SITETRACKER

Artificial Intelligence Acceptable Use Policy

1. **Scope**
   a. This Artificial Intelligence Acceptable Use Policy (this "**Policy**") applies to customers' use of all services offered by Sitetracker, Inc. or its affiliates ("**Sitetracker**"), or third-party products, applications or functionality that interoperate with services offered by Sitetracker, that incorporate artificial intelligence (collectively, "**Covered AI Services**"). Within the Covered AI Services, those that use Generative AI will be referred to as the "Covered Generative AI Services." The terms of this Policy are in addition to the Sitetracker Acceptable Use Policy at https://www.sitetracker.com/legal/.
2. **Last Updated**
   a. April, 2025
3. **Changes to Policy**
   a. Sitetracker may change this Policy by posting an updated version of the Policy at https://www.sitetracker.com/legal/ and such updates will be effective upon posting.
4. **Violations**
   a. A customer's violation of this Policy will be considered a material breach of the Master Subscription Agreement at https://www.sitetracker.com/legal/, or a written master subscription/services agreement executed by Customer and Sitetracker (the "**MSA**").
5. **Definitions**
   a. "Input" means any text, query, prompt, data, or content submitted by Customer or its users to a Covered AI Service.
   b. "Output" means any result or content generated by a Covered AI Service in response to an Input.
6. **Disallowed Usage:**
   a. Customers may not use a Covered AI Service, nor allow their users or any third party to use a Covered AI Service, for the following:
      i. Automated Decision-Making Processes with Legal/Similarly Significant Effects
         1. As part of an automated decision-making process with legal or similarly significant effects, including in any domains that may affect an individual's rights, safety, health or well-being (for example, in the domains of finance, employment, healthcare, housing, insurance, social welfare, or other essential goods and services), unless Customer ensures that the final decision is made by a human being and complies with all applicable laws related to such use, which may include any requirements for specific review, special audit and testing, consent, notice, or disclosure. Customer must take account of other factors beyond Covered AI Services' recommendations in making the final decision.
         2. As part of an automated decision-making process for payday lending even when the final decision is made by a human being.
      ii. Individualized Advice from Licensed Professionals
         1. Generating individualized advice that in the ordinary course of business would be provided by a licensed professional. This includes, for example, financial and legal advice.
         2. Generating or providing individualized medical advice, treatment, or diagnosis to a consumer or user.
         3. For clarity, this section does not limit a customer from using Covered AI Services for other purposes, such as general customer support in regulated industries, or assisting a licensed professional where Covered AI Services were not leveraged in the generation of individual advice. When a customer uses such services to assist in providing individualized advice (e.g., summarization), there must be a qualified person reviewing the Output.
      iii. Explicitly Predicting Protected Characteristics
         1. Explicitly predicting an individual's protected characteristic, including, but not limited to, racial or ethnic origin, and past, current, or future political opinions, religious or philosophical beliefs, trade union membership, age, gender, sex life, sexual orientation, disability, health status, medical

condition, financial status, criminal convictions, or likelihood to engage in criminal acts.
    a. Section 6(a)(iii) should not limit or prohibit use cases or tools designed specifically to identify security breaches, unauthorized access, fraud, and other security vulnerabilities, or to identify and reduce bias in Covered AI Services.
    b. Additionally, a customer may not submit images of individuals for the purposes of creating or analyzing biometric identifiers, such as face prints or fingerprints or scans of eyes, hands, or facial geometry.

iv. Interference with Safety
    1. Disabling, circumventing, or interfering with any safety mechanisms or technical safeguards included in the Covered AI Services.

v. Adversarial Use
    1. Attempting to manipulate, subvert, or degrade the features/functionality of Covered AI Services, including by means of prompt injection, model inversion, or other techniques intended to: (i) bypass content safeguards or usage restrictions; (ii) extract underlying model data, training content, or confidential system behavior; and (iii) impair service performance or reliability.

vi. Use under Applicable AI Regulation
    1. Using Covered AI Services in any manner that would qualify as a prohibited or high-risk use case under applicable AI-specific regulations, including the European Union Artificial Intelligence Act. This includes, without limitation, use in biometric surveillance, emotion recognition in the workplace, social scoring, or real-time remote biometric identification in public spaces.

vii. Deceptive Activity
    1. Engaging in, generating or promoting disinformation, misinformation, plagiarism or academic dishonesty

viii. Child Exploitation and Abuse
    1. Creating, sending, uploading, displaying, storing, processing, or transmitting material that may be harmful to minors including, but not limited to, for any purposes related to child exploitation or abuse, such as real or artificial Child Sexual Abuse Material (CSAM).

ix. Disclosures
    1. A customer must disclose to users when they are interacting directly with automated systems, such as AI-empowered bots, AI agents, or similar features, unless there is a human in the loop, and when required by law, provide a means for users to interact with a human instead of an automated system.

b. Customers may not use a Covered Generative AI Service, nor allow its users or any third party to use any Covered Generative AI Services, for the following:

i. Weapons Development
    1. Developing, advertising, marketing, distributing, or selling weapons, weapon accessories, or explosives, as enumerated by the United States Munitions List.

ii. Political Campaigns
    1. Targeting, creating, or distributing political campaign materials for external public or semi-public audiences. Political campaign material refers to material:
        a. That may influence a political process, such as an election, passage of legislation, regulation or ballot measure, judicial ruling, and content for campaigning purposes; or
        b. Soliciting financial support for (a).

iii. Adult Content
    1. Creating, sending, uploading, displaying, storing, processing, or transmitting sexually explicit material;
    2. Creating, sending, uploading, displaying, storing, processing, or transmitting sexual chatbots or engaging in erotic chat.

iv. Disclosures
    1. Customers may not deceive users or any third parties by misrepresenting Output generated through Covered Generative AI Services as human generated or original content.
        a. Customer may not remove markings or disclosures that indicate Output was generated by AI.

7. **Notices**
    a. AI technology will continue to be used in new and innovative ways. Customer is solely responsible for determining if its use of these technologies is safe.