GENERATIVE AI TOOLS USAGE

I. Policy Section

15.0 Information Technology

II. Policy Subsection

15.4 Generative AI Tools Usage

III. Policy Statement

This Generative AI Tools Usage Policy governs the use of GRCC unlicensed 3rd party AI services to perform GRCC work, processes, and tasks.

IV. Reason for Policy

The emergence of generative AI tools (e.g. ChatGPT) holds the possibility for increased efficiencies, including assistance with tasks such as composing emails, drafting documents, and writing code. Generative AI technology also creates concern regarding the potential for privileged data exposure. The purpose of this policy is to ensure responsible, ethical, and secure use of generative AI tools.

V. Entities Affected by this Policy

This policy will affect employees, volunteers, and contractors that have been granted access to resources containing PII or other sensitive data.

VI. Who Should Read this Policy

Employees, Volunteers, and Contractors

VII. Related Documents

- Personally Identifiable Information Policy
- Family Education Rights to Privacy Act (FERPA)
- Health Insurance Portability and Accountability Act (HIPAA)
- Payment Card Industry Data Security Standard (PCI-DSS)
- Gramm–Leach–Bliley Act (GLBA)
- GRCC Information Security Program
- GRCC Acceptable Use Agreement (AUA)

VIII. Contacts

- Policy Owner: Chief Information Officer
- Information Security Officer
- Information Security Analyst
- Data Privacy Officer
- HIPAA Security Officer
- Registrar/FERPA Security Officer

IX. Definitions

A. Generative Artificial Intelligence (AI) – A broad concept encompassing various forms of content generation.

B. Large Language Model (LLM) – A category of generative AI models with a specialized focus on text-based data, serving as a basis for a wide range of natural language processing.

C. GPT (Generative Pre-Trained Transformer) - A GPT can take simple prompts in natural human language as an input, and answer questions, write poems, translations, blog posts, or any other style of human-like text. GPT is one kind of Large Language Model, and a text-based artificial intelligence (AI).

D. Personally Identifiable Information (PII) - is any information pertaining to an individual that can be used to distinguish or trace a person's identity. For more information about PII, including the difference between Public and Protected PII, see Policy 15.1 Personally Identifiable Information. (If a question arises about what is or isn't PII please contact the Information Security Department at ITSecurity@grcc.edu)

E. GRCC Information System - A collection of computing resources that is designed to store student and employee data (e.g. PeopleSoft, Blackboard, and Blackbaud), which is accessible through privileged credentials.

X. Procedures

1. General Acceptable Use

Users are expected to interact with AI technology in a respectful and lawful manner. This includes refraining from using offensive, discriminatory, or harmful language. AI tools shall not be used for any illegal activities, including but not limited to harassment, hate speech, fraud, generation of malware, or any malicious intent.

GRCC employees must adhere to the generative AI vendor's usage policy for any tools that they utilize.

B. FERPA Compliance

Any interaction involving personally identifiable information (PII) must adhere to FERPA regulations and should not disclose sensitive student information.

C. Data Privacy and Security

The Institution is responsible for protecting user data and ensuring that it complies with FERPA, HIPAA, PCI-DSS, and other applicable data protection laws. Users should not share personally identifiable student or employee information, or other sensitive data with AI tools, as it does not guarantee confidentiality.

D. Accuracy

Users should be aware that AI chatbot responses are generated based on patterns in the data it was trained on and may not always be entirely accurate or up-to-date.

E. Ethical Use

An AI chatbot should not be used to generate or distribute content that violates ethical guidelines, intellectual property rights, or copyrights.

F. Reporting Misuse

The Information Security Department must be informed of a real or suspected disclosure of Protected PII data within 12 hours after discovery, e.g. entering student or employee PII into an AI tool.

XI. Enforcement

Anyone found to be in violation of this policy may be subject to disciplinary or other adverse action as deemed appropriate based on the facts and circumstances giving rise to the violation.

XII. Forms

N/A

XIII. Effective Date

April, 2024

XIV. Policy History

Policy created April, 2024

XV. Next Review/Revision Date

April, 2025