

AI Legal & Compliance Policy

Brix Holdings

1. Purpose and Scope

This policy sets out how artificial intelligence (AI) tools may be used at Brix Holdings (the “Company”). It explains what is permitted, what is prohibited, and how employees can use AI responsibly, securely, ethically, and in compliance with applicable law.

The goal is to enable employees to benefit from AI for efficiency and creativity while minimizing legal, security, privacy, ethical, and reputational risk to the Company, its franchisees, and its customers.

1.1 Who this policy applies to

This policy applies to all employees, officers, contractors, temporary staff, and third-party vendors who use AI tools in the course of work performed with or for the Company. It applies regardless of whether the AI tool is publicly available, licensed by the Company, or embedded within another approved platform.

1.2 What this policy covers

This policy covers all AI tools and technologies used for Company purposes, including but not limited to public or enterprise large language models, image and content generators, automation platforms, analytics assistants, and internal AI applications. Where the Company has signed specific terms for an AI tool (such as Keboola’s Kai AI Assistant in Annex A), those terms apply in addition to this policy.

2. Definitions

The following definitions apply throughout this policy:

- **Artificial Intelligence (AI):** Software that performs tasks normally associated with human intelligence, such as analyzing data, recognizing patterns, making decisions, or generating content.
- **Generative AI:** A type of AI that produces new content — such as text, images, audio, or code (for example, Claude, ChatGPT, Microsoft Copilot, GitHub Copilot, or Midjourney).
- **Machine Learning (ML):** Algorithms that improve through exposure to data and experience, often operating behind the scenes within an AI tool.
- **Large Language Model (LLM):** A generative AI model trained on large volumes of text to understand and produce human-like language.

- **Public / Consumer AI Tool:** An AI service available to the general public, typically free or self-service, where inputs may be retained or used to improve the provider's models unless an enterprise agreement states otherwise.
- **Enterprise AI Tool:** An AI service the Company has licensed and vetted under contractual terms that govern security, data handling, and confidentiality.
- **AI Output:** Any content, recommendation, analysis, or decision produced by an AI tool.
- **Sensitive Information:** Information that could cause harm if disclosed, including customer data, financial and payment records, personal employee information, legal documents, trade secrets, and other confidential or proprietary Company data.
- **Sub-processor:** A third party engaged by an AI vendor to process data on its behalf in delivering the service.

3. Roles and Responsibilities

Responsible AI use is a shared responsibility. The following roles support governance of this policy:

Role	Key Responsibilities
Executive Leadership	Endorse the policy, allocate resources, and set the tone for responsible AI use.
IT & Security	Vet and approve AI tools, maintain the approved-tools list, review security and data-handling terms, and monitor for misuse.
Legal & Compliance	Confirm regulatory alignment, review vendor terms and data processing agreements, and advise on incidents.
Managers & Team Leads	Ensure their teams understand and follow this policy, and approve new use cases where required.
All Users	Use AI within the rules below, verify outputs, protect sensitive information, and report concerns promptly.

4. Authorized Use

Employees are encouraged to explore AI tools to work more efficiently and creatively — within the limits set by this policy.

4.1 Acceptable uses

- Summarizing meeting notes, internal reports, or long documents.
- Drafting first versions of internal communications and documentation.
- Automating repetitive tasks such as formatting, tagging, or data clean-up.
- Brainstorming, research support, and generating ideas for later human review.

- Analyzing Company data within approved enterprise tools that are covered by appropriate security terms.

When in doubt: If you are unsure whether a use is acceptable — especially a new purpose or a new tool — check with your team lead or IT before proceeding.

5. Prohibited Uses

The following uses are not permitted. Items 5.1–5.3 below consolidate the restrictions from across this policy so they appear in one place.

5.1 Outputs and judgment

- Generating client- or customer-facing content without human review and approval.
- Using AI to replace human judgment in decision-making, particularly in the high-oversight areas listed in Section 9.

5.2 Data and infrastructure

- Uploading, processing, or training tools on sensitive or proprietary data in violation of Section 6.
- Developing or deploying unapproved AI applications within the Company's infrastructure.

5.3 Integrity and the law

- Creating deepfakes, impersonating individuals, or fabricating information.
- Using AI tools for personal gain during work hours or on Company systems.
- Using AI to circumvent laws, regulations, or compliance requirements.
- Producing content that is biased, discriminatory, offensive, or misleading, or that infringes intellectual property (see Section 7).

Enforcement

Violations of this policy may result in disciplinary action up to and including termination of employment, particularly for serious or repeated offenses. Violations involving unlawful conduct may also be referred to the appropriate authorities.

6. Data Privacy and Security

Protecting Company, customer, and employee data is paramount when using AI.

6.1 Sensitive information

Public or consumer AI tools must never be used to process Sensitive Information. This includes, but is not limited to:

- Customer data.
- Financial and payment records.
- Personal employee information.

- Legal documents and contracts.
- Trade secrets and other confidential or proprietary information.

6.2 Tool vetting and data-protection alignment

All AI tools must be used in line with the Company's existing data protection and information security policies. Enterprise AI tools must be vetted and approved by IT for security compliance before adoption and must be governed by appropriate contractual terms (for example, a Data Processing Agreement).

6.3 Approved-tool data commitments

Approved enterprise tools are selected in part because their terms restrict how inputs are handled. For example, under the terms in Annex A, Keboola does not use Kai AI Assistant inputs to train, re-train, or fine-tune its own models or any third-party models, and the authorized sub-processors are disclosed. Even so, users must still avoid placing Sensitive Information into any tool unless its approved terms and the relevant data-protection policy expressly permit it.

7. Ethical and Responsible Use

AI use at Brix Holdings should reflect the Company's values. This means:

- Avoiding content that could be biased, discriminatory, or offensive.
- Not using AI-generated content to mislead, deceive, or manipulate others.
- Respecting copyright and intellectual property — third-party content must not be copied or adapted without permission, and AI outputs must not be presented in ways that infringe others' rights.

When in doubt, assume a human touch is still needed.

8. Transparency and Disclosure

People affected by AI use are entitled to appropriate transparency.

- Where users or customers interact with an AI system, they should be clearly informed that they are interacting with AI, not a human.
- Necessary information and notices about how personal data is processed must be provided to affected individuals, including any disclosures about international data transfers required by an approved tool's terms (see Annex A).
- AI-generated content used externally should be reviewed and, where appropriate, disclosed in line with Company communications standards.

9. Human Oversight and Accountability

AI tools assist people; they do not replace human accountability. AI outputs are provided on an "as-is" basis and may be inaccurate, incomplete, or contain errors. Users are responsible for verifying all outputs before relying on them or putting them to further use.

A human staff member must always review and approve any AI-generated output used in the following high-oversight areas:

- Recruitment and hiring.
- Employee evaluation and performance management.
- Customer interactions.
- Strategic or financial decisions.
- Any legally significant or regulated decision.

10. Approved AI Tools and Vendor Management

To balance innovation with safety, the Company maintains a list of approved AI tools. New tools must be requested through, and vetted by, IT before use for Company purposes.

10.1 Approval criteria

- Documented security and data-handling practices, reviewed by IT and, where applicable, Legal.
- Contractual terms governing confidentiality, data use, and sub-processors (for example, a Data Processing Agreement).
- A clear statement of whether inputs are used to train the provider's models.
- Disclosure of the tool's status (for example, general availability vs. "beta").

10.2 Currently approved enterprise tools

Tool	Primary Use	Status & Notes
Keboola — Kai AI Assistant	Data source with connection to POS, FranConnect, Ovation, Lunchbox, Online Reviews	Full terms in Annex A.
Claude.AI	Drafting, summarizing, research, analytics	Current templates and organization skills used for reporting & analytics only

Tools not on the approved list must not be used for Company work involving non-public information until IT has been reviewed and approved them. To request a new tool, contact it@brixholdings.com.

11. Risk Management and Incident Reporting

If you notice anything amiss — such as an incorrect or harmful output, signs of bias, a data exposure, or any other security concern — report it promptly so it can be addressed and tracked.

1. **Report it:** Contact it@brixholdings.com.
2. **Document it:** Record what happened, the tool involved, and any data affected, as part of the Company's regular risk-tracking process.
3. **Contain it:** Stop using the tool for the affected task until you receive guidance, and do not attempt to "fix" a suspected data exposure on your own.

12. Legal and Regulatory Compliance

AI use must comply with all applicable laws and regulations. Depending on the activity and jurisdiction, these may include:

- Data protection and privacy laws (for example, GDPR and U.S. state privacy laws such as the CCPA/CPRA), where applicable.
- Intellectual property and copyright law.
- Employment and anti-discrimination law, particularly where AI supports hiring or evaluation.
- Consumer-protection and advertising rules for customer-facing content.
- Emerging AI-specific regulation (for example, the EU AI Act) as it becomes applicable to the Company.

AI must never be used to circumvent a legal or compliance obligation. Where an approved tool's contractual terms conflict with this policy, the controlling terms are as set out in Section 15.4 and the relevant annex.

13. Training and Awareness

The Company will provide training to help employees use AI safely and ethically.

- New employees must complete a basic AI training module during onboarding.
- Additional resources and updates will be shared through [platform: LMS, intranet, etc.].

If you have questions or concerns, contact it@brixholdings.com.

14. Compliance and Enforcement

Compliance with this policy is mandatory. Failure to comply may result in disciplinary action up to and including termination of employment, particularly for serious violations or repeat offenses. Where conduct may be unlawful, the Company may take additional steps, including notifying relevant authorities. Contractors and vendors who breach this policy may have their engagement terminated.

15. Policy Review and Updates

This policy will be reviewed and updated at least every 12 months, or sooner if AI capabilities or associated risks shift significantly. Employees are encouraged to share feedback so the policy

stays accurate, useful, and up to date. Material changes will be communicated through standard internal channels.

This policy does not replace the specific terms agreed with individual AI vendors. Where a vendor updates its terms (for example, the Keboola terms in Annex A may be updated on notice), the updated vendor terms govern that tool, and this policy will be revised at the next review to remain consistent.

Annex A — Keboola Kai AI Assistant Terms

The following terms apply to the Keboola Kai AI Assistant, an approved enterprise tool referenced in Section 10. They are reproduced here for reference and form part of the contractual terms governing that tool.

By requesting, instructing, or otherwise authorizing Keboola to activate the Kai AI Assistant features within your environment, or by accessing or using such features, you (“**Client**”) agree to these AI Assistant Terms (“**Terms**”). These Terms supplement the agreement (“**Agreement**”) for Keboola services between Keboola and Client, including the applicable Master Subscription Agreement.

A.1 Security and Data Protection

A.1.1 No Training. Keboola does not use Kai AI Assistant inputs to train, re-train, or fine-tune its own models or any third-party AI models.

A.1.2 Sub-processors. Client authorizes the use of Google LLC (Vertex AI service for LLM inference) and LangChain Inc. (LangSmith service for observability) as sub-processors.

A.2 Service Nature

A.2.1 Output Accuracy. AI-generated outputs are provided on an “as-is” basis and may be inaccurate, incomplete, or contain errors. Client is solely responsible for verifying all outputs before any reliance or further use.

A.2.2 Beta Status. The Keboola AI Assistant service is “beta.” It is provided “as is” and “as available,” and Client uses it at its own risk. Keboola makes no warranties, express or implied, for this service. No service level agreement or similar arrangement applies to beta features.

A.3 Transparency and Compliance

A.3.1 User Notification. Client is responsible for ensuring that its authorized users are clearly informed that they are interacting with an AI system.

A.3.2 Transparency Responsibility. Client is responsible for providing all necessary information and notices to its users regarding the processing of their data, including disclosures regarding international data transfers.

A.4 Final Provisions

A.4.1 Sub-processor Updates. Keboola may add or change sub-processors for the Kai AI Assistant. Any such changes will be conducted in accordance with the existing Data Processing Agreement (DPA) between the parties.

A.4.2 Modifications. Keboola reserves the right to update these Terms at any time. Changes will be notified via email or other notice and will become effective 30 days after notification.

A.4.3 Privacy Policy. The processing of user account data remains subject to Keboola's general Privacy Policy.

A.4.4 Conflict of Terms. In the event of any conflict between these Terms and the Agreement, these Terms shall prevail solely concerning the Kai AI Assistant features.

— *End of Policy* —