Greater Milwaukee Foundation

Artificial intelligence (AI) has been around and evolving for over 50 years. Traditional AI, such as machine learning, has become a valuable tool for understanding complex data sets, creating efficiencies and making informed business decisions. This technology is incorporated into many business systems. AI predicts email responses, summarizes Zoom recordings and keeps organizations safe from phishing attacks.

Recently, the release of generative AI tools, such as ChatGPT, has changed how individuals think about AI and how to use it in the future: the outputs have shifted from predictive to creative. AI can now draft a proposal, generate images for marketing and even simulate speech. As exciting as these potential applications are, there are genuine risks to using them both in personal and business contexts.

Ethical and Legal Concerns

Four (4) main ethical and legal concerns exist related to generative AI:

- Bias: Because the data that AI uses is "trained" by humans, the data can be biased based on the unconscious (or conscious) biases of these people. How do we know who is training AI and how can we

  prove models are unbiased?
- Trust: The data sets used by generative AI are so massive, it is impossible to know what data is being used for a specific task. How can we be sure the output is accurate?
- Privacy: It is currently unclear who sees the information that is input into a generative AI tool and how

  that information is protected. How can we be sure our data remains confidential?
- Ownership: Sometimes, generative AI produces outputs like text or imagery that are very similar to existing works. Many AI models are trained using material that is subject to copyright protections, trademark protections or other intellectual property rights. Who owns what AI creates and how do we ensure we are not infringing on others' intellectual property rights?

The policy landscape around the use of AI is evolving rapidly as government entities at every level examine the implications of generative AI on society. Like data privacy, AI regulation will begin in a patchwork fashion
- the Foundation is actively monitoring AI-related state and federal legislation.

Security Considerations

Because all AI systems use data to function, data security regulations and Foundation policies surrounding data security also apply to AI tools. While the IT team protects data on Foundation systems, it takes all employees working together to keep information secure.

Consider the following guidance when using Generative AI tools:

- Never input any (a) personally identifiable, confidential or sensitive business information, or (b) content that is abusive, illegal, protected by intellectual property rights or in violation of Foundation policies into a Generative AI app like ChatGPT.
- Do not input any data or "ask" ChatGPT or other generative AI apps anything you would not want as a headline on the front page of a newspaper.

Responsible Use Cases

The following are examples of ways to responsibly use generative AI at work. Before using this type of AI, employees must gain approval from their people leader.

- Creating initial summaries of a book, article or whitepaper
- Creating preliminary, working drafts of an email response (if the input does not include names or specific Foundation data)
- Asking a question and starting your thinking with some generated "ideas"
- Writing a first draft of a document (again - no specific Foundation data or personal information)

Employees are responsible for fact-checking and reviewing all content generated by AI and for ensuring that their AI use is consistent with the ethical and legal considerations described in this policy.

If employees have any questions about the use of generative AI at work or suspect there has been data input into an AI app in a manner inconsistent with these guidelines, contact the IT and Facilities Manager immediately.