Acceptable Use Policy

1. Purpose, Scope and Status

This Acceptable Use Policy ("AUP") sets the rules for using the Subcontext platform and services (the "Service"). It applies to every Customer and to everyone and everything that uses the Service under a Customer's Organisation: its employees, contractors and agents, and any automated process acting within the Service, including AI Agents, Tools and the dashboard assistant.

This AUP forms part of the Terms of Service between Subcontext and the Customer. Capitalised terms used but not defined in this AUP have the meanings given to them in the Terms of Service. A user who accepts this AUP, for example when signing up or joining an Organisation, accepts it on the Customer's behalf and agrees to follow it personally. The Customer is responsible for its users' compliance.

A serious or repeated breach of this AUP is a material breach of the Terms of Service. Subcontext responds to breaches proportionately, as set out in Section 10.

2. General Obligations

Customer must:

- Use the Service only for lawful purposes and in accordance with all applicable laws, regulations, and the rules of its regulators
- Ensure that all individuals and automated processes operating under Customer's Organisation comply with this AUP
- Implement and maintain appropriate internal controls, monitoring, and oversight of all Service usage within Customer's Organisation
- Promptly report any suspected breach of this AUP to Subcontext at hello@subcontext.com
- Cooperate with Subcontext in the investigation and remediation of any suspected breach

3. AI Agent Conduct

3.1 Prohibited Agent Configurations

Customer must not deploy or configure Agents to:

- Impersonate real individuals, named professionals, government officials, or specific organisations without explicit written authorisation from the person or entity being represented
- Claim to be human, or deny being an AI system, when a Contact asks or where the law requires the Contact to be told
- Generate false, fabricated, or deliberately misleading information, including fake reviews, testimonials, credentials, qualifications, or certifications
- Engage in social engineering, manipulation, coercion, or psychological pressure tactics against Contacts, or exploit a Contact's vulnerability

- Give regulated advice, including a personal recommendation on an insurance, investment, mortgage or other financial product. Agents may support non-advised sales and give factual information, and must refer anyone who needs advice to a qualified person at Customer
- Give medical diagnoses, legal advice, or therapeutic counselling
- Make binding commitments, guarantees, warranties, or promises on Customer's behalf that Customer is unable or unwilling to honour
- Collect personal data from Contacts through deceptive means or without adequate disclosure

3.2 Agent Safety Requirements

Customer must:

- Configure and maintain appropriate Guardrails, conduct rules and Agent Policies for all production Agents
- Thoroughly test all Agents before promoting them to production use
- Regularly review Agent Conversations and outputs for quality and compliance
- Maintain human oversight and a route to a person at Customer for Agents operating in sensitive contexts
- Promptly disable or modify any Agent that exhibits harmful, non-compliant, or unintended behaviour
- Not bypass, disable, or undermine the baseline safety controls the Service applies to every Agent

3.3 AI Disclosure and Sensitive Contexts

Customer must tell Contacts that they are dealing with an AI system wherever the law or a regulator's guidance requires it, including under Article 50 of the EU AI Act for Contacts in the European Union. Subcontext recommends telling consumers in every case as good practice. The Service provides an AI disclosure rule that Customer can switch on for its Agents.

Customer must put in place additional safeguards, including clear escalation to a person at Customer, when deploying Agents in the following contexts:

- Healthcare or medical information, including health questions in insurance applications
- Legal information or dispute resolution, including complaints handling
- Lending or credit
- Education of minors
- Employment or recruitment decisions
- Emergency or crisis situations
- Contacts who may be vulnerable (for example because of ill health, bereavement, financial difficulty, mental health or domestic abuse). The Service's vulnerability detection is a safeguard, not a substitute for Customer's own processes.

