Acceptable Use of AI Tools at Company

Company is committed to maintaining a safe and secure environment for all employees and organizations we partner with through the responsible use of Artificial Intelligence (AI) technology (including any Generative AI, LLMs and/or Machine Learning Tools).

To achieve this, we have implemented an Acceptable Use of AI Tools Policy outlining the principles and guidelines that Company staff must adhere to when using AI capabilities. The policy aims to ensure that all Company employees use AI systems that align with the organization's values, policies, and standards. It applies to everyone at Company who uses AI systems to perform their work.

The policy provides guidelines for the appropriate use of AI tools in the workplace, particularly when handling the organization's and its customers'/test takers/others and partners' personal, sensitive and confidential information. **It outlines the acceptable use policies of Company for AI tools, given their increasing prevalence in day-to-day work**.

The policy aims to ensure that all Company employees use AI tools safely and securely. **The policy requires employees to follow security best practices**, such as evaluating security risks and safeguarding confidential data when using AI tools.

This policy brief and purpose, scope, definitions, and security best practices are detailed below:

Policy Purpose

Our Acceptable Use of AI Tools policy applies to the appropriate and secure use by any employee of Company of any third-party or publicly available AI Tools, especially with personal data, sensitive data and proprietary organization information.

As equity, bias, discrimination and trust issues arise with AI tools we use, we also will rely on this policy to guide our use of *appropriate* AI in our workplace.

Scope

The use of AI tools has revolutionized the way we work. These tools have the potential to automate tasks, improve decision-making, and provide valuable insights into our operations. However, their use also poses new information security and data protection challenges. To mitigate these risks, this policy guides employees on using AI tools ethically, responsibly, safely and securely, especially when sharing potentially sensitive organization information including any personal information, sensitive data and proprietary organization information (copyright and trade secret protected materials. This includes all test taker information and information related to Company tests.

Definitions

AI Systems are any machine-based system that, for any explicit or implicit objective, infers from the inputs the system receives how to generate outputs, including content, decisions, predictions, or recommendations, which can influence physical or virtual environments.

Generative AI is AI that can learn from and mimic large amounts of data to create new content based on inputs or prompts, such as text, images, music, audio, and videos. Generative AI is powered by foundation models (large language AI models) that can multi-task and perform out-of-the-box tasks, such as summarization, Q&A, classification, and more.

Large Language Model (LLM) is a type of language model notable for its ability to achieve general-purpose language understanding and generation. LLMs acquire these abilities by using massive amounts of data to learn billions of parameters during training and consuming large computational resources during their training and operation. LLMs are artificial neural networks pre-trained using self-supervised and semi-supervised learning.

Machine Learning is a branch of artificial intelligence that enables computers to learn from data and perform tasks normally requiring human intelligence. Machine learning algorithms use statistical methods to find patterns in data and make predictions or decisions based on inputs or prompts. Machine learning primarily focuses on making decisions based on historical inputs instead of generating new responses.

Security Best Practices

All employees must follow these security best practices when using AI tools:

- **Meet Company Security Standards:** AI tools used by employees must meet our security and data protection standards.
- **Evaluation of AI tools**: **The evaluation of new AI tools is the responsibility of the Company AI Governance Committee**. This includes reviewing the tool's security features, terms of service, and privacy policy.
- **Protection of confidential data**: Employees must not upload or share any personal, proprietary, or protected data without prior approval from the Company AI Governance Committee. This includes data related to employees, customers, or partners.
- **Access control**: Employees must not give access to AI tools outside the organization without prior approval from the appropriate department or manager and subsequent processes as required to meet security compliance requirements. This includes sharing login credentials or other sensitive information with third parties.
- **Human Review of Output**: Employees must review output for accuracy and relevance before using the results of generative AI. That includes generated natural language and code.

- **Evaluate discrimination, equity, bias, and trust concerns**: As discrimination, equity, bias, and trust issues arise with AI tools, it is the responsibility of staff to bring these issues to their supervisor.
- Further, it is the responsibility of the **AI Governance Committee to evaluate and make recommendations to the** organization on using or refusing to use the AI tool, as appropriate with the policies of Company regarding discrimination, bias, equity, and inclusion.

Acceptable Use of AI Technology

- **The generative AI tool use should be limited to business-related purposes and aligned with Company's standards.**
- **Human review and decision-making is required** before any substantive decisions are made impacting individuals, including but not limited to: stopping any testing, scoring or other test related activities, any accommodations applications review and any accommodations decisions. This must be a meaningful not cursory review by a human.
- **Employees must not engage in any behavior that could be considered discriminatory, harassing, or biased when using generative AI.**
- **Staff must not share any personal, confidential, or sensitive information with AI technology,** including but not limited to passwords, certificates, personally identifiable information (PII), secrets, and tokens.
- **Multi-factor authentication should be in place** across all third-party tools and technologies used for generative AI services.
- **Generative AI systems must comply with all applicable laws and regulations, including data protection and privacy laws.**
- **Company reserves the right to review and monitor all communications shared with generative AI systems**, including but not limited to messages, prompts, attachments, and files.
- **Always obtain explicit consent** before using AI tools to create content that involves another person.
- **Keep confidential information confidential** by not sharing it with unauthorized individuals, including external parties that provide generative AI services.
- **Use generative AI systems responsibly** that do not compromise Company Name's or its data's security or integrity.
- **Comply with all applicable laws and regulations**, including data protection and privacy laws.

- **Document use of Generative AI tools** including the business purpose and the outputs and that employees disclose whether internal and/or external work product was created in whole or part by Generative AI tools.
- **Any outputs must be marked to indicate they were created by Generative AI** as applicable.
- **Independently verify accuracy of Generative AI outputs**. Employees should understand that: Generative AI outputs can be incorrect, out-of-date, biased, or misleading. Employees are responsible for the content they create, regardless

of the assistance of generative AI tools, and employees must independently verify the accuracy of any outputs.

Staff Responsibility When Using AI Technology

- Employees are responsible for ensuring they use AI technology in compliance with this Acceptable Usage Policy and any other relevant organization policies or procedures.
- All employees must be aware of their responsibilities for protecting confidential and sensitive information and take all necessary steps to safeguard the privacy and security of this information when using generative AI technology.
- Managers and supervisors are responsible for ensuring their teams know and comply with this policy. They must also report policy violations to Company's AI Governance Committee.
- Company AI Governance Committee is responsible for agreeing on and documenting an approved list of AI systems to ensure that only authorized applications of these technology capabilities are applied by the organization.

Training and Education

Company provides a collaborative learning environment. Employees will keep updated with the ongoing AI use and adoption changes. Staff should check with their supervisors for available training resources.

Updates and Review

This Acceptable Use of AI Tools Policy will be updated periodically to reflect the dynamic and changing nature of the use of AI tools in our sector. Changes to this policy will be informed by the potential risks and biases that these tools can interject into our work and by changing AI, data privacy, data protection, and/or cybersecurity recommendations.[i]

This is a sample AI/GAI acceptable use policy created for the workshop "*Practical, Legal and Ethical Considerations While Navigating the Roadmap of Generative AI Adoption*" at ATP Innovations in Testing Conference on March 24, 2025, presented by Jamie Armstrong, Donna McPartland, Trushant Mehta and Rachel Watkins Schoenig.