Artificial Intelligence (AI) and Large Language Model (LLM) Usage Policy

Purpose

The purpose of the Legislative Council Agencies (Council) AI (Artificial Intelligence) and LLM (Large Language Models) Usage Policy is to establish the acceptable use of AI and LLM technologies within the operations of the Legislative Council Agencies. Council Agencies permit the use of AI tools in the workplace. Users must exercise due diligence and critical thinking when using AI-generated outputs, as AI systems may produce biased, inaccurate, or inappropriate results and save and utilize information inputs.

Audience

The Artificial Intelligence (AI) and Large Language Model (LLM) Usage Policy applies to any individual, entity, or process that interacts with any Council Information Resource.

Policy

1. Usage of any Council information resource is governed by the Acceptable Use Policy.

2. To minimize the risk of intentional or unintentional misuse that may result in harm to individuals, the organization, or our clients, using sensitive, confidential, or proprietary information related to Council Agencies or our clients in an AI tool is strictly prohibited. Do not disclose or share any sensitive data during interactions with AI or LLM platforms.

3. Ensure that AI and LLM platform interactions occur over secure channels and on systems with appropriate security measures to protect customer information from unauthorized access or disclosure.

4. Usage must adhere to all relevant laws, regulations, and industry standards, such as data protection and privacy regulations (e.g., GDPR, CCPA) and financial industry guidelines (e.g., PCI DSS).

5. AI and LLM platform usage and/or integration into existing tools will require review and approval by the Legislative Service Bureau Information Services Division Management. All vendors must be reviewed in accordance with Council's Vendor Management Policy and an impact analysis must be completed before the committee will consider usage.

6. Report any data breaches or incidents involving AI systems to the Information Services team immediately.

7. Avoid storing or retaining chat logs longer than necessary. Delete or anonymize customer interactions as per data retention policies.

8. Exercise caution when relying on AI and LLM responses for critical decisions or actions. Use these models as a support tool rather than a sole source of information.

9. Information Services will conduct periodic audits and assessments of AI and LLM usage, including access controls, data handling practices, and compliance with policies and regulations.

10. Information Services will implement monitoring mechanisms to track and record interactions with AI and LLM platforms for security, compliance, and quality assurance purposes.

11. Information Services, in conjunction with Council management, will educate employees on the appropriate usage of AI and LLM platforms, including data privacy, security best practices, and the importance of adhering to the established policies.

12. Regularly review and update the policy as needed to address emerging risks, changes in regulations, or advancements in technology.

Definitions

See Appendix A: Definitions

Enforcement

Personnel found to have violated this policy may be subject to disciplinary action, up to and including termination of employment, and related civil or criminal penalties.

Any vendor, consultant, or contractor found to have violated this policy may be subject to sanctions up to and including removal of access rights, termination of contract(s), and related civil or criminal penalties.

Version History

Version	Modified Date	Authored by	Reason/Comments
1.0.0	November 2024	Alan Wright	Document Origination
1.0.1	March 2025	Alan Wright	Including comments from Shanda Greco
1.0.2	March 2024	Alan Wright	Including comments from Jennifer Bucienski
1.0.3	March 2024	Alan Wright	Incorporated comments from Jennifer Dettloff