4. Messaging and Communications

4.1 Prohibited Messaging Practices

Customer must not use the Service to:

- Send unsolicited direct marketing to individuals without the consent or other basis the law requires

- Send messages or make calls using a false, misleading, or spoofed sender identity or calling line identity
- Continue sending messages to individuals who have opted out, unsubscribed, or asked not to be contacted
- Send messages at unreasonable hours or at excessive frequency
- Use the Service for phishing or any form of fraudulent communication
- Send messages containing malware, malicious links, or deceptive redirects
- Send messages promoting illegal products, services, or activities

4.2 Consent and Compliance

Customer must:

- Have a lawful basis for every outbound communication, on every channel, and the Contact's consent or a valid soft opt-in where the law requires it (for example, for electronic marketing)
- Have a Contact's prior consent before an Agent makes an automated voice call to them for direct marketing, as the Privacy and Electronic Communications Regulations ("PECR") require
- Screen live marketing calls against the Telephone Preference Service and Corporate Telephone Preference Service where the law requires it, and display a valid calling line identity. The Service's TPS check is a safeguard and does not replace Customer's own responsibility
- Honour all opt-out and unsubscribe requests promptly and completely, and not remove, hide or obstruct the opt-out mechanisms the Service adds to messages
- Include clear identification of the sender and a mechanism to opt out in all marketing communications
- Comply with all applicable messaging laws in every jurisdiction where messages are received, including the UK GDPR and PECR
- Maintain records of consent sufficient to demonstrate compliance upon request, and record consent through the Service only where it was actually given, with an accurate account of how and when
- Describe each message's purpose accurately, and not mark marketing as a service or essential message to send it to someone who has said no
- Make sure that any financial promotion an Agent communicates has been approved as the rules that apply to Customer require

5. Data and Information

5.1 Prohibited Data Practices

Customer must not:

- Use the Service to collect, store, or process personal data without a lawful basis under applicable data protection legislation
- Upload or import data to the Service that Customer does not have the right to use
- Use Tools to exfiltrate, scrape, or systematically extract data from third-party services in breach of those services' terms
- Store payment card numbers, bank account numbers, government identity numbers, or other highly sensitive data in free-text fields within the Service (such data should be collected only through the

payment and other secure features designed for it)

- Process personal data of children without a lawful basis and, where it applies, compliance with the ICO's Age Appropriate Design Code (the Children's Code). Insurance products may cover children as insured lives: Customer is responsible for handling their data lawfully
- Use the Service to circumvent data protection rights, including rights of access, rectification, erasure, and objection
- Share or transfer data between Organisations in breach of data protection law or applicable data sharing agreements

6. Knowledge Bases

Customer must not:

- Ingest copyrighted material into Context Blocks without appropriate licence or authorisation
- Build Context Blocks from personal data scraped from social media, public directories, or other sources without a lawful basis
- Upload content to Context Blocks in a manner that infringes any third-party intellectual property right

7. Payments and Financial Transactions

Customer must not:

- Use Agents to collect payments from Contacts under false pretences, duress, or deceptive circumstances
- Process fraudulent, unauthorised, or illegal transactions through the Service
- Use the payment features for money laundering, terrorist financing, or any prohibited financial activity
- Charge amounts that differ from what was communicated to the Contact
- Fail to honour refund obligations arising from transactions processed through the Service

As between Subcontext and Customer, Customer is responsible for payment disputes, chargebacks, and regulatory compliance relating to payments collected through Agents, except to the extent caused by Subcontext's breach of the Terms of Service.

8. Platform Security and Integrity

Customer must not:

- Attempt to gain unauthorised access to the Service, other users' accounts, other Organisations, or data belonging to other customers
- Probe, scan, or test the vulnerability of the Service or any related system or network, unless Subcontext has agreed in writing in advance. Security researchers should follow the Vulnerability Disclosure Policy
- Reverse engineer, decompile, disassemble, or attempt to derive the source code of the Service, except to the extent the law permits this despite this restriction
- Introduce viruses, worms, trojans, or other malicious code into the Service
- Interfere with or disrupt the Service, servers, or networks connected to the Service

- Use the Service to conduct denial-of-service attacks against any system
- Circumvent, disable, or tamper with any security, authentication, or access control mechanism
- Share account credentials or allow unauthorised individuals to access the Service
- Use the Service, or information obtained from it, to build a competing product or service, or publish benchmark results without Subcontext's prior written consent. Benchmarking and testing for Customer's own internal evaluation are permitted
- Resell, sublicence, or redistribute access to the Service without Subcontext's prior written consent

9. Content Restrictions

Customer must not use the Service to create, store, transmit, or distribute content that:

