ADMINISTRATIVE POLICY
GENERATIVE AI ACCEPTABLE USE
This policy pertains to employees.

FVTC is committed to providing a safe and secure computing environment for its employees. This includes our responsible use of generative AI systems such as Open AI ChatGPT, Microsoft Bing, Google Bard, and other AI systems that retrieve uncontrolled external information which can carry risks for the College. The risks arise both from entering FVTC confidential or proprietary information into the AI systems as well as from using output from the AI systems. While generative AI systems can be helpful and provide valuable information, the information retrieved from these unknown or uncontrolled sources may be unverifiable, inaccurate, or biased which creates a risk for FVTC. This Policy outlines the accepted uses all FVTC employees must follow when using such AI systems for FVTC work or when using FVTC's systems and data.

Risks of Generative AI

- **Loss of confidentiality**: Submitting FVTC proprietary or confidential information may result in loss of confidentiality. AI companies may look at your information to assist them with developing their models. ChatGPT, for example, explicitly states this in its terms of service. We have no control over information once it is entered into an AI system. Assume your information will become public.
- **Loss of privacy**: Entering personal information may also lead to privacy issues and possible exposure for FVTC under federal and state privacy laws.
- **Loss of attorney-client privilege**: Entering communications with your attorney into the AI system may result in loss of attorney-client privilege.
- **Loss of intellectual property rights**: Submitting information about an innovation may constitute a public disclosure, which may result in a loss of patent rights in most countries. A generative AI system's output is derived from input from third parties. Any inventions suggested by the generative AI system may include third-party inventors and be owned by those third parties.
- **Copyright infringement**: AI systems receive and output information from third parties, who may own copyrights in that information (software code, images, text). Use of third-party copyrighted materials that are outputted by an AI system may constitute copyright infringement.
- **Reputation damage**: Using inappropriate or offensive content generated by the AI may harm FVTC's reputation.
- **Data security**: Information entered into an AI system may be subject to hacking or a data breach.
- **Data integrity**: Generative AI systems generate responses based on patterns and examples from the language model they create from a database(s) and training data. Sometimes, they output information that has not been changed. Sometimes, they modify the information which might cause it to become inaccurate. And sometimes, they create new information, based on their models, which may be inaccurate or fictional. They do not have the ability to verify the accuracy of their responses, and they often do not inform the user when the information is changed or newly created. Other AI systems that access

uncontrolled databases may also retrieve inaccurate information. As a result, the information provided may be outdated, incorrect, or biased.

- **Legal and regulatory non-compliance**: AI systems as well as their users are subject to an increasing number of laws and regulations. For example, laws in certain countries require a company to provide notice when AI is used for certain tasks or to generate output. Failure by the AI system provider or FVTC to comply with these laws and regulations creates risk for FVTC.
- **Contractual risk**: Entering into contracts with AI system providers that lack favorable terms and conditions or protections for FVTC creates risk for FVTC.

Guidelines for AI System Use

- **Do not use FVTC proprietary or confidential information**: Do not share FVTC proprietary or confidential information with a generative AI system or any other AI system that retrieves uncontrolled external information. Never enter information relating to FVTC's personal information, employee information, student information, customer or supplier information, innovations, proprietary source code, financial data, marketing information, plans, or business data.
- **Verify the output**: Verify the accuracy of information received from an AI system.
- **Modify the output to avoid copyright infringement**: Confirm the information is not copyrighted by a third party. Create your own work by modifying the output.
- **Adhere to the FVTC Code of Conduct**: Use of AI systems should adhere to FVTC's Code of Conduct.
- **Adhere to the FVTC Acceptable Use of Computers Policy**: Employees should adhere to the FVTC Acceptable Use of Computers Policy. Protect your login credentials and ensure that your AI system accounts are not vulnerable to unauthorized individuals.
- **Control third-party use**: Require third parties who do work for FVTC to disclose when their work product includes output generated by AI systems.
- **Explicit Permission**: Do not use AI to genereate images, video, or audio of a person without explicit permission to do so.
- **Review contract terms**: Review contracts with AI system providers to ensure they include representations and warranties that the AI system is in compliance with laws and regulations and allow transparency around the AI model and data. Further, the AI system provider should contractually meet FVTC's performance and delivery **requirements, and assume responsibility for liability for incidents, such as security or privacy breaches.**

Acceptable uses

With these precautions in mind, there are numerous ways to use generative AI tools without risk to FVTC.

Examples of acceptable uses of generative AI include:

- **Syllabus and lesson planning**: Instructors can use generative AI to help outline course syllabi and lesson plans, getting suggestions for learning objectives, teaching strategies, and assessment methods. Course materials that the instructor has authored (such as course notes) may be submitted by the instructor.
- **Correspondence without the use of student or employee information**: Students, faculty, or staff may use fake information (such as an invented name for the recipient of an email

message) to generate drafts of correspondence using AI tools, as long as they are using general queries and do not include institutional data.

- **Professional development and training presentations**: Faculty and staff can use AI to draft materials for potential professional development opportunities, including workshops, conferences, and online courses related to their field.
- **Event planning**: AI can assist in drafting event plans, including suggesting themes, activities, timelines, and checklists.
- **Reviewing publicly accessible content**: AI can help you draft a review, analyze publicly accessible content (for example, proposals, papers and articles) to aid in drafting summaries, or pull together ideas.

Even if you use generative AI tools for activities that do not share personal or institutional data, you should still check the tool's output for accuracy. Since these tools have been known to produce inaccurate content (sometimes called "hallucinations"), verify any factual information generated by an AI tool, and make sure to reference the tool as you would any other source.

Employee Responsibilities

- Employees are responsible for ensuring that they use AI systems in compliance with this policy, FVTC's Code of Conduct, and any other relevant policies or procedures.
- All employees must be aware of their responsibilities for protecting confidential and proprietary information and must take all necessary steps to safeguard the privacy and security of this information when using AI systems.
- If you become aware of any breach of this policy, report the breach to your manager or the FVTC IT Department.
- Employees must cooperate fully with any investigations related to suspected violations or incidents where AI has been applied.

Adopted: 09/20/23
Reviewed: 09/20/23
Revised: