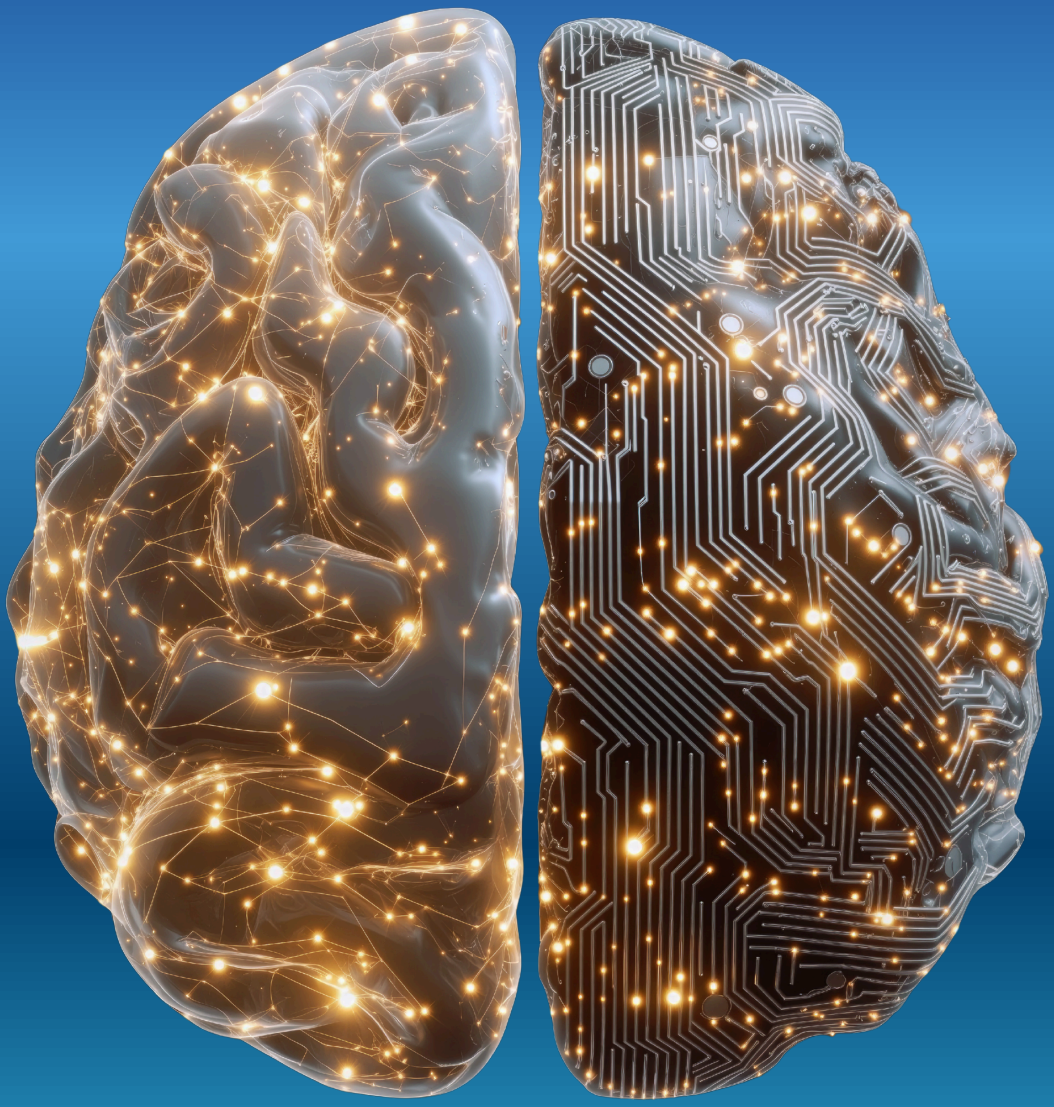

DOs & DON'Ts for using AI at work

OFFICE OF STATE TECHNOLOGY

ARDATA
ardata.arkansas.gov

DOs

✓ Do Use Approved AI to Support Work Goals

Leverage Artificial Intelligence (AI) tools approved by Office of State Technology (OST) to assist with official business tasks, ensuring they align with State/your department's objectives. It is imperative that the use of any AI tool(s) for State business is done in compliance with the State's AI Policy and the State's Acceptable Use Policy. If you have any questions or concerns about policy compliance, consult with your department's Privacy Officer or the State Chief Privacy Officer.

