

## **Collibra AI Acceptable Use Policy**

This Artificial Intelligence Acceptable Use Policy ("AI AUP") applies to Customers' use of all products and services offered by Collibra and its affiliates that incorporate artificial intelligence, including Generative AI ("AI Services"). Capitalized terms not defined herein shall have the meanings ascribed to them in the Agreement pursuant to which Collibra or its affiliates provide Customer with such product or services ("Agreement").

### **1. Customer Responsibilities**

Customers are solely responsible for: (a) ensuring their use of AI Services complies with all applicable laws, regulations, and internal policies; (b) determining whether their use cases are appropriate and safe; (c) reviewing and validating all AI-generated outputs before use; and (d) maintaining appropriate human oversight for decisions with significant consequences.

### **2. Prohibited Uses of AI Services**

Customers may not use or allow their users to use AI Services for:

- 2.1. **Illegal or Harmful Activities:** Child sexual abuse or exploitation content (CSAM); violent extremism or terrorism; illegal activities; malware or malicious code; unauthorized access or hacking; non-consensual intimate imagery (NCII); or self-harm promotion.
- 2.2. **High-Risk Automated Decisions:** Making automated decisions with legal or similarly significant effects without human oversight, including credit, employment, housing, insurance, education, payday lending, or criminal justice decisions.
- 2.3. **Professional Advice:** Providing individualized legal, medical, or financial advice without qualified human review by licensed professionals.
- 2.4. **Discrimination:** Evaluation or classification of individuals based on their social behavior, personal traits, or biometric data (including social scoring, profiling, or inferring sensitive attributes); emotion detection in workplace or educational settings (except medical/safety purposes); or predicting criminality based on personality profiling.
- 2.5. **Deception:** Impersonating individuals without disclosure; creating deepfakes to deceive; generating misleading expertise claims; plagiarism or academic dishonesty;; bypassing safety filters; or misrepresenting AI-generated content as human-created.
- 2.6. **Intellectual Property Violations:** Infringing copyrights, trademarks, or other IP rights; extracting or reverse-engineering model weights or training data; or creating derivative works that violate third-party rights.
- 2.7. **System Abuse:** Attempting to "jailbreak" or manipulate models; overwhelming AIServices with excessive requests; using AI Services to train competing AI systems without authorization; or probing for security vulnerabilities without prior consent.
- 2.8. **Further Generative AI Restrictions:** Sexually explicit material, pornography, or sexual chatbots; weapons or explosives development; or hate speech, harassment, or content promoting violence or discrimination.

### **3. Monitoring and Enforcement**

Except as expressly stated in the Agreement, Collibra reserves the right to: (a) monitor usage patterns to detect policy violations; (b) log prompts and outputs for abuse detection; (c) temporarily or permanently restrict access to AI Services; and (d) report violations to law enforcement when required. Customers should report suspected abuse through Collibra's designated reporting channels.