, access to these tools/sites will be continually reviewed for its benefits versus security risks to the county. If in doubt or if you have questions, please contact either the Director or Assistant Director of Information Technology.