

AI GUIDING PRINCIPLES

Whenever you use AI, always remember to apply these 4 guiding AI principles. Together, these principles form a foundation for the responsible governance of AI, promoting the use of AI technologies in ways that are ethical, legal, respectful of privacy and security, and aligned with our institutional values and goals, all while we enable innovation, gain efficiency, and harness even greater untapped potential.

1. Integrity



- Promote educational and spiritual values and objectives.
- Prioritize data quality and accuracy.
- Develop and apply standardized processes.

2. Data Protection



- Embed security, privacy, data governance, and data retention.
- Prevent and mitigate risk.

3. Transparency



- Be honest and open.
- Provide clear information about when AI is in use.

4. Accountability



- Adhere to policies, standards, and procedures.
- Be responsible for how we use AI.

AI GUIDING PRINCIPLES: SELF-CHECK

For additional guidance, below is a quick checklist to assist you in adhering to the four AI Guiding Principles.

1. Integrity



- Use AI to promote educational and spiritual values and objectives, enhancing lives in positive and uplifting ways.
- Increase awareness of the strengths and limitations of the AI tool to set realistic expectations on how you can leverage it. Use it to supplement, not replace human work.
- Review data outputs to verify accuracy, relevancy, and data quality.
 - Always cross-check AI-generated results to make sure they are accurate and appropriate.
- Periodically evaluate the AI tool's performance using diverse and updated datasets to identify and address potential biases or inaccuracies.

2. Data Protection



Security

- Keep your device and application versions updated to prevent vulnerabilities.
- Ensure that if you use mobile app versions, they are kept up to date as well.
- Use Multi-Factor Authentication (MFA) to enhance account security.
- Only use well-vetted and approved AI tools.

Privacy

- Review the privacy notice and data handling/sharing practices of any AI tool before usage.
- Only use well-vetted and approved AI tools.
- Do not share data with any AI tool without a business contract to ensure data privacy.
- Do not expose sensitive data or violate privacy regulations.
 - Do not enter Nonpublic Institutional Data into any AI tool. This type of data includes personally identifiable employee data, FERPA-covered student data, HIPAA-covered patient data, and may include research that is not yet publicly available. Refer to BYU's Data Use, Privacy, and Security Policy for more information.
- Maintain the strictest default privacy settings within the AI Tool.
 - Do not allow your data or conversations to be used or stored to improve or train models when possible. If this is a requirement for usage, question if usage is strictly necessary.
- Stay informed about data privacy best practices, by participating in institutional trainings, asking questions, and learning together about this constantly evolving space.

Data Retention

- If feasible, delete chats or threads within an AI tool once they have fulfilled their intended purpose.
- Follow applicable data retention policies and standards for all data outputs.

3. Transparency



- Cite the use of AI tools when applicable.
- Maintain documentations of data handling, chatbot training protocols, and decision-making processes when appropriate and when used to make decisions that influence individuals and the institution.
 - Provide individuals insight into AI-enabled decisions when requested.

4. Accountability



- Take time to understand how the AI tool or software works and know its limitations.
- Use AI tools in appropriate and ethical ways, aligned to our institution's values and objectives.
 - Only input data and prompts that would not cause harm to an individual or the institution.
- Restrict access to customized GPTs or similar chatbots and data outputs based on user roles and responsibilities.
- When in doubt of what is appropriate use; ask, do not assume.
 - Ask your department CSR or OIT representative for clarification on AI usage or reach out to the CES Privacy Center for Privacy or AI Governance related concerns.
- Adhere to the existing policies, standards, and procedures put in place by the institution.
 - A few key ones are Data, Use, Privacy, and Security; Privacy Notice; Academic Integrity Policy; and CES Honor Code
- Stay informed. Participate in trainings to increase awareness and understanding of both potential risks and gains tied to the usage of various AI tools.