

Networker Acceptable Use Policy

The conduct rules that apply to every Networker account

Effective Date: July 30, 2026

1. Purpose and Incorporation

This Acceptable Use Policy sets out what you may and may not do with Networker. It is incorporated into and forms part of the Networker Terms of Service. Capitalized terms have the meaning given in the Terms. If this policy and the Terms conflict, the Terms control.

Networker exists to support genuine professional networking, contact research, and career development. Every rule below follows from that purpose, from the rules of the mailbox providers we connect to, and from the law that applies to commercial and professional email.

We may update this policy as the product, provider requirements, or the law change. Continued use after an update means you accept the updated policy.

2. Outreach Standards

You must have a genuine, good-faith reason to contact each recipient, such as a shared school, employer, alumni network, club, program, or industry, or a public invitation to be contacted. You may not contact people selected at random, purchased from a list, or scraped in bulk.

You are the sender of every message you send through Networker. You are responsible for the accuracy of your identity, your subject lines, and your content, and for complying with the CAN-SPAM Act, CASL, the UK and EU GDPR and ePrivacy rules, and every other anti-spam, privacy, or electronic communications law that applies to you or your recipients.

You must honor opt-out and unsubscribe requests promptly. If a recipient asks not to be contacted, stop contacting them and remove them from your workflows. Networker maintains a suppression list; addresses that have opted out, hard bounced, or been suppressed for abuse or compliance reasons are blocked from further sending, and you may not attempt to reach a suppressed address from another address, mailbox, or account.

You may not send spam, mass unsolicited email, cold commercial marketing to strangers, political persuasion at scale, fundraising blasts, chain messages, phishing, malware, or deceptive messages of any kind.

You may not falsely imply a relationship, referral, endorsement, employment status, school affiliation, authorization, or identity, and you may not send on behalf of anyone other than yourself.

3. Data and Platform Integrity

You may not scrape, crawl, spider, harvest, bulk export, republish, resell, broker, or build datasets from Networker, its contact database, school and firm data, club and alumni data, user data, match scores, rankings, or generated outputs, except through functionality Networker expressly provides for your own permitted use.

You may not use bots, scripts, headless browsers, browser extensions, reverse engineering, API abuse, credential sharing, rate-limit circumvention, session replay, or screen scraping to collect data from Networker or from other users.

You may not use Networker to build or improve a competing product, data brokerage, lead database, recruiting database, or outreach automation service.

You may not create multiple accounts, use another person's account, or share credentials to obtain additional plan capacity, database access, or sending volume, and you may not connect additional mailboxes or rotate accounts to evade sending limits.

You may not resell, sublicense, or provide Networker's sending capability to a third party, operate Networker on behalf of other people's outreach, or use Networker as infrastructure for another product or service.

4. Respect for People

You may not use Networker to identify, target, profile, discriminate against, harass, dox, threaten, impersonate, stalk, or otherwise harm any person.

You may not include sensitive personal information, protected class information, health information, government identifiers, or financial account details in outreach, notes, custom contacts, or profile fields. That information is not needed for professional networking and creates risk for the people it describes.

When you add your own contacts, you represent that you obtained the information lawfully, that you may store and use it for professional outreach, and that you will honor any request from that person to be removed.

Information you access through Networker about other people is to be used for your own lawful outreach workflow only. You may not disclose, sell, publish, or transfer it.

5. Security

You may not probe, scan, or test the vulnerability of Networker or its infrastructure without written authorization; access accounts, data, integrations, or non-public systems that are not yours; bypass authentication, authorization, rate limits, quotas, or security controls; or interfere with other users or with service availability.

You may not upload or transmit malware, or use Networker to distribute anything designed to damage, disable, or gain unauthorized access to a system.

If you believe you have found a security vulnerability, report it to support@trynetworker.com rather than exploiting it. Please give us a reasonable opportunity to fix the issue before disclosing it publicly, do not access or modify data belonging to other users, and do not degrade the service while testing. We will not pursue action against good-faith research that follows these conditions.

6. Provider Rules

You may not use Networker in a way that causes Networker or its integration providers to violate the terms, API policies, or acceptable use rules of Google, Microsoft, Composio, Stripe, or any mailbox provider. Networker may act immediately on any report or signal of abuse from a provider.

Provider sending limits, deliverability protections, and anti-abuse measures apply in addition to Networker's own limits. Where they are stricter, they govern.

7. Enforcement

Networker may investigate suspected violations and may throttle sending, restrict features, pause campaigns, disconnect mailboxes, suspend or terminate accounts, reclaim workspace identifiers, preserve evidence, and disclose records as needed to enforce this policy, protect recipients, or comply with law.

Networker records administrative actions, import operations, and security-relevant events in audit logs, which may be used to investigate abuse and support enforcement.

Serious or repeated violations may result in permanent termination without refund. Enforcement decisions are at Networker's discretion, and nothing here obliges Networker to act in any particular case or waives any remedy it does not use.

To report a violation of this policy, including unwanted messages sent through Networker, email support@trynetworker.com with the message details. Reports about outreach you received are reviewed and the sending address can be added to the suppression list on request.