Company Code of Conduct

Last Updated: March 11, 2025

1. Purpose

This Company Code of Conduct establishes the ethical principles, standards, and commitments that guide how Synthetic Users operates as a business. It applies to all company activities, partnerships, and interactions with customers, users, and the public.

While our Employee Code of Conduct governs individual behavior within the organization, this document defines how we conduct business as a company — particularly in the context of AI-powered research and synthetic data generation.

2. Our Mission and Values

Synthetic Users exists to make user research faster, more accessible, and more inclusive through AI-powered synthetic interview participants. We believe that better research leads to better products, and that AI can augment — not replace — the human understanding at the heart of good design and decision-making.

Our core values:

- **Integrity** — We are honest about what our technology can and cannot do.
- **Privacy** — We treat customer data as sacred and never use it to train our models.
- **Transparency** — We communicate clearly about our methods, limitations, and data practices.
- **Responsibility** — We hold ourselves accountable for the outputs and impact of our AI systems.
- **Inclusion** — We design for diverse perspectives and work to reduce bias in AI-generated research.

3. Ethical AI Practices

As a company that generates synthetic research participants using frontier large language models, we have a heightened responsibility to use AI ethically.

3.1 Honest Representation

- We clearly communicate that our participants are AI-generated, not real people.
- We do not represent synthetic interview outputs as equivalent to human research without appropriate qualification.
- We encourage customers to use synthetic research as a complement to — not a replacement for — research with real participants where appropriate.

3.2 Bias Mitigation

- We use multiple frontier LLMs (our "LLM Shuffle" approach) to reduce the biases inherent in any single model.
- We continuously evaluate our systems for demographic, cultural, and cognitive biases.
- We are transparent with customers about the known limitations of synthetic research.

3.3 No Deceptive Use

- We do not allow our platform to be used to fabricate evidence, manufacture false consensus, or deceive end users.
- Our Acceptable Use Policy explicitly prohibits harmful, deceptive, or manipulative uses of our platform.
- We actively monitor for and take action against misuse.

3.4 Human Oversight

- We maintain human oversight over AI systems at every stage of our product pipeline.
- We empower our customers to review, question, and contextualize AI-generated insights.

- We do not automate decisions that should involve human judgment without appropriate safeguards.

4. Data Protection and Privacy

Data stewardship is foundational to our business. We commit to:

- **Zero Model Training** — We do not use customer data to train, fine-tune, or improve our AI models. Customer data belongs to the customer.
- **Data Minimization** — We collect and process only the data necessary to deliver our services.
- **Regional Data Residency** — Sensitive customer data is stored in the customer's own geographic region.
- **Transparent Data Flow** — We maintain clear documentation of our subprocessors and data flows and provide a Data Processing Addendum for enterprise customers.
- **Secure Deletion** — We honor data deletion requests promptly and maintain clear retention policies.

For full details, see our Privacy Policy.

5. Security Commitment

We maintain enterprise-grade security standards to protect our customers and their data:

- **SOC 2 Type 2 Certified** — We undergo independent audits to verify our security controls.
- **Encryption** — Data is encrypted in transit and at rest.
- **Access Controls** — We enforce least-privilege access, MFA, and SSO across our systems.
- **Incident Response** — We maintain and test an Incident Response Plan to respond quickly to security events.

- **Penetration Testing** — We engage third-party firms to conduct regular penetration tests.
- **Vulnerability Management** — We proactively identify, assess, and remediate vulnerabilities.

For full details, see our Security Policy Document.

---

6. Fair Business Practices

6.1 Anti-Corruption and Anti-Bribery

We do not tolerate bribery, corruption, or improper payments in any form. We comply with applicable anti-corruption laws, including the U.S. Foreign Corrupt Practices Act (FCPA) and equivalent international regulations. No employee, contractor, or partner may offer or accept bribes, kickbacks, or improper incentives.

6.2 Fair Competition

We compete on the merits of our products and services. We do not engage in anti-competitive practices, misrepresent competitors, or use unlawful means to gain market advantage.

6.3 Honest Marketing

We represent our products and capabilities truthfully. We do not make misleading claims about the accuracy, reliability, or scope of our AI-generated research. Where limitations exist, we disclose them.

---

7. Third-Party and Partner Standards

We expect our vendors, subprocessors, and partners to uphold standards consistent with this Code. We:

- Conduct third-party risk assessments before engaging new vendors.
- Require contractual commitments to data protection, security, and ethical conduct.
- Monitor ongoing compliance and terminate relationships where standards are not met.

8. Intellectual Property

We respect the intellectual property rights of others and protect our own:

- We do not knowingly infringe on third-party patents, copyrights, trademarks, or trade secrets.
- We ensure that our use of open-source software complies with applicable licenses.
- We protect our proprietary technology, including our models, architectures, prompt systems, and research methodologies.

9. Environmental and Social Responsibility

We recognize the environmental impact of operating AI systems and commit to:

- Evaluating the energy and compute footprint of our services.
- Choosing infrastructure providers with strong sustainability commitments.
- Supporting diversity, equity, and inclusion within our team and in the products we build.
- Upholding the principles outlined in our Human Rights Policy.

10. Reporting and Accountability

We maintain open channels for reporting concerns:

- Employees, contractors, and partners may report violations of this Code without fear of retaliation.
- Reports can be directed to compliance@syntheticusers.com or through internal reporting channels.
- All reports are investigated promptly and confidentially.
- We take corrective action where violations are confirmed, up to and including termination of business relationships.

---

11. Governance and Review

- This Code of Conduct is approved by the leadership of Synthetic Users and applies across all operations.
- It is reviewed at least annually and updated as our business, technology, and regulatory environment evolve.
- All employees receive training on this Code as part of onboarding and on an ongoing basis.

---

12. Contact

For questions about this Code of Conduct, contact us at support@syntheticusers.com.

Synthetic Users, Inc. 4223 Glencoe Ave, Suite C215-523, Marina del Rey CA 90292