

LIBRARY & INFORMATION TECHNOLOGY GUIDELINES FOR THE USE OF GENERATIVE AI

The University acknowledges the availability of generative artificial intelligence (“AI”) tools and services. There are important considerations to keep in mind when using these tools, including information security and data privacy, compliance, copyright, and academic integrity. These guidelines set forth guidance for the appropriate use of generative AI tools at Bucknell.

What is Generative AI?: Generative AI refers to a type of artificial intelligence that utilizes deep-learning models that can generate high-quality text, images, and other content based on the data they were trained on (such as ChatGPT, Dall-e, and Gemini).

Protect Confidential Data: No Generative AI tool meets the University’s security, privacy, and compliance standards for handling anything besides publicly available information in accordance with the University’s [Data Classification Policy](#) and [Appropriate Use Policy](#). You should never enter any institutional data or information protected by the Family Education Rights and Privacy Act (FERPA) into a Generative AI tool or service in accordance with the University’s [Student Records Policy](#).

Entering data into a Generative AI tool or service is like posting that data on a public website. Generative AI tools collect and store data from users as part of their learning process. Any data you enter into a Generative AI tool becomes part of its training data, which it may then share with other users outside the University and could expose proprietary or sensitive information to unauthorized parties.

Review Content Before Publication: Generative AI content can be inaccurate, misleading, or entirely fabricated (sometimes called “hallucinations”) or may contain copyrighted material. Generative AI material may exhibit biases and discriminatory ideas or content.

You are responsible for any content that you produce or publish that includes Generative AI material. You should review all outputs from Generative AI for accuracy, including spot-checking of sources or facts, and bias.

Adhere to Existing Academic Policy: Faculty should be clear with students they are teaching and advising about their policies on permitted uses, if any, of Generative AI in classes and on academic work. Students are also encouraged to ask their instructors for clarification about these policies as needed.

Be Alert for Phishing: Generative AI has made it easier for malicious actors to create sophisticated phishing emails and “deepfakes” (i.e., video or audio intended to convincingly mimic a person’s voice or physical appearance without their consent) at a far greater scale. Continue to [follow security best practices](#) and report suspicious messages to techdesk@bucknell.edu or by calling (570) 577-7777.

If you would like more information about Generative AI tools or have any questions, please contact the Library and Information Technology staff at techdesk@bucknell.edu.