

Networker Privacy Policy

California-focused privacy notice for Networker users

Effective Date: July 24, 2026

1. Introduction and Scope

This Privacy Policy explains how Networker collects, uses, discloses, