Acceptable Use of Artificial Intelligence (AI)

Policy Statement: Artificial Intelligence (AI) technologies stand to transform employees' means and methods for synthesizing content, both written and visual. However, AI technologies are merely tools. A responsible approach to the adoption and use of such tools must include provisions for mitigating the risks associated with accuracy, completeness, bias, data privacy and cybersecurity in the use of AI. This policy establishes guidelines for the acceptable use of AI technologies but may be supplemented by additional governance mechanisms such as product standards, employee training, or practical guidance. Employees should be mindful that there is a difference between establishing parameters for the acceptable use of AI technologies as an organization, and determining that the use of AI technologies is appropriate in a given department or division for a given employee to perform a given task.

Version History: Version 1.0

Effective Date: 10/15/2025

Revision Date: N/A

Reviewed Date: N/A

Policy Number: CIO - 22

Authority: The Chief Administrative Officer has authorized the Office of the Chief Information Officer to establish and enforce policies governing the use of technology to align with industry standards, best practices, or other operational requirements. Nothing herein displaces departmental and divisional authority to determine appropriate means and methods for its employees to perform their assigned duties.

1. Purpose

This policy sets clear rules for how AI tools may, and may not, be used in the course of business. Its purpose is to ensure AI is used to improve productivity and decision-making without exposing LFUCG to unmanaged legal, privacy, or security risks. It applies to all AI use that interacts with LFUCG's data, systems, or workflows, whether through approved platforms or public tools. Employees should utilize AI technology as a means, and not as an end. All work performed for LFUCG remains the responsibility of employee users, and no acceptable use of AI contemplated herein is intended to substitute for or displace an employee's responsibility to consult with

appropriate LFUCG experts in the use of AI technologies, including but not limited to LFUCG's IT, information security, and legal teams.

2. Scope

This policy applies to anyone using AI tools in connection with LFUCG's work. This includes employees, contractors, consultants, interns and third-party vendors. It covers AI usage on any device, network or system where the activity involves LFUCG data, systems or business processes.

If you are using AI in a way that touches LFUCG business, whether the AI tool is officially provided by LFUCG or accessed independently through personal accounts, this policy applies.

3. Definitions

Artificial Intelligence (AI): Machine learning and related technologies that use data to train statistical models for the purpose of enabling computer systems to perform tasks normally associated with human intelligence or perception.[1]

Agentic AI: AI systems capable of taking action or making decisions with limited or no human involvement, such as sending messages, executing code or performing tasks on behalf of users.

Generative AI: An artificial intelligence system that is capable of producing and used to produce synthetic content, including audio, images, text, and videos[2] based on its manufacturer's training and its consumers' activities.

Authorized AI tools: AI tools that have been reviewed and approved by LFUCG's legal, privacy and information security teams for specified use cases. These tools are provisioned through official channels and configured for enterprise use.

Public AI tools: AI platforms available to the general public that have not been formally approved by LFUCG. This includes free, browser-based, subscription, or trial versions of tools like ChatGPT, Google Gemini, Claude, etc. that are acquired through personal means (e.g. a personal email address).

Retention Period: The timeframe in which an AI tool will retain prompt inputs and uploaded content.

Sensitive data: Any data that is confidential, regulated, or proprietary in nature, including customer records, HR data, legal documents, health records, credentials,

[1] KRS 42.722(1).
[2] KRS 42.722(9).

payment system information, security-related information, or personally identifiable information (PII) as defined in KRS 61.931(6)(a-f).

4. Acceptable Use

Authorized AI tools may be acceptable for work-related tasks if they have been formally approved by LFUCG's legal, privacy and information security teams. While authorized AI tools may be acceptable for work-related tasks as set forth herein, LFUCG departments and divisions shall determine whether the use of AI tools by their employees for the performance of their job duties is appropriate. Tools must be provisioned through official channels; configured for enterprise use; and include appropriate controls for access, logging and data handling ("configured for enterprise use" contemplates that the documents governing the terms and conditions of use have been reviewed and approved by the Department of Law).

