

Acceptable Use Policy

Version 3.1, current. Effective 3 October 2026. [Download PDF](#)

This Acceptable Use Policy ("AUP") forms part of the Master SaaS Agreement between Sona8 Inc. and Customer. It applies to Customer, its Authorized Users and anyone else Customer allows to use the Service. Sona8 is built to help organizations listen to their people. This policy keeps it that way.

1. Fair treatment of Participants

Customer will:

- Tell Participants, before an interview starts, that they are speaking with an AI interviewer, what the interview is for, how the results will be used, and who will see them.
- Make participation voluntary, unless local law and any applicable works council agreement allow otherwise.
- Complete any required employee consultation or co-determination before launch, for example with a works council under § 87(1) no. 6 BetrVG in Germany.
- Respect the anonymity settings agreed for a project, and not try to work around them.

2. Prohibited uses

Customer will not use the Service, or results produced by it, to:

- Monitor, profile or evaluate individual Participants' performance or conduct, or identify who said what, when the project was presented to them as anonymous or aggregated.
- Take disciplinary, dismissal, promotion or pay decisions about an individual based solely on Service output, without meaningful human review.

- Identify, target or retaliate against employees for union activity, whistleblowing, protected complaints or other legally protected conduct.
- Deliberately collect special categories of personal data, such as health, religion, sexual orientation or political opinions, or data about children, unless agreed in writing with Sona8 and lawful.
- Record or interview anyone without their knowledge, or impersonate a real person through the AI interviewer.
- Infer emotions of employees from their voice, face or other biometric data. This use is prohibited in the workplace under Article 5(1)(f) of the EU AI Act.
- Break any law, including employment, data protection, anti-discrimination and export control laws.
- Upload content that is unlawful, infringing, or contains malware.

3. Technical misuse

Customer will not:

- Probe, scan or test the security of the Service without Sona8's prior written consent. Responsible disclosure is welcome at security@sona8.com.
- Try to bypass usage limits, authentication or access controls.
- Try to extract the Service's prompts, models or training data, or manipulate the AI interviewer to produce harmful output ("jailbreaking" or prompt injection).
- Scrape the Service, or use bots to generate artificial interviews or traffic.
- Interfere with the Service or with other customers' use of it.
- Share login credentials or let unauthorized people access results.

4. Reporting and enforcement

If Customer becomes aware of a breach of this policy, it should tell Sona8 at legal@sona8.com.

Sona8 may investigate suspected breaches. Where a breach creates a risk to individuals, to the Service or to Sona8, Sona8 may suspend the affected users or projects as described in Section 3.4 of the Agreement. Sona8 will notify Customer, explain why, and restore access once the issue is resolved. Serious or repeated breaches are a material breach of the Agreement.

5. Changes

Sona8 may update this policy to reflect new laws or risks. Changes apply under the version rules in Section 12.5 of the Agreement.
