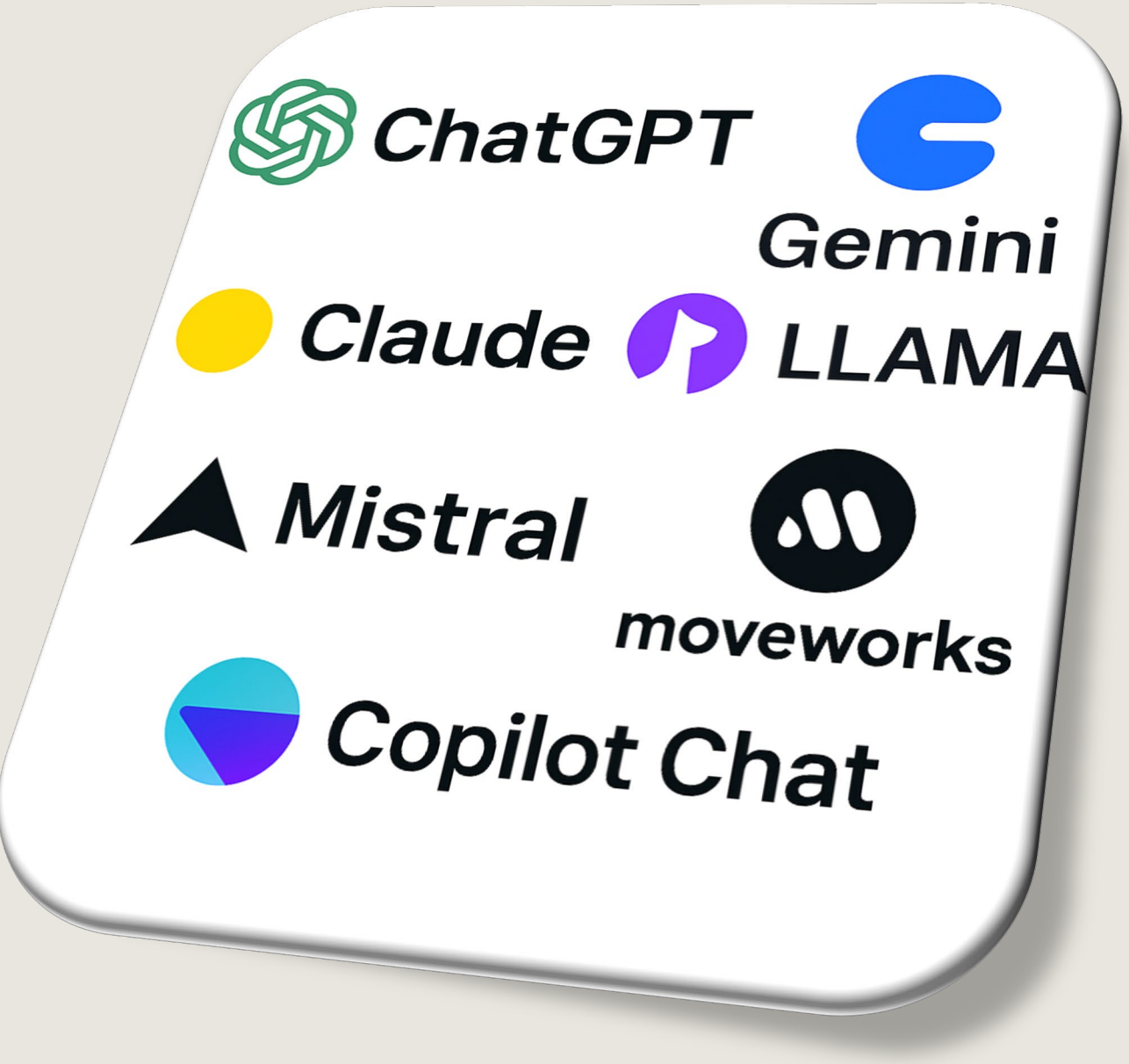
SPOKANE COUNTY
ADOPTION & GOVERNANCE OF AI



AI PLATFORM SELECTION

AI tools have been rapidly adopted and leveraged across the workplace, spreading like wildfire. At Spokane County we found ourselves scrambling to catch up—trying to understand not only what AI is, but also its implications and security risks. We quickly found ourselves asking the important questions.

- Do we allow AI to be used?
- What are the risks?
- Which AI platform is the safest?

