# Think Intelligently About Artificial Intelligence at Home

Artificial intelligence, including so-called “large language models” like ChatGPT, has rapidly become a major talking point in the press, amongst governments, and maybe even in your department!

While AI has been a subject in the background for decades, everyday web users can now engage with AI like never before. Metro continues to develop policy and guidance around the use of this transformative technology, but it is important to keep in mind the need to securely use AI when not at work.

Whenever there is a sea change in technology, it is always smart to think about the security issues. This is how you can stay safe online over the years.

With any shiny new technology, you should consider security and privacy risks before diving in. When it comes to AI-powered language models and other services, there are a few major factors to consider when loading up AI for help at work, school, or for fun. And no AI wrote this article – I promise!

## DON’T HAND OVER YOUR CROWN JEWELS!

Data, including user input, might be used by the companies that power these systems. Any information that includes personally identifying information could inadvertently be shared with others.

Remember, AI models partly “learn” from what users input into the system. Therefore, you shouldn’t put any information into an AI model you want to keep private, including any sensitive information about your family.

## PROMPTING ISN’T THE SAME AS CREATING

When it comes to your child’s homework or perhaps your own work endeavors, know that putting a query to AI and then copy/pasting the results isn’t the same as doing the work yourself. Consider the following when deciding to cite the use of AI when it is used to produce any content:

1. Did its output form a **substantial part** of your presentation, analysis, or argument?
   “Significant Contribution” - Cite AI-generated content when it makes a significant contribution to your work. If the AI-generated content forms a substantial part of your presentation, analysis, or argument, it's advisable to provide proper attribution.

2. Did its output have a **distinctive impact on the overall message** or findings or play a crucial role in shaping the information presented?
   “Distinctive Impact” - If the AI-generated content has a distinctive impact on the overall message or findings, it's a good practice to cite it. This is especially true if the AI plays a crucial role in shaping the information presented.

3. Did its output **provide critical or unique information** that is not easily obtainable from other sources?
   "Critical Information" - Consider citing AI-generated content when it provides critical or unique information that is not easily obtainable from other sources. This is important for transparency and giving credit where it's due.

4. Was its output copied **verbatim**?
   "Verbatim Use" - To avoid plagiarism concerns, cite AI-generated content as you would any other source when using verbatim text or when the ideas presented are directly drawn from the AI-generated material.

## "INTELLIGENCE" DOESN'T MEAN INFALLIBLE

If you are asking a fact-based question to an AI model (like "what atoms are in a water molecule?") you need to fact check everything, because these models have become infamous for giving very confident but very wrong information in many situations. Other times, people have noted that AI models produced bizarre – and sometimes creepy – responses suggesting that the model had a mind of its own, which have been deemed "hallucinations." We say it's best to look at AI models as tools: they can help you get the work done, but we think you're more talented than a machine!

It is important to understand the limitations of any AI being used. This includes understanding how it is trained, the sources of the training data and the currency of the training data.

## PRIVACY CONCERNS

There are many concerns over how AI models scrape the web, from how these programs utilize the creations of artists and writers to what sort of personal information they know about us. Many experts are worried that it is collecting data on children, for example, and how these services can alert people about sharing their data remains an open question. In many cases, your chats with an AI are not private – the company can see what you input, even if it is anonymized. Carefully read the privacy notices of any AI service you use and ensure that you are okay with sharing the data it collects.

Also, be aware of data collected by devices listening in your home. Be aware of the wake words used for your devices and review the privacy settings and notices for any such devices.

## BAD GUYS ALSO USE AI

Another trend is the rise of cybercriminals using AI to get better at their crimes. There is evidence that bad actors are using AI to craft more deceptive phishing emails and help develop malware. When there is any big disruption in tech, take it as a good time to review your cybersecurity basics: use strong passwords, take advantage of password managers, and enable MFA for all accounts that allow it.

---