ARTIFICIAL INTELLIGENCE POLICY

1. Purpose

Our mission at Quinnipiac is to build the University of the Future with a strategy propelling us from our storied past toward an ambitious and innovative future. This mission requires Quinnipiac to proactively consider how we will incorporate Artificial Intelligence (AI) into what we do. Engaging with this question at various institutional levels is key to maintaining our identity as a forward-thinking institution. As part of this conversation, we must focus on innovation, be mindful of AI's limitations and ethical considerations, and prepare our students and faculty to engage effectively with this revolutionary technology.

The responsible use of AI requires understanding how the technology works, along with its inherent limitations and risks. These limitations and risks must be actively addressed, mitigated, or at the very least, acknowledged. For example, we must remain mindful that private or confidential information entered into an AI tool may become public. We must educate users that AI tools may produce outputs that are inaccurate, misleading, or biased. Additionally, we must ensure that our use of AI complies with our policies on academic integrity as well as all governing local, state, and federal laws.

Quinnipiac University has established two key bodies to guide and innovate AI initiatives: the **AI Steering Committee** and the **AI Innovations Working Group**.

- **AI Steering Committee:** This smaller group includes senior leaders who will involve relevant IT, General Counsel, and policy experts from across the campus as needed.
- **AI Innovations Working Group:** This group comprises thought leaders from across the faculty, staff, and student body, ensuring diverse and innovative areas of expertise and perspectives are included in AI efforts.

2. Scope

This Generative AI policy ("Policy") governs the use of Generative AI tools by staff, faculty, students, and researchers (the "Quinnipiac community") in the performance of their functions for or on behalf of Quinnipiac. Because AI is a rapidly evolving technology, the Steering Committee will continue to monitor developments and updates to this policy. Responses or feedback from the community regarding this policy may be directed to provost@qu.edu

3. Definitions

Generative AI Policy

This Generative AI policy ("Policy") governs the use of Generative AI tools by staff, faculty, students, and researchers (the "Quinnipiac community") in the performance of their functions for or on behalf of Quinnipiac. Because AI is a rapidly evolving technology, the Steering Committee will continue to monitor developments and updates to this policy. Responses or feedback from the community regarding this policy may be directed to provost@qu.edu

Confidential Information

Staff and faculty must take reasonable steps to protect and constrain the transfer of confidential information to unauthorized persons. Confidential information may only be shared within the university on a "need-to-know" basis in accordance with applicable privacy laws and regulations. All relevant procedures related to safeguarding information, including computer use protocols, must be followed. Employees must maintain the confidentiality of proprietary information entrusted to them by the university or its constituents, vendors, or suppliers, except when disclosure is authorized or required by laws or regulations.

Generative AI

Generative AI ("GenAI") includes any machine-based tool designed to consider user questions, prompts, and other inputs (e.g., text, images, videos) to generate a human-like output (e.g., a response to a question, a written document, software code, or a product design). Generative AI includes both standalone offerings, such as Microsoft Copilot, OpenAI ChatGPT, Google Gemini, and Anthropic Claude, and offerings that are embedded in other software, such as Khan Academy's Khanmigo and GitHub's Copilot. In addition to Generative AI chatbots, other tools use similar Large Language Models to rephrase text, such as Grammarly and Microsoft Editor.

FERPA-Protected Information

"FERPA-Protected Information": FERPA protects "education records," which are personally identifiable records of present and past students maintained by QU in its data systems and/or by any QU employee. "Education records" include not only grades, transcripts, papers, exams, and the like, but also non-academic student information database systems, class schedules, financial aid records, financial account records, disability accommodation records, disciplinary records, and even "unofficial" files, photographs, and email messages.

4. Guidance for Use

Quinnipiac expects all Quinnipiac community members to follow these guidelines when using Generative AI tools for teaching and learning, research, and work-related functions:

Using Generative AI tools (including free tools)

In Section 5, you can find information regarding approved Generative AI tools. The available tools change quickly and can be challenging to evaluate. Importantly, some Generative AI tools provide a more secure environment in which to operate. Students and faculty are responsible for learning which Generative AI tool offered by Quinnipiac, if any, is suited to the desired use. The AI Steering Committee will provide prompt answers to the community for any questions on this issue. All Generative AI tools fall under existing policies for Use of Computer and Information Resources (https://catalog.qu.edu/handbooks/undergraduate/university-policies/computer-information-resources/) in the Student Handbook.

Information Types

The following are specific guidelines for different types of information:

- **Use good judgment and use the right Generative AI system for information protected under local, state, or federal privacy law:** Quinnipiac community members must ensure that the information they wish to input into a Generative AI tool does not violate privacy laws like HIPAA, FERPA, COPPA, and state privacy laws.
  - **Non-QU Approved:** It is against university policy to place this protected information in public models under local, state, and federal privacy laws.
  - **QU Approved:** For protected data such as student work, remove personally identifiable information.

- **Do not input information into Generative AI tools if doing so would violate intellectual property rights or general contract terms and conditions:** Quinnipiac community members must be aware of the terms and conditions under which they are using Generative AI tools. AI-generated content may contain copyrighted material. It is incumbent on individual users to ensure that information used with an AI tool is permitted under copyright and patent laws, data protection regulations, and identity theft laws. Vendor licenses govern many of the digital resources available to our community members, and some publishers are asserting that using their content with Generative AI tools is not allowed. Library electronic resources are most affected by these issues. Please contact your library liaisons for assistance. Quinnipiac will continue to advise the institution based on updated guidance from the U.S. Copyright Office.
- **Use good judgment and use the right Generative AI system for information that is confidential or sensitive in nature:** Information such as employee records, financial information, sensitive internal information, legal and compliance data, medical records, and sensitive PII should not be entered in any model.
  - **Non-QU Approved:** No, do not place this information in public models.
  - **QU Approved:** Yes. Make sure to remove all personally identifiable information.

Key Points to Remember about Generative AI Systems

The following guidelines provide an overview of the functional principles behind Generative AI systems, outlining their mechanics and how they generate content.

- **Confirm the accuracy of the output provided by Generative AI tools:** Quinnipiac community members must check the accuracy of information generated by Generative AI tools prior to relying on such information. Generative AI tools should not be relied upon without confirmation of accuracy from additional sources.
- **Check the output of Generative AI tools for bias:** Quinnipiac community members must consider whether the data input into, and the output of, Generative AI tools produces decisions that may result in a disparate impact to individuals based on their protected classifications under applicable law, such as race, gender, ethnicity, national origin, age, sexual orientation, or disability status.
- **Disclose the use of Generative AI tools:** Quinnipiac community members who leverage Generative AI to produce any written materials or other work product should disclose that those materials and that work product are based on or derive from the use of Generative AI.

5. University-Approved Applications, Exemptions, and Exceptions

The university is working to facilitate the use of cutting-edge AI technology while also proactively addressing the potential risks. The Steering Committee, in partnership with the university's information security and information technology leaders, will identify and facilitate access to AI tools that serve its different data needs and publish a list of specific applications that have been vetted by the university and identify the uses for which they are appropriate.

Quinnipiac community members are expected to use any Generative AI tools in accordance with the scope of this policy. Currently, Quinnipiac makes available Microsoft Copilot, Copilot Designer, Adobe Acrobat, Adobe Firefly, AI capabilities in Instructure Canvas LMS, Khan Academy's Khanmigo, and Zoom AI Companion. Visit the QILT site's *AI Tools at QU* page for up-to-date guidance and comparisons of available tools and recommendations.

Quinnipiac designates Zoom AI Companion as the preferred platform for meeting transcription and summaries due to its strong privacy protections and secure data handling. Zoom ensures that meeting content remains within its controlled environment, reducing risks associated with third-party data processing. To maintain data security and consistency, the use of external tools such as Otter.ai, Fireflies.ai, Read.ai, and similar platforms is restricted, as their privacy policies and data management practices may not meet Quinnipiac's standards. Standardizing on Zoom AI Companion helps safeguard user interactions and institutional data.

Quinnipiac will provide AI education and skills training for faculty and students to ensure all community members feel empowered to use the Generative AI tools the university provides access to. Any skills training will also educate the community on the limitations and dangers (e.g., bias, inequity, and misinformation) of AI technology.

6. Generative AI and Academic Integrity

It is our shared responsibility to promote intellectual honesty and scholarly integrity, which could be undermined by the use of AI-generated content being passed off as one's own work. To ensure academic integrity, please refer to the guidance below.

For Students

Absent a clear statement from a course instructor granting permission, the use of Generative AI tools to complete an assignment or exam is prohibited. The unauthorized use of AI shall be treated similarly to the unauthorized use of materials and/or plagiarism in accordance with the Academic Integrity Policy (https://catalog.qu.edu/university-policies/academic-integrity-policy/).

Students are encouraged to speak with their instructors regarding their expectations. Instructors should engage in discussions with their students about appropriate use, both generally and in relation to specific assignments and situations.

For Instructors

Instructors should provide students with a clearly stated policy about the acceptable use of AI tools in each course (e.g., syllabus statements, assignment directions, in-class instructions). AI represents a significant advancement across various domains, industries, and society. As we look toward a university of the future, it is essential to assist students in navigating these changes. Instructors should explain and discuss how AI tools may interfere with or aid students' learning and their achievement of particular goals.

If the use of Generative AI tools is permitted, students should be required to disclose their use of AI and cite material obtained through a Generative AI tool. Additionally, faculty are encouraged to share their AI usage with students. Visit the QILT site's *Artificial Intelligence at QU* page for classroom guidelines, resources, workshops, and consultation.

If an instructor has reasonable suspicion of unauthorized use of AI by a student in the completion of a test or assignment, then per the Academic Integrity Policy (https://catalog.qu.edu/university-policies/academic-integrity-policy/), the instructor must file an academic integrity violation report for the student. Instructors should NOT use AI detection software due to its technical imperfections and potential violations of student

privacy under FERPA. Reports of violations that use these methods cannot be processed.

7. Generative AI in Research, Grants, and Publication

As generative artificial intelligence (GenAI) tools become increasingly integrated into research and grant-writing processes, it is essential to ensure their use aligns with ethical, legal, and compliance standards. Quinnipiac University is committed to maintaining integrity in research by adhering to funder policies, journal guidelines, and institutional best practices regarding GenAI. Faculty, staff, and students must be transparent about their GenAI usage in grant applications, research publications, and data handling to uphold academic rigor and ethical responsibility.

Quinnipiac University follows the policy of the funder in determining the extent to which GenAI tools may be used in the grant application preparation process. This includes compliance with any funder-specific guidelines on GenAI disclosure, authorship, and ethical considerations.

As part of the **internal grant review process**, faculty and staff must indicate whether GenAI tools were used in the preparation of the application, specifying the nature and extent of their use. This information will help determine whether external disclosures—either mandatory or voluntary—should be made to the funder at the time of submission.

For **research publications**, faculty, staff, and students should adhere to the editorial policies of the relevant journals and publishers regarding GenAI usage. Most academic publishers and funding agencies do not recognize GenAI as an author, and its use in drafting or analyzing research findings must be appropriately acknowledged. Any GenAI-generated content that contributes substantively to the research should be transparently disclosed in accordance with journal guidelines.

Additionally, researchers must take precautions when using GenAI tools in research activities. Specifically:

- **Transparency & Disclosure:** Researchers should document and disclose GenAI utilization in their methodologies, ensuring academic integrity and research reproducibility.
- **Data Privacy & Security:** GenAI tools must not be used with sensitive, proprietary, or protected research data, particularly Personally Identifiable Information (PII), health-related data (e.g., HIPAA-covered information), or confidential funding-related materials.
- **Intellectual Property Considerations:** Researchers should be aware that GenAI-generated outputs may not be legally copyrightable and that using GenAI tools for analysis or content creation could have implications for data ownership and authorship attribution.

Faculty and staff are encouraged to visit the Office of Research and Sponsored Projects (ORSP) Policies and Compliance (https://quinnipiacuniversity.sharepoint.com/sites/ORSP/Shared%20Documents/Forms/AllItems.aspx?csf=1&web=1&e=qegSrC&FolderCTID=0x0120008281DCCF3EC5B24E868ED475B4324100&id=%2Fsites%2FORSP%2FShared%20Documents%2FPolicies) page for comprehensive information on research-related policies. This statement also includes the ORSP's policy on the use of AI in proposal preparation.

8. Related University Policies

For more information regarding information security requirements for working with third-party service providers, please refer to **IS POL-04**.

For guidance on the proper disposal of sensitive electronic or hardcopy information, please refer to **IS POL-14**.

For information on security requirements for records retention, please refer to **IS POL-15**.