Huntingdon College Guidelines: Use of Generative AI Tools

Definitions:

i. Public Generative AI is defined to be any generative AI, large language model (LLM), or similar technology that is openly accessible to the general public whether free or for compensation.

ii. Private Generative AI is defined to be any generative AI, large language model (LLM), or similar technology that has been procured for the private and explicit use of Huntingdon College, and is comprised of an instance not generally accessible to non-Huntingdon College employees and/or students.

iii. Sensitive Data for the purposes of this document will refer to data in any of the following categories:
   (1) Personally identifiable information (PII), as defined in the College's Information Security Policy
   (2) Personally identifiable financial information (PIFI), as defined in the College's Information Security Policy
   (3) Nonpublic personal information (NPPI), as defined in the College's Information Security Policy
   (4) Any HR Data that should reasonably be expected to remain a private record

iv. Academic Performance Data is defined as Data pertaining to student academic performance, including but not limited to: grade data and test scores

v. Public Data: Data reasonably known to be available to the general population via ethical means

vi. Submission to AI: is defined to be allowing any of the following:
   (1) Intentionally uploading all or part of the given data to Generative AI
   (2) Allowing Generative AI to have access in any capacity to the given data

Prohibitions and Allowances:

(The Qualified Individual is defined in the College's Information Security Policy.)

DATA CATEGORIZATIONS

Data Type	Generative AI Type	Submission Allowed?	Exceptions
Sensitive Data	Public	No	None
Sensitive Data	Private	No	Allowed with Written Approval of Qualified Individual
Academic Performance Data	Public	No	No

Data Type	Generative AI Type	Submission Allowed?	Exceptions
Academic Performance Data	Private	No	Allowed with Written Approval of Qualified Indivdual
Intellectual Property of Self	Public/Private	Yes	Unless the data falls into other categories in this chart that disallow this
Intellectual Property of Others or Other Entity	Public/Private	No	Allowed with Written Approval of Qualified Individual
Public Data	Public/Private	Yes	Unless access is from a device prohibited in this document

DEVICE ACCESS TO GENERATIVE AI

AI Access From Device	Generative AI Type	AI Access Allowed	Exceptions or Notes
Employee Device Allowed to House Sensitive Data	Public and/or Private	No	None
Employee Device NOT Allowed to House Sensitive Data	Public and/or Private	Yes	Use must follow guidelines about data submission
Academic Performance Data	Public	No	No
Academic Performance Data	Private	No	Allowed with Written Approval of Qualified Indivdual

Acquisition of Generative AI or LLM Tools

Acquisition of any technology falling into these categories should follow the standard technology approval process at the College at the time.

Rationale for this Document

1. Information Security: data security and cybersecurity are paramount. Generative AI tools are emerging, as are best practices for security protocols surrounding AI tools.
2. Intellectual Property: College employees should not misuse the intellectual property of others, per our Intellectual Property Policy. Vetting whether data is being used to train a LLM or Generative AI is important and requires thorough investigation.
3. Accuracy: The accuracy of output from Generative AI and LLMs is known to not always be accurate, so using such tools for a particular task must weigh this.
4. Bias: Some Generative AI tools or LLMs may output data that is biased, discriminatory, offensive, or otherwise potentially damaging. This must be weighed when considering output from such tools.