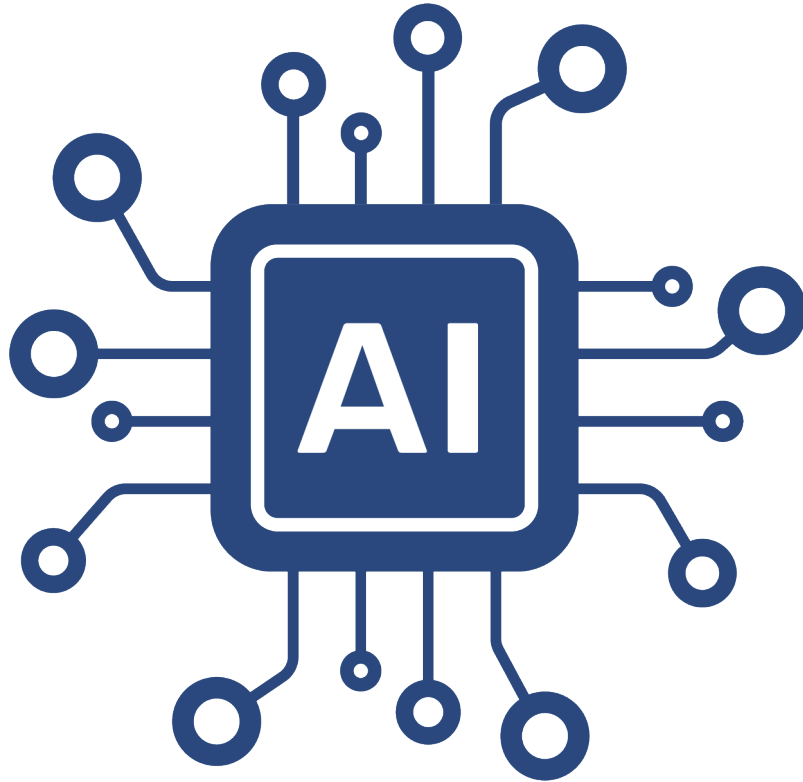




DO'S AND DON'TS FOR USING AI AT WORK

MANAGEMENT
PERFORMANCEHUB





DO'S

✓ **Do Use Approved AI to Support Work Goals**

Leverage Artificial Intelligence (AI) tools approved by MPH and IOT to assist with official business tasks, ensuring they align with State/your agency'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](#). If you have any questions or concerns about policy compliance, consult with your [Agency Privacy Officer \(APO\)](#):

- <https://www.in.gov/mph/cdo/files/State-Of-Indiana-Agency-Privacy-Officers.pdf>

✓ **Do Maintain Confidentiality**

Remember to handle sensitive information responsibly. Use anonymized or public data when possible. Avoid entering Personal Information (PI), confidential, or proprietary data that could still present a risk if misused. Always consult with your [APO](#) if you are unsure or concerned about confidentiality.

- [View the OCDO Data Suppression & Obfuscation Guidance Document at in.gov/mph/cdo/files/20230908-FINAL-OCDO-Guidance-Suppression-and-Obfuscation.pdf.](#)

✓ **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 APO 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 is an integral function 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 APO 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 their access to LinkedIn Learning as a no-cost resource. Additionally, you could work with your APO to contact your agency's Director of Engagement and Analytics from Management Performance Hub (MPH) and ask about more up-to-date, reliable resources.



DON'TS

× **Don't Input Sensitive Data Without Proper Authorization**

Sensitive, protected, or confidential data must not be entered into AI systems without proper authorization. Only data considered public under the Access to Public Records Act (APRA, IC 5-14-3) may be used without approval. Sensitive data includes customer information, employee records, intellectual property, financial data and information governed by legal or privacy regulations. Before using sensitive data in AI systems, consult with your Agency Privacy Officer (APO) and obtain proper approval as prescribed by State or agency policy. Only APOs and the State Chief Privacy Officer (CPO) are authorized to approve mitigation and de-identification strategies that comply with state policy.

× **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**

Avoid using AI to create misleading, harmful, or discriminatory content. 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 the proper permissions, especially if it contains any State-related information. Always work with your APO to ensure all policies and prescribed protocols are followed if content is shared outside of your agency.

× **Don't Forget About Bias**

AI models can sometimes reflect biases present in their training data. The NIST AI RMF 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.