

LEG-006 / CURRENT PUBLIC VERSION

Acceptable Use and Prohibited Conduct Policy

Rules protecting people, content, accounts, and SideOf systems.

EFFECTIVE DATE

26 September 2026

ISSUED BY

LIBRASIDE TECHNOLOGIES LLC d/b/a SideOf

CONTACTsupport@sideof.app**READ THIS FIRST**

This policy does not authorize scraping, penetration testing, automated collection, or security testing. Written authorization is required before testing systems you do not own.

Contents

[1. Lawful personal use](#)[3. Minors](#)[5. Fraud and deception](#)[7. Automation and data collection](#)[9. Commercial and political activity](#)[11. Enforcement](#)[2. Abuse and exploitation](#)[4. Intimate and private content](#)[6. System interference](#)[8. Intellectual property](#)[10. Security reporting](#)

1. Lawful personal use

Use SideOf only for lawful personal social and connection purposes. Do not use it to facilitate crime, evade legal obligations, or provide a regulated service without required authorization.

2. Abuse and exploitation

Harassment, stalking, threats, coercion, hate, trafficking, sexual exploitation, extortion, blackmail, doxing, and encouragement of violence or self-harm are prohibited.

3. Minors

A minor may not access SideOf. Do not contact, groom, sexualize, exploit, or create, request, possess, or distribute sexual material involving a minor. Apparent child sexual abuse material is reported and preserved as law requires.

4. Intimate and private content

Do not share or threaten to share intimate depictions without consent, including altered or synthetic material. Do not copy, publish, sell, or expose private messages, photos, contact details, or location information without permission and lawful basis.

5. Fraud and deception

Do not impersonate, catfish, manipulate verification, run romance or investment scams, solicit financial credentials, submit false claims, operate coordinated fake accounts, or misrepresent affiliation with SideOf.

6. System interference

Do not probe, scan, exploit, overload, disrupt, introduce malicious code, bypass authentication or access controls, evade rate limits, enumerate accounts, interfere with logging, or access data beyond your authorization.

7. Automation and data collection

Do not scrape, crawl, index, archive, train on, resell, or build profiles from SideOf content or member data. Bots, autoswipers, browser automation, and bulk messaging require written authorization.

8. Intellectual property

Do not infringe copyrights, trademarks, publicity rights, database rights, or other intellectual property. Do not remove notices, clone the interface, misuse brand assets, or distribute modified service software.

9. Commercial and political activity

Unsolicited advertising, recruiting, political solicitation, deceptive promotions, paid sexual services, illegal sales, pyramid schemes, and account, membership, reward, or eligibility transfers are prohibited.

10. Security reporting

Send a good-faith vulnerability report through the published security policy. Minimize access and data, stop when personal information is encountered, do not disrupt service, and allow reasonable remediation time. This policy is not a safe-harbor promise beyond the published security policy.

11. Enforcement

SideOf may rate-limit, remove content, revoke sessions, restrict features, suspend, terminate, preserve evidence, notify affected people, or refer conduct to providers or authorities where justified. Evasion may result in additional restrictions.