

Generative AI Acceptable Use Guidelines

Purpose and scope:

These guidelines outline how Generative AI technology may be used at Barton Community College. It applies to all employees, contractors, and third-party vendors who use Generative AI tools in their work with the college.

The goal is to protect sensitive information including Personal Identifiable Information (PII), ensure responsible, legal and ethical use of Generative AI technology while minimizing risks, maintaining the integrity and reputation of the college with data privacy and security.

These guidelines apply to all Generative AI use including but not limited to text, image, video, and audio generation for any purpose related to the college.

Approved AI Software Subscriptions and Platforms – Tools

Accountability:

The following college departments and groups provide oversight for managing AI use and serve as point of contact for resources, questions, and authorized use.

- Information Technology Services
- AI for All Advisory Council

Data privacy and security concerns:

1. Unknowingly sharing confidential college and customer data with external AI platforms.
2. Free AI tools should never be used to process sensitive information.
3. Such information includes but is not limited to following:
 - Student personal data
 - Employee personal data
 - Human Resources employee/student worker data
 - Financial Aid student data
4. Ensure all personal or sensitive data used by AI systems is anonymized.
5. Securely store all AI data.
6. Adhere to the college's data protection policies.
7. Recognize AI's limitations and ensure that any content is also checked by a human.
8. Utilize AI as a tool to be used alongside humans, not as a full replacement.

Legal and regulatory compliance:

This policy aligns with relevant laws (EU AI Act) and organizational values. Ensuring compliance with regulations for HIPAA (Health Insurance Portability and Accountability Act) or GDPR (General Data Protection Regulation), and handling retention of AI-generated content.

AI-generated content can lead to copyright violations, breaches of privacy laws, and/or the unintentional spread of misinformation. A lack of policy raises the risk of non-compliance, which could lead to costly lawsuits or regulatory penalties.

Authorized user guidelines:

Acceptable uses:

- Summarizing meeting notes or internal reports
- Drafting first versions of internal communications or drafting/summarization
- Automating repetitive tasks (e.g. formatting, tagging)
- Analyze data
- Create charts
- Answering technical questions

Unacceptable uses included but not limited to:

- Generating client-facing content without human review or approval
- Using AI to replace human judgement in decision-making processes
- Uploading or training tools on sensitive or proprietary data, especially in free versions of these tools.
- Do not enter personal data (PII) into unvetted third-party AI tools or services

If in doubt, check with your supervisor or Information Technology Services before using any AI tool for a new purpose.

Monitoring and review processes:

Providing training on effective uses and limitations of AI tools provides a regular process of review. This facilitates efficiency and adoption of new tools and prevents unauthorized use. This can then build confidence and prevent misuse of AI. Without proper oversight, AI tools may generate content that reflects hidden biases, factual errors, or problematic assumptions.

Regular reviews are accomplished by:

- Barton Technology Advisory Council (BTAC)
- Information Technology Services Tech Request Form

- AI for All Advisory Council (AIAAC) provides information about training and conducts refresher courses for faculty and staff on guideline updates
- BTAC and AIAAC reviews latest developments in AI

Enforcement

Unlike traditional security incidents that might involve isolating compromised systems, AI policy violations may require immediately suspending user access to specific AI tools, blocking certain types of prompts or content, or implementing enhanced monitoring for specific users or data types.

Ethical Considerations

Examples of Generative AI ethics include data responsibility and privacy, fairness, explainability, robustness, transparency, environmental sustainability, inclusion, moral agency, value alignment, accountability, trust, and technology misuse.

Reputation damage – AI tool misuse that results in unethical or discriminatory outcomes can lead to immediate, widespread backlash. Public trust is hard to earn and easy to lose.

Transparency – When and how AI contributes to a deliverable.

Key Components:

Artificial intelligence (AI): Software that mimics human intelligence to perform tasks like analyzing data, making decisions, or generating content (e.g. ChatGPT, Grammarly, Microsoft Copilot).

Generative AI: Is a subset of artificial intelligence that can create original content such as text, images, videos, audio, or software code in response to user prompts. (e.g., ChatGPT, GitHub Copilot, Prezi, Dall-E).

Machine Learning: Algorithms that improve through experience and data exposure, often used underlying application algorithms in AI tools. (e.g., Netflix, Facebook, image processing tools)

Transparency & Disclosure: Clearly stating when and how AI is used, including by employees or in publications (e.g., using language models).

Fairness & Bias Mitigation: Processes to identify and counteract discrimination in algorithms.

Privacy & Security: Handling personal data responsibly and securing AI systems.

Accountability: Defining who is responsible for AI development, decisions, and outcomes.

Safety & Risk Management: Testing and mitigating risks from powerful AI systems, including potential fabrication or errors.

Regulatory Compliance: Adhering to national and international laws (like GDPR).