Acceptable uses include:

- Drafting and content support: AI tools may be used to assist with the creation of internal communications, documentation, presentations or templates, provided the content is reviewed by the human user and approved pursuant to applicable departmental or divisional policies or procedures before distribution.
- Process and workflow efficiency: AI tools may assist with internal tasks such as summarizing information, formatting documents, organizing notes or prepopulating forms. All AI assisted content should be treated as a first draft and subjected to fact checking, review, and approval pursuant to applicable governmental, departmental, or divisional policies or procedures.
- Data review and research support: Users may employ AI tools to summarize nonsensitive documents, extract patterns from unclassified data, or assist with public or internal research. All outputs used in decision-making must be checked for accuracy and completeness and independently verified and approved pursuant to applicable governmental, departmental, or divisional policies or procedures.
- Training and enablement: AI tools may support employee learning or onboarding by assisting in the creation of educational materials, FAQs, or simulated scenarios using approved datasets and inputs. AI assisted content must be checked for accuracy, completeness, and bias and approved pursuant to applicable governmental, departmental, or divisional policies or procedures.

Use conditions:

- Human accountability: AI-generated content must be reviewed by the user for accuracy, completeness, appropriateness, bias, and compliance. Final responsibility for AI-generated content rests with the user, subject to applicable governmental, departmental, or divisional policies or procedures, not the tool.
- Data inputs: Only data that is considered appropriate for consumption by the general public at the time of use shall be uploaded, used to prompt, or otherwise input to AI tools. Users must not input sensitive data, as defined above, or customer-specific data into any AI tool, regardless of purpose.
- External communication: AI-generated output intended for clients, regulators or external audiences must be formally reviewed and approved pursuant to applicable governmental, departmental, or divisional policies or procedures prior to release. The reviewer will be identified in the external communication.
- Disclosure requirements: Users must comply with internal policies regarding labeling or disclosing, in a clear and conspicuous manner, AI-assisted content where transparency is expected or legally required.

5. Prohibited Use

The following uses of AI tools are strictly prohibited, regardless of whether the tool is public, personal or LFUCG-approved:

- Use of public or unapproved AI tools: Only AI tools that have been approved for use by the Department of Information Technology, in accordance with this policy, shall be used for work-related activities. Use of publicly accessible AI tools, whether free, browser-based, trial version, or via subscription are not permitted for any work-related activity, regardless of data sensitivity or perceived risk. These tools are considered noncompliant with LFUCG privacy and security standards.
- Inputting or handling sensitive data: Users must not input sensitive data, as defined above, or customer-specific data into any AI tool, regardless of purpose.
- Autonomous actions or automation without oversight: Agentic AI or other AI tools may not send messages, make decisions, approve transactions, execute scripts or perform tasks on behalf of LFUCG without direct human initiation, oversight, and review, pursuant to applicable governmental, departmental, or divisional policies or procedures. Automated use must be formally reviewed and approved by LFUCG information security and IT teams.
- Impersonation or misrepresentation: AI tools may not be used to mimic or impersonate employees, customers, vendors or regulators in any format,

including written, visual, audio or synthetic media. Creating or distributing deepfakes, fake voices or AI-generated likenesses, avatars, or images tied to LFUCG is strictly forbidden.

- Unsafe, noncompliant or misleading output: Users must not use AI tools to generate content that is inaccurate, incomplete, biased, deceptive, defamatory, discriminatory, or in violation of legal, regulatory or ethical standards. No AI-generated content may be relied on in ways that could cause harm to LFUCG, its customers/residents or third parties.
- Bypassing corporate controls: Users must not use personal devices, incognito browsers, proxies, VPNs or alternate tools to circumvent LFUCG policies or restrictions on AI tool usage. Attempting to enable experimental features, plug-ins or agentic behavior in AI tools without approval is a violation of this policy.

