Exhibit F: Acceptable Use Policy

Acceptable Use Policy

Version 1.4

Effective September 15, 2023

Safety is core to Anthropic's mission and we are committed to building an ecosystem where users can safely interact with and build on top of our products in a harmless, helpful, and honest way. Our Acceptable Use Policy (AUP) applies to anyone who uses Anthropic's tools and services, and is intended to help our users stay safe and to ensure our products and services are being used responsibly.

If we discover that your product or usage violates Anthropic's policies, we may issue a warning requesting a change in your behavior, adjust the safety settings of your in-product experience, or suspend your access to our tools and services.

Finally, it's important to remember that generative models are capable of producing factually inaccurate, harmful, or biased information. Our mission is to make safe AI systems and as we work to meet this goal, we ask that you independently verify our model responses and notify us at usersafety@anthropic.com when our model outputs inaccurate, biased, or harmful content.

Prohibited Uses:

We do not allow our products and services to be used in connection with, including to generate, any of the following:

Abusive or fraudulent content. This includes using our products or services to:

- Promote or facilitate the generation or distribution of spam;
- Generate content for fraudulent activities, scams, phishing, or malware;
- Compromise security or gain unauthorized access to computer systems or networks, including spoofing and social engineering;
- Violate the security, integrity, or availability of any user, network, computer or communications system, software application, or network or computing device;
- Violate any natural person's rights, including privacy rights as defined in applicable privacy law;
- Inappropriately use confidential or personal information;
- Interfere with or negatively impact Anthropic's products or services;
- Utilize prompts and results to train an AI model (e.g., "model scraping").

Child sexual exploitation or abuse content. We strictly prohibit and will report to relevant authorities and organizations where appropriate any content that exploits or abuses minors.

This includes content related to grooming, pedophilia, and nudity or that describes, encourages, supports or distributes any form of child sexual exploitation, abuse or material.

Deceptive or misleading content. This includes using our products or services to:

- Impersonate a human by presenting results as human-generated, or using results in a manner intended to convince a natural person that they are communicating with a natural person;
- Engage in coordinated inauthentic behavior or disinformation campaigns;
- Target or track a person's location, behavior, or communication without their consent;
- Generate deceptive or misleading comments or reviews;
- Engage in multi-level marketing or pyramid schemes;
- Plagiarize or engage in other forms of academic dishonesty.

Illegal or highly regulated goods or services content. This includes using our products or services to:

- Engage in any illegal activity;
- Provide instructions on how to create or facilitate the exchange of illegal substances or goods;
- Encourage or provide instructions on how to engage in or facilitate illegal services such as human trafficking or prostitution;
- Design, market, help distribute or utilize weapons, explosives, dangerous materials or other systems designed to cause harm to or loss of human life;
- Provide instructions on how to commit or facilitate any type of crime;
- Gamble or bet on sports.

Psychologically or emotionally harmful content. This includes using our products or services to:

- Encourage or engage in any form of self-harm;
- Shame, humiliate, bully, celebrate the suffering of, or harass individuals.

Sexually explicit content. This includes using our products or services to:

- Generate pornographic content or content meant for sexual gratification, including generating content that describes sexual intercourse, sexual acts, or sexual fetishes;
- Engage in erotic chats.

Violent, hateful, or threatening content. This includes using our products or services to:

- Threaten, incite, promote, or actively encourage violence or terrorism;
- Describe, encourage, support, or provide instructions on how to commit violent acts against persons, animals, or property;
- Encourage hate speech or discriminatory practices that could cause harm to individuals or communities based on their protected attributes, such as race, ethnicity, religion, nationality, gender, sexual orientation, or any other identifying trait.

Prohibited Business Use Cases:

In addition to the above use cases, we prohibit businesses from using our products and tools for any of the following:

- **Political campaigning or lobbying.** Creating targeted campaigns to influence the outcome of elections or referendums; political advocacy or lobbying;
- **Covertly tracking, targeting, or surveilling individuals.** Searching for or gathering information on an individual or group in order to track, target or report on their identity, including using the product for facial recognition, covert tracking, battlefield management applications or predictive policing;
- **Social scoring:** Utilizing Claude to assign scores or ratings to individuals based on an assessment of their trustworthiness or social behavior;
- **Criminal justice decisions.** Eligibility for parole or sentencing decisions;
- **Automated determination of financing eligibility of individuals.** Making automated decisions about the eligibility of individuals for financial products and creditworthiness;
- **Automated determination of employment and housing decisions.** Making automated decisions about the employability of individuals or other employment determinations or decisions regarding eligibility for housing, including leases and home loans;
- **Any law enforcement application.** Except for the following permitted applications by U.S. law enforcement organizations:
    - Back office uses including call center support, document summarization, and accounting;
    - Analysis of data for the location of missing persons and other applications, provided that such applications do not otherwise violate or impair the liberty, civil liberties, or human rights of natural persons.

Additional Requirements for Businesses:

If your business is using or deploying our tools and services as part of providing ***legal, medical, or financial advice*** to consumers, we require that you implement the additional safety measures listed below:

- **Human-in-the-loop:** any content that is provided to your consumers must be reviewed by a qualified professional in that field prior to dissemination. Your business is responsible for the accuracy and appropriateness of that information.
- **Disclosure:** you must disclose to your customers that you are using our services to help inform your decisions or recommendations.

Finally, if your business is using or deploying our products as part of an automated service where your external customers or users interact directly with our products, for example chatbots, you must disclose to your users that they are interacting with an AI system rather than a human.

If you have any questions about whether your business or use case is permitted or prohibited by this AUP, please email us at usersafety@anthropic.com.