Guiding Principles for the Use of AI

Elder David A. Bednar counseled, "As you strive to learn the gospel of Jesus Christ and perform the work you have to do, I specifically exhort you to be wise in your use of contemporary technological tools. Innovations such as artificial intelligence have the potential to both (1) assist you in receiving magnificent blessings and (2) diminish and suffocate your moral agency."[1]

As a CES Privacy Center, we believe embracing the use of Artificial Intelligence (AI) technologies in responsible and ethical ways is essential to heeding this inspired admonition. To do this effectively, we want to promote researching, evaluating, and understanding new and innovative ways to incorporate well-vetted AI technology and practices into business and academic activities. We strongly encourage taking a measured and responsible approach, always weighing potential increases in efficiency, learning outcomes, and other wins against possible pitfalls that could damage our institution's stewardship to develop capable and trusted disciples of Jesus Christ.

As we incorporate AI into our daily activities, we encourage all stakeholders across CES to seek to maintain our unique spiritual environment and our role as innovators in higher education. In working with AI, we rely on the Spirit, wisdom, and trusted sources as we strive to align with the principles of 1) Integrity; 2) Data Protection; 3) Transparency; and 4) Accountability. These principles can be summarized as follows:

Integrity:

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

Integrity includes integrity in our data, our processes, and as individuals. It involves maintaining the quality and accuracy of data inputs and outputs when using AI systems. This principle requires us to develop and apply standardized processes and rules as we test and operate AI systems. It involves measures to mitigate risk, prevent data hallucinations, and to avoid biases and inaccuracies. Integrity requires a steadfast commitment to acting in ethical and inclusive ways to promote fairness and compliance. It also includes using AI technologies to promote our educational and spiritual values and objectives to enhance lives in positive and uplifting ways.

Data Protection:

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

Data Protection emphasizes both security and privacy. It encompasses the safeguarding of personal data against unauthorized access, use, and loss. This involves implementing robust security measures, adhering to data privacy laws (such as GDPR and FERPA), and ensuring that personal data is collected, used, and stored only for specified, legitimate purposes. Processing data in line with data governance standards and retention policies helps us handle it in a way that respects individual privacy rights and mitigates risk. Data Protection also includes prioritizing safety, avoiding harm to individuals, and using AI systems that are resilient and reliable.

Transparency:

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

Transparency is about making the AI systems' functionalities, data usage, and decision-making processes open and understandable to users and stakeholders. It entails providing clear, intelligible information about how AI systems operate, when they are in use, the data they use, and the logic behind their decisions. This principle supports the right to explanation, enabling individuals to understand and, if necessary, challenge AI-driven decisions.

Accountability:

- Adhere to policies, standards, and procedures.

[1] David A. Bednar, "Consider the Wondrous Works of God" (Job 37:14), BYU Devotional Address (Jan. 23, 2024).

- Be responsible for how we use AI.

Accountability entails our commitment to be answerable for the outcomes of the AI systems we use. This includes establishing clear governance structures that define roles and responsibilities within the institution for AI decision-making and ensuring that AI systems are used in compliance with ethical standards and legal requirements. Accountability mechanisms may include policies, procedures, internal audits, trainings, and the establishment of a committee to oversee AI practices.

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.

Self-Checklist

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

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.

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. Nonpublic Institutional 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.

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.

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.

This is a rapidly evolving space. Updates to this checklist may be needed at any time. Please check out https://genai.byu.edu for more information and updates.

Need additional help or have more questions?

Please contact:

Gabrielle Harris
CES Privacy Officer
Gabrielle_Harris@byu.edu
801-422-4219

Nick Turley
Mng Dir, CES IT Architecture
Nick_Turley@byu.edu
801-422-4994

Howard Loos
Chief Privacy Officer, BYU
Howard_Loos@byu.edu
801-422-2161