Sample AI Usage Guidelines

OVERVIEW

These guidelines outline the responsible use of artificial intelligence (AI) tools, particularly generative AI, within our organization. They are designed to ensure ethical, effective, and secure use of AI technologies in our operations. While we embrace innovation and experimentation, we must balance that with information integrity, privacy, transparency, and accuracy.

Given the rapidly evolving nature of AI, these guidelines serve as a working framework and may be revised as we learn more about AI's benefits and challenges.

1. Employee Responsibility and Accountability

- Employees using AI tools remain fully responsible for their work output.
- AI-generated content must be thoroughly reviewed and edited by employees before publication.
- The use of AI does not absolve employees of their professional responsibilities or accountability for the final work product.
- If errors or misrepresentations occur due to AI use, it is the staff member's responsibility to correct them promptly.

2. Human Oversight and Judgment

- Human oversight is essential in all AI-assisted processes.
- Employees must exercise critical thinking and judgment when using AI-generated content.
- Final decisions and approvals must always be made by authorized human employees, not AI systems.

3. Privacy and Security

- Employees are to always protect the privacy and security of our stakeholders and sensitive association information.
- Do not input confidential, proprietary, or personal information[i] into AI tools without proper authorization and safeguards.
- AI tools shall be vetted by the employer prior to use to ensure they adhere to best practices in data privacy and security.

4. Ethical Use and Respect for Intellectual Property (IP)

- Use AI tools in a manner consistent with [EMPLOYER]'s values and ethical standards.
- The employer shall actively monitor AI tools for biases, inaccuracies, and unintended outcomes which may be learned through ongoing diligence and reading reviews of the AI tools.
- Do not knowingly use AI tools that generate content infringing on the rights of others.
- Review all AI-generated content to ensure it does not violate copyright laws or plagiarize other works.

5. Transparency and Disclosure

- If AI-generated content constitutes a significant portion of a document, image, or decision-making process, it should be disclosed whether in writing or verbally communicated to a supervisor. *[Sample language: This document contains AI-generated content.]*.

Review and Compliance

- These guidelines will be reviewed and updated periodically to reflect changes in AI technology and regulations.
- Non-compliance with these guidelines may result in disciplinary action.
- All staff members are expected to follow these guidelines and maintain the highest standards of accuracy, privacy, and accountability.

By following these guidelines, we aim to harness the benefits of AI while maintaining the high standards of professionalism and integrity expected in our industry. As AI technology evolves, the employer will stay informed about the latest developments and best practices, and we will continue to refine these guidelines to address new challenges and opportunities.

DISCLAIMER ON AI GUIDELINES

The sample AI policy provided by the California Hotel & Lodging Association (CHLA) is intended solely as general information to help CHLA members develop their own guidelines for the use of AI within their businesses. The adoption of this sample policy is at the discretion of each member and should be adapted to fit the unique needs and circumstances of each business.

CHLA makes no representation or warranty regarding the applicability, sufficiency, or compliance of this sample policy with current or future laws. Members are strongly encouraged to consult with legal professionals to ensure any adopted AI policy aligns with their specific operational requirements and complies with all applicable laws and regulations.

By making these guidelines available, CHLA does not assume any responsibility or liability for the actions taken by its members in adopting or implementing the policy. This document is provided "as-is," and members adopt or adapt this policy at their own risk.

Employees and others covered by the policy should know what exactly constitutes "personal information."

California Civil Code Section 1798.140(v) states that (v) (1) "Personal information" means information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. Personal information includes, but is not limited to, the following if it identifies, relates to, describes, is reasonably capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household:

(A) Identifiers such as a real name, alias, postal address, unique personal identifier, online identifier, Internet Protocol address, email address, account name, social security number, driver's license number, passport number, or other similar identifiers.
(B) Any personal information described in subdivision (e) of Section 1798.80.

> [i.e., (e) "Personal information" means any information that identifies, relates to, describes, or is capable of being associated with, a particular individual, including, but not limited to, his or her name, signature, social security number, physical characteristics or description, address, telephone number, passport number, driver's license or state identification card number, insurance policy number, education, employment, employment history, bank account number, credit card number, debit card number, or any other financial information, medical information, or health insurance information. "Personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.]

(C) Characteristics of protected classifications under California or federal law.
(D) Commercial information, including records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.
(E) Biometric information.
(F) Internet or other electronic network activity information, including, but not limited to, browsing history, search history, and information regarding a consumer's interaction with an internet website application, or advertisement.
(G) Geolocation data.
(H) Audio, electronic, visual, thermal, olfactory, or similar information.
(I) Professional or employment-related information.
(J) Education information, defined as information that is not publicly available personally identifiable information as defined in the Family Educational Rights and Privacy Act (20 U.S.C. Sec. 1232g; 34 C.F.R. Part 99).
(K) Inferences drawn from any of the information identified in this subdivision to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.
(L) Sensitive personal information.

Sensitive personal information is a specific subset of personal information that describes certain types of personal information that are more sensitive in nature. Civil Code Section 1798.140(ae) defines "sensitive personal information" as follows:

(ae) "Sensitive personal information" means:

(1) Personal information that reveals:
(A) A consumer's social security, driver's license, state identification card, or passport number.
(B) A consumer's account log-in, financial account, debit card, or credit card number in combination with any required security or access code, password, or credentials allowing access to an account.
(C) A consumer's precise geolocation.
(D) A consumer's racial or ethnic origin, citizenship or immigration status, religious or philosophical beliefs, or union membership.
(E) The contents of a consumer's mail, email, and text messages unless the business is the intended recipient of the communication.
(F) A consumer's genetic data.

(2) (A) The processing of biometric information for the purpose of uniquely identifying a consumer.
(B) Personal information collected and analyzed concerning a consumer's health.
(C) Personal information collected and analyzed concerning a consumer's sex life or sexual orientation.

(3) Sensitive personal information that is "publicly available" pursuant to paragraph (2) of subdivision (v) shall not be considered sensitive personal information or personal information.