

# AI Usage Policy

**Policy Owner:** Brendan Moore, CTO

**Applies to:** All employees, contractors, and third-party partners

## Purpose

This policy governs the design, development, deployment, and governance of AI systems to ensure they are safe, ethical, secure, and compliant with the EU AI Act and other relevant legislation.

### Definitions

- **AI (Artificial Intelligence):** Machine-based systems that perform tasks typically requiring human intelligence, including natural language processing, data summarisation, insight generation, or predictive modelling.
- **Inference:** The processing of data using a pre-trained AI model to generate outputs without modifying the model.
- **RAG (Retrieval-Augmented Generation):** An architecture that combines pre-trained AI with retrieval of external data sources to inform responses.
- **Customer Data:** Any data submitted, uploaded, or processed by the customer or participants within the Ballpark platform.
- **High-Risk AI Systems:** AI systems subject to elevated regulatory scrutiny or registration under the EU AI Act, including recruitment, biometric identification, and credit scoring systems.

## Scope

This policy applies to:

## Ballpark

- All AI features developed or integrated into Ballpark products and internal systems.
- All staff involved in the lifecycle of AI models, including design, testing, deployment, and monitoring.
- Third-party AI systems integrated with Ballpark services.

## Core Restrictions

### Inference-Only Operations

Ballpark restricts all AI system usage to inference operations only. This means:

- **AI systems may only be used for inference:** processing data and generating outputs from pre-trained models
- **Prohibited:** Using any customer data, user-generated content, or customer-specific business data for training, fine-tuning, retraining, model evaluation, or performance testing

### Retrieval-Augmented Generation (RAG) Systems

Ballpark may use RAG systems to enhance AI capabilities with internal knowledge and expertise.

#### Permitted content:

- Ballpark's internal documentation and procedures
- Team member professional knowledge and expertise
- Industry best practices and publicly available technical documentation
- Ballpark's proprietary methodologies and frameworks

#### Prohibited content:

- Customer data
- Customer-generated content
- Customer-specific business information

All RAG knowledge bases must be reviewed and approved by the CTO before implementation.

## Data Protection

## Customer Data Isolation

- Customer data must remain completely isolated from AI training pipelines and RAG systems
- Technical controls required to prevent inadvertent customer data usage
- All customer data processing must be transient with no storage for improvement purposes

## Consent Requirements

- Explicit, granular opt-in consent required for any AI processing of customer data
- Clear specification of AI processing being performed
- Confirmation that data will not be used for training
- Accessible opt-out mechanisms

## Compliance Framework

### Risk classification

All AI systems must be assessed and classified according to the EU AI Act's risk-based framework:

- **High-risk systems:** Require pre-deployment assessments, documentation, and registration (e.g. recruitment tools, critical infrastructure decisions)
- **Limited/minimal-risk systems:** Implement proportionate safeguards with transparency and user control

Ballpark will maintain documentation of all AI use cases, classification outcomes, and applicable controls.

### Human Oversight

All high-risk AI systems must include documented human-in-the-loop or human-on-the-loop mechanisms to allow for oversight, correction, or override of automated decisions. Responsibility for each AI system must be assigned to an accountable individual or team.

## Transparency Requirements

- Users must be notified when interacting with AI systems
- Clear communication that data is used for inference only, never for training

## **Ballpark**

- Explanation of AI decision-making logic and limitations, especially for high-risk cases

## **Third-Party AI Services**

- Contracts must explicitly prohibit using Ballpark/customer data for training or improvement
- Service agreements must guarantee inference-only usage
- Regular compliance audits required

## **Quality Assurance**

### **Fairness and Security**

- Regular bias testing for discriminatory impacts
- Pre-deployment security testing and ongoing performance evaluation
- Protection against adversarial attacks and model drift
- Fallback mechanisms for service degradation

### **Ethical Impact Assessments**

Required for high-risk systems, including:

- Societal and human rights impact assessment
- Potential harm identification and mitigation strategies
- Confirmation of customer data protection compliance
- Annual review and registration in AI systems register

## **Incident Management and Redress**

Users must have access to a channel to report:

- Negative effects or harms from AI usage
- Errors or inappropriate decisions made by AI systems

Reports will be reviewed under Ballpark's incident response framework, and affected parties will be informed of outcomes and potential redress options.

## **Sustainability and Social Benefit**

Teams are encouraged to evaluate the environmental impact (e.g. energy consumption of model training) and consider more efficient alternatives.

Priority will be given to projects where AI applications contribute to social good, accessibility, or public benefit.

## Monitoring and Policy Review

AI systems must be regularly audited to ensure:

- Accuracy and reliability
- Ongoing compliance with evolving legal standards
- Annual policy review or upon significant legislative changes
- Ethical performance

This policy will be reviewed annually or upon significant changes in legislation or AI practices.

## Roles and Responsibilities

Role	Responsibility
CTO	Policy owner and final authority on AI governance decisions
Engineering Team Leads	Classification, documentation, and testing of AI systems
Security & Compliance	Legal risk assessment, GDPR/Data Privacy alignment, and ethical impact review
Support & Customer Ops	Communicating AI usage and managing incident reporting and redress

## Exceptions

Any deviations from this policy must be approved by the CTO in writing, with a supporting risk justification and mitigation plan.