AQUA-AEROBIC SYSTEMS, INC.
A Metawater Company

Quick Reference Guide: Using POE Securely and Effectively

Welcome! This guide has simple tips for using AI safely and effectively at work. These best practices ensure we get the most out of AI without risking sensitive information.

AI Working Group document (from Q:\AI-Artificial Intelligence\) - updated 11/22/2024

- Report on Potential Uses of AI 2024-10-01.pdf

Uploading Documents and Security

Pertaining to the question that was raised in terms of uploading potentially sensitive and confidential documents into the AI platform, here are some basic starting points:

1. Publicly available or open-source- A great majority of work we do (80-90%) relates to documentation that is either already in the public domain, or is intended to be in short order after a master version is revised according to specific project requirements. These are typically municipal projects that are procured through ABC or a version of a direct-bid approach. This applies to many different document types, including AASI standard specs, engineer's specifications, vendor specifications and data sheets, etc, contractor terms and conditions, etc. In these cases, there is **no concern** with using these documents for this purpose, nor the output they generate.
2. Sensitive, private, industrial or military - For documents pertaining to private/industrial clients, collaborative delivery projects (i.e. DB, CMAR) or federal/military projects, there may be an additional level of caution that is required. For the time being, we will refrain from using AI functionality for these projects, but it is very likely that the security protocols, data privacy and firewall protection offered with enterprise-level AI platforms will also allow the use of sensitive documents without issue.
3. Strictly confidential - For documents specifically marked as "confidential", utilize the same process as #2 above. This extends to both AASI documents as well as third party.

As we further understand the use cases, security and data privacy of the specific platform we select, this guidance will be formalized into a full procedure which may evolve our position on these items. Again, it is very likely that the security protocols, data privacy and firewall protection offered with enterprise-level AI platforms will also allow the use of sensitive and even confidential documents without issue.

Top 5 Tips for Secure Use

1. Avoid Sensitive Data: Don't input personal, financial, or proprietary information. For example, avoid specifics like "Client A's billing info" or detailed product designs. Instead, use generic descriptions like "Client details" or "Project outline."

2. Use Generic Terms: If discussing internal projects or people, use initials or code names. This keeps sensitive details secure while allowing you to get the help you need from **POE**.

3. Keep Chats General: Use **POE** for brainstorming, summaries, or general inquiries. Avoid using it for tasks that would reveal detailed internal data.

4. Limit Data Retention: If **POE** provides output you want to save, be mindful of where and how you store it. Avoid saving it in places with broad access or limited security.

5. Share Feedback: If you notice anything odd or have questions about security, let the team know! We're all learning together, and your insights help keep our use of **POE** safe and productive.

Do's and Don'ts

- DO ask **POE** for help with general knowledge, summaries, or brainstorming.
- DO use code names or initials when discussing sensitive topics.
- DON'T paste confidential data, including client names, sensitive company info, or personal details.
- DO feel free to reach out with any questions or if you need guidance on a specific use case.

Frequently Asked Questions

- Why can't I share sensitive data? **POE** doesn't store data permanently, but exercising caution helps prevent accidental exposure of our sensitive information.

- Can I ask **POE** about a specific project? Yes, but keep details general. Instead of describing every aspect, focus on asking for general advice or ideas that don't require confidential information.

- How should I handle the output I want to save? Make sure you store it in a secure location, ideally one with access restrictions to keep it within our team.

By following these simple steps, you're helping to ensure that we all get the most out of **POE** without compromising our data. Thanks for being part of keeping our use safe, effective, and fun!