✓ Do Maintain Confidentiality

Remember to handle sensitive information responsibly. Use anonymized or public data when possible. Users should never enter personal, confidential, or proprietary information into AI. Always consult with your department's privacy officer or the State Chief Privacy Officer if you are unsure or concerned about confidentiality.

✓ Do Inform Others When AI is Used

If AI-generated content or data is used in your work product, make it clear to others (including end users) that AI was part of the process (i.e. "Content generated with the assistance of AI"). Providing this notice builds trust and enables transparency in how AI is impacting decision-making.

✓ Do Report Inappropriate Outputs

If you encounter any AI-generated content that is inappropriate, biased, or harmful, report it to your department's privacy officer or the State Chief Privacy Officer immediately. This includes work within a sandbox that is a controlled environment. It is critical that we monitor and address any undesirable model behavior.

✓ Do Understand the Limitations of AI

Always verify AI outputs before using them in any decision-making or official processes. Recognize that AI is not a perfect tool. It generates content based on patterns from training data, and it can produce inaccurate or misleading information. Human involvement and verification are integral functions in the ethical use of AI.

✓ Do Protect AI Integrity

Keep the environment secure by following cybersecurity best practices and effective policy. If you observe any suspicious activity or technical issues (these could be unauthorized access or log-in attempts at odd hours from locations outside of normal geographic boundaries), notify your department's privacy officer or the State Chief Privacy Officer right away so they can set the appropriate protocols in motion.

✓ Do Collaborate and Seek Continuous Improvement

Work in partnership with others across departments and agencies to build AI knowledge and skills. AI is rapidly evolving, so aim to stay informed and improve your AI practices continuously. While no one source is perfect or all-encompassing, State Employees may utilize Innovate-US (www.innovate-us.org) as a no-cost resource for training. Additionally, the Office of Personnel Management will be developing AI training available to all employees at no cost.

DON'Ts

Don't Input Sensitive Data

Protected, or any data classified or deemed to be sensitive in nature must never be entered into or processed by any AI system. This includes (but is not limited to) customer information, employee records, intellectual property, financial data, or any information governed by legal or privacy regulations. Any mitigation and deidentification strategies must fully comply with state policies to ensure that protected information is never uploaded, processed, or exposed when using AI tools while still reaping the benefits of AI.

Don't Circumvent Security Protocols

Do not attempt to modify, hack, bypass or ignore security protocols in place. Any attempt to do so compromises the security and integrity of the system. Ensure all AI use stays within the established security and compliance boundaries, and do not tamper with or alter the AI models. Do not attempt to introduce external data sources or transfer AI outputs to unapproved environments.

Don't Use AI for Unethical Purposes

The use of AI to create misleading, harmful, or discriminatory content is strictly prohibited. As a state employee, you must ensure you are operating within your legal obligations and statutory purpose. Keep in mind that those who may be harmed or impacted by your actions are not always direct users of the system according to the National Institute of Standards and Technology's AI Risk Management Framework.

Don't Over-Rely on AI Outputs

AI can be a helpful tool, but it is not a replacement for human judgment. Don't assume the AI-generated content is 100% accurate or reliable. Always review, refine, and verify its outputs before applying them in your work.

Don't Share Content Externally

Do not share AI-generated content or outputs outside the organization without proper permission, especially if it contains any State-related information. Always work with your department's privacy officer or the State Chief Privacy Officer to ensure all policies and prescribed protocols are followed if content is shared outside of your department.

Don't Forget About Bias

AI models can sometimes reflect biases present in their training data. The National Institute of Standards and Technology AI Risk Management Framework identifies the following categories of AI bias: systemic, computational & statistical, and human cognitive. Don't ignore signs of biased outputs whether it's in language, tone, or content. Be vigilant and actively question the fairness of AI results.