- Depicts child sexual abuse material (CSAM) or the sexual exploitation of minors
- Promotes or facilitates terrorism, violent extremism, or radicalisation
- Provides instructions for the manufacture of weapons, explosives, or dangerous substances
- Constitutes or facilitates human trafficking or modern slavery
- Promotes the sale or distribution of illegal drugs or controlled substances
- Constitutes hate speech targeting individuals or groups based on race, ethnicity, religion, gender, sexual orientation, disability, or other protected characteristics
- Infringes the intellectual property rights of any third party
- Breaches the privacy rights of any individual
- Constitutes defamation, harassment, or intimidation

10. Monitoring and Enforcement

10.1 Subcontext's Rights

Subcontext may:

- Monitor use of the Service for compliance with this AUP, using automated and manual means, in line with the Data Processing Agreement
- Investigate suspected breaches of this AUP
- Remove or disable access to specific content that breaches this AUP
- Report illegal activity to the appropriate law enforcement or regulatory authorities
- Respond to a legally binding request from a public authority, handling any Customer personal data as the Data Processing Agreement sets out (including telling Customer about the request unless the law prohibits it, and disclosing only the minimum required)

10.2 Reporting Breaches

If you become aware of any use of the Service that breaches this AUP, please report it promptly to hello@subcontext.com.

10.3 Responding to Breaches

Subcontext responds to a breach of this AUP in proportion to its seriousness. Depending on the circumstances, Subcontext may:

- Ask Customer to remedy the breach within a reasonable time
- Remove or disable the content, Agent, Tool, channel or feature concerned
- Suspend all or part of the Service, but only to the extent reasonably necessary and in accordance with the suspension provisions of the Terms of Service
- Terminate the Terms of Service for a serious or repeated breach, in accordance with the termination provisions of the Terms of Service
- Take legal action, including claims for damages and injunctive relief
- Report the matter to law enforcement or regulatory authorities

Subcontext normally gives notice and an opportunity to remedy before suspending. Where a breach creates an immediate risk to security, a risk of breaking the law, or a risk of harm to Contacts or other third parties, Subcontext may act first and will give notice as soon as practicable. Subcontext never deletes Customer data as an enforcement step: on termination, data is exported and deleted under the termination and deletion provisions of the Terms of Service.

11. The Subcontext Apps and the Dashboard Assistant

This AUP applies in full when the Service is used through a Subcontext app for iPhone, iPad, Mac or Android, or any other app Subcontext publishes (each an "App"), and to the dashboard assistant, including any action the assistant takes with a user's approval, which is treated as that user's own action. In addition, Customer must ensure that users:

- protect any device signed in to the App with a passcode or biometric lock, and sign out of the App (or revoke its sign-in from their profile) before a device is lost, sold, shared or passed to someone else;
- do not let anyone else use the App while it is signed in to their account;
- install the App only from Apple's App Store, Google Play, subcontext.com or another source subcontext.com names as official, and not a modified copy;
- turn on the App's caller ID only where Customer's data protection obligations permit Contact names and numbers to be held on that device, and turn it off (or sign out) when the device stops being used for Customer's business;
- do not copy, screenshot, forward or otherwise take Contact personal data out of the App except as Customer's own data protection obligations permit;
- choose notification settings, and where needed lock-screen settings, so that Contact details shown in push notifications are not exposed to people who should not see them; and
- do not decompile, reverse engineer, or attempt to extract data or credentials stored by the App, or use the App's connection to the Service other than through the App, except to the extent the law permits this despite this restriction.

12. Changes to this AUP

Subcontext may update this AUP, for example to reflect changes in the law, its providers' rules or the Service. Where a change is materially adverse to Customer, Subcontext will give at least 30 days' notice by email and in the dashboard before it takes effect, unless the law or a provider requires it sooner, and Customer may terminate as the changes provisions of the Terms of Service allow. Other changes take

effect when published. Where Customer has a signed order form or Enterprise agreement, its terms change only as that agreement allows.

13. Contact

To report a breach of this AUP or to ask questions about permitted use:

Subcontext Ltd Registered in England and Wales, No. 17019645 ICO registration No. ZC098511 124 City Road, London, EC1V 2NX Email: hello@subcontext.com

---

Subcontext Ltd, registered in England and Wales, Company No. 17019645. Registered office: 124 City Road, London, EC1V 2NX. The current version of this document is published at subcontext.com.