6. Responsibilities of Users

All individuals using AI tools for work are expected to understand and adhere to their responsibilities for ensuring safe, compliant and effective use. This includes using only tools that have been formally approved by LFUCG and provisioned through official channels. Users must check AI-generated content for accuracy and completeness and independently verify the AI-generated content before relying on it or sharing it with others, ensuring outputs are accurate, appropriate and aligned with business needs.

Where transparency is required, such as in communications with clients, residents, regulators or external stakeholders, users must clearly disclose when AI has assisted in content creation, in line with internal policy or legal obligations. Prior to using AI tools, all users should be trained on this policy and should remain attentive to evolving policies, tool capabilities and approved use cases.

If any AI tool behaves unexpectedly, produces inappropriate content or is suspected of misusing data, users must report the issue immediately through the IT Helpdesk. Failure to meet these expectations may result in access restrictions, disciplinary action, up to and including charges for dismissal or other consequences, depending on the severity and impact of the violation.

7. Data Handling and Privacy

AI tools, whether public or approved, must be treated similarly to other data processing systems. Any input or output involving these tools can carry privacy, confidentiality and compliance risks. Users must never enter sensitive data, as defined above, into any AI tool. Public AI tools are never authorized to process sensitive data or regulated information under any circumstance.

Existing data protection policies and procedures still apply. Users may not attempt to bypass these policies by altering, deidentifying, or masking sensitive data for AI input unless they have formal approval to do so. Even redacted content can carry risk and should be handled with caution.

Outputs generated by AI tools must be reviewed carefully, especially if they summarize internal documents, describe proprietary workflows or may contain inferred confidential details. Outputs should not be shared, stored or reused in ways that could expose sensitive data.

Finally, users should assume any prompt or response sent to a public AI tool may be retained, reused or analyzed by the tool's provider. Even where AI tools have been vetted and configured for enterprise use, users are responsible for understanding the provider's data retention policies and ensuring they align with LFUCG's or other applicable data handling requirements.

8. Monitoring and Logging

AI activity conducted through LFUCG-managed tools, accounts, devices or networks may be monitored and logged to ensure compliance, investigate potential misuse, and meet legal or regulatory obligations.

This monitoring may include the collection of prompts, outputs, user identifiers, access times and metadata related to the use of AI tools. Interactions involving sensitive or regulated data shall be subject to additional scrutiny. Users should operate with the understanding that all AI-related activity is attributable and auditable.

Attempts to bypass monitoring, including use of personal accounts, private browsing modes, unauthorized devices or unapproved tools are considered violations of this policy and may result in disciplinary action up to and including charges for dismissal. All monitoring data is handled in accordance with LFUCG's retention, access control and incident response procedures and is only accessible by authorized personnel.

9. Violations and Enforcement

Failure to comply with this policy, whether through intentional misuse, negligence or unauthorized experimentation, shall result in disciplinary action, including revocation of access to AI tools and formal HR action up to and including charges for dismissal or termination of contract. Failure to comply with this policy may constitute inefficiency, insubordination, and/or misconduct in violation of KRS Chapter 67A and Chapters 21, 22, and 23 of the LFUCG Code of Ordinances and may otherwise violate the LFUCG Uniform Disciplinary Code, and employees are hereby advised that they are subject to discipline regarding same.

In cases involving legal, regulatory or third-party impact, violations may also lead to financial penalties, legal proceedings or mandatory external reporting.

All suspected violations will be reviewed by the appropriate internal teams, including information security, legal, HR and/or compliance teams, and users are expected to cooperate fully with any investigations. Where required, incidents involving AI misuse may be escalated to external authorities or regulators in accordance with applicable laws and contractual obligations.

10. Exceptions

Exceptions to this policy may be requested via email to the IT Helpdesk. An exception may be granted upon verification of need by the Office of the CIO but will be subject to routine review and reauthorization. No user should act on their request for an exception until expressly notified by the Office of the CIO that such request has been granted.

This policy is approved by the CIO.

Signature:  **Date:** 10/15/2025