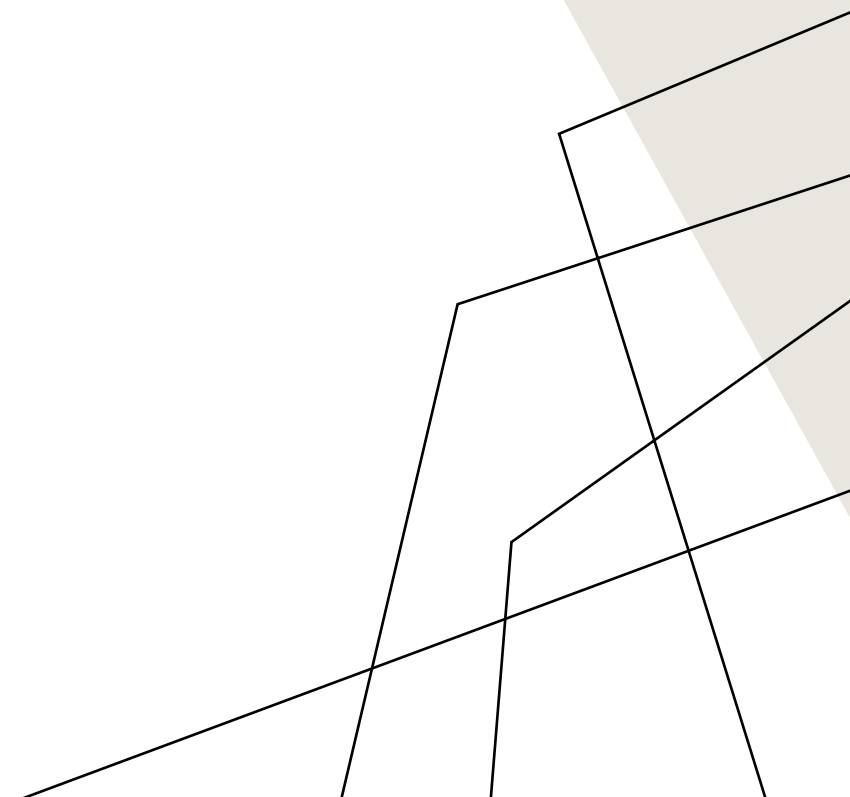
We evaluated each of these questions independently.

DO WE ALLOW AI TO BE USED?

With AI's advantages on improving workflow efficiency, fast information gathering, problem solving, and content creation, the answer is a no-brainer. We have to, carefully, and with appropriate policy in place.

With many other organizations asking the same question, we felt that allowing usage of AI in the workplace would benefit business processes by augmenting workflow efficiency. Additionally, the rapid adoption of AI tools by employees makes it clear that AI is perceived as an essential resource in the workplace.

And now you can't swing a cursor without hitting an app or software that's branded as 'AI-powered.' The revolution isn't coming—it's already here. But at what cost?



WHAT ARE THE RISKS?

- **AI Hollucinations:** Generates information that sounds plausible but is actually **false, misleading, or entirely made up**.
- **Data Leakage:** Employees may unintentionally input sensitive or proprietary information into AI tools, risking exposure of confidential data.
- **Compliance and Legal Risks**: Using AI-generated content without understanding licensing, copyright, or regulatory implications can expose the organization to legal challenges.
- **Erosion of Critical Thinking**: Overreliance on AI can reduce employees' analytical skills and judgment, especially if outputs are accepted without scrutiny.
- **Bias and Ethical Concerns**: AI models can reflect and amplify societal biases, leading to discriminatory or inappropriate content if not carefully monitored.
- **Phishing and Social Engineering**: AI can craft highly convincing phishing emails or impersonate executives using deepfake audio or text, increasing the risk of credential theft and unauthorized access.
- **Malware Obfuscation**: Threat actors can use AI to generate polymorphic malware—code that constantly changes to evade detection by antivirus and endpoint protection tools.

REAL WORLD RISKS

One of the most striking cases involved a multinational company in Hong Kong, where an employee was tricked into transferring over $25 million during a video call populated entirely by AI-generated deepfakes. The scammers used AI to impersonate the company's CFO and several other executives, creating a convincing video conference. The employee, believing they were speaking with real colleagues, followed instructions to make multiple high-value transactions. It wasn't until later that the fraud was discovered—none of the people on the call were real.



WHICH AI PLATFORM IS THE SAFEST?

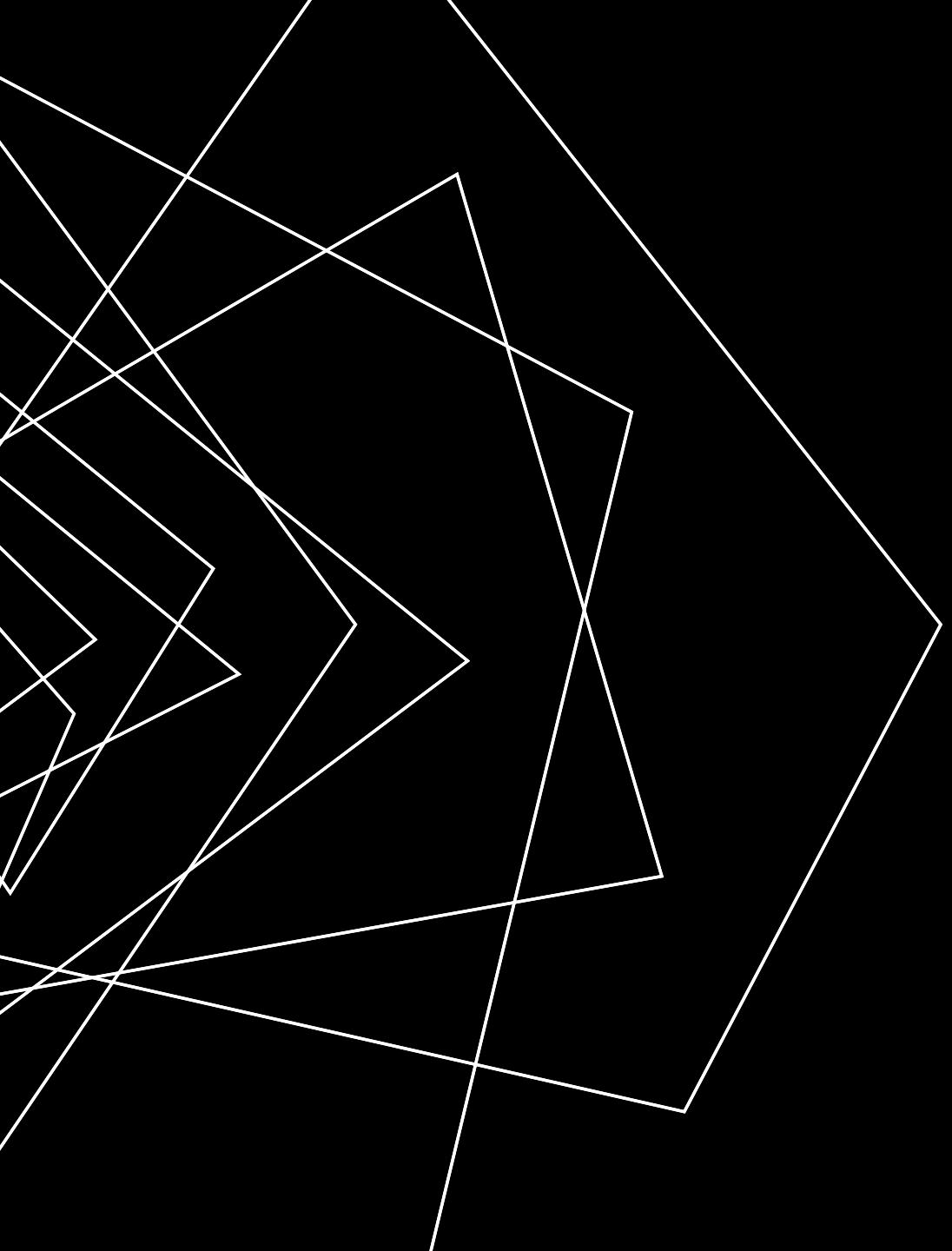
There’s a plethora of AI tools available these days. All of which have their own set of inherent risks and limitations. So, do you choose one, or many? For multiple reasons, Spokane County has taken the stance to standardize on a single sanctioned AI chat platform, Microsoft Copilot Chat. We felt this product has the best overall industry leading AI engine based on GPT-4 created by OpenAI. Plus Copilot Chat offers the most seamless integration to our other Microsoft products. And more importantly, it allows robust security and administration than Copilot’s competitors such as ChatGPT.

The greatest threat outside of AI itself is the unchecked human use of it. When employees leverage generative AI without oversight, the security risks can exceed anything we’ve previously encountered.

SOLUTION

Our approach to AI in the workplace.

- Standardize on a single AI chat platform to streamline management, strengthen controls, simplify oversight, reduce risk, and maintain enterprise-grade security.
- Create and implement policy that clearly defines proper access and use of AI.
- Make sure policy includes AI generated content will be reviewed, validated, and verified by a human before use. No exceptions.
- Block the use of all other AI chat platforms within the organization.
- Make best effort to stay informed of the exceedingly rapid AI advancements in capability and the evolving risks.



Conclusion

Amid AI's unprecedented evolution, even its creators can no longer fully explain how or why it sometimes reasons, deceives deliberately, or makes autonomous decisions. It is paramount that there are safeguards, governance, and even law created to keep this revolutionary technology in check and in balance.

Additionally, it is our responsibility to ensure that any governance placed around AI be reviewed consistently and often to ensure proper boundaries evolve to match the constant change and evolution of AI and the ambivalent power within.

THANK YOU