Valley Clean Energy Alliance

Acceptable Use of AI (Artificial Intelligence) Policy

(adopted September 10, 2026)

Contents

Purpose:

This policy establishes guidelines for the responsible, ethical, and secure use of Artificial Intelligence (AI) technologies at Valley Clean Energy (VCE). It is intended to help employees use AI effectively while protecting confidential information, complying with legal requirements, and managing organizational risk.

Risks of using generative AI

- **Inaccuracy**: AI-generated content may be incorrect, outdated, biased, misleading, or entirely fabricated ("hallucinated"). Users must review and verify AI outputs before relying on them for business purposes.

- **Confidentiality:** Information entered into public AI platforms may be stored, disclosed, or used for future model training. Employees should never enter confidential, sensitive, customer, employee, or other non-public information into unauthorized AI systems.

- **Usage restrictions:** AI tools may have contractual, legal, or operational limitations that restrict how they can be used. Employees are responsible for complying with the terms and conditions of approved AI platforms.

- **Litigation:** Because generative AI is relatively new, the ethical, legal, and business landscape regarding its use, commercialization, and regulation remains unsettled and is evolving. Generative AI has already resulted in high-profile litigation against operators of several generative AI platforms, and this litigation could extend to users of generative AI platforms in the future.

1. Scope

This policy applies to all employees, contractors, and third parties who use AI technologies within the VCE's infrastructure or on behalf of VCE. VCE's CFO and VCE's outsourced IT support services provider will administer this policy.

2. Definitions

- **AI (Artificial Intelligence):** Any software, system, or tool that uses algorithms to simulate human intelligence processes, including learning, reasoning, and problem-solving.
- **Generative AI:** Any AI system capable of generating text, images, audio, or other content, including but not limited to models such as GPT, DALL-E, and other similar technologies.
- **Sensitive Data:** Any data that could potentially be used to identify an individual or is protected under data protection laws, including personal, financial, and health information.

3. General Principles

- **Ethical Use:** All AI applications must be used in a manner that aligns with the VCE's ethical standards, promoting fairness, transparency, and accountability.
- **Compliance:** All use of AI technologies must comply with applicable laws, regulations, and industry standards, including data protection and privacy laws.
- **Security:** AI systems must be implemented with appropriate security measures to protect against unauthorized access, data breaches, and other security risks.

4. Data Privacy and Security

- **Data Collection and Use:** Data used by generative AI systems must be carefully controlled. Sensitive Data, especially non-public customer information, should not be input into generative AI systems without explicit authorization and clear business need.
- **Prohibition of Non-Public Data Use:** Non-public Sensitive Data, including names and contact details, must not be included in training datasets or used in generating content without proper controls and permissions.

- **Data Access:** Access to data used by AI systems must be restricted to authorized personnel only. Proper access controls and logging mechanisms must be in place.
- **Data Storage and Retention:** Data should be stored securely and only retained for as long as necessary for the AI system's purpose.

5. Transparency and Accountability

- **Disclosure:** When interacting with AI systems, users should be informed that they are interacting with an AI system, and the purpose of the interaction should be clear.
- **Decision-Making:** AI systems that assist in decision-making processes should provide explanations for their recommendations or actions, where feasible.
- **Responsibility:** Employees must take responsibility for the proper functioning and ethical use of AI systems. Employees are responsible for ensuring that the use of generative AI systems complies with this policy and must report any concerns or issues promptly. Any concerns or issues should be reported to the appropriate manager.

6. Prohibited Uses

- **Discrimination:** AI systems must not be used to discriminate against individuals or groups based on race, gender, age, disability, religion, sexual orientation, or any other protected characteristic.
- **Surveillance:** AI technologies must not be used for unauthorized surveillance of employees, clients, or other individuals.
- **Manipulation and Deception:** AI systems should not be used to deceive, manipulate, or exploit individuals.
- **Unauthorized Use of Sensitive Data:** It is strictly prohibited to use generative AI systems to process, generate, or disseminate non-public client or VCE information without explicit permission.

7. Employee Training and Awareness

- Employees must receive training on the ethical and secure use of AI technologies and be aware of the potential risks and benefits associated with AI applications.

8. Monitoring and Review

- **Monitoring:** The use of AI systems will be monitored to ensure compliance with this policy. Any unauthorized use or security breaches must be reported immediately to the appropriate manager.
- **Review and Update:** This policy will be reviewed regularly and updated as necessary to reflect changes in technology, laws, and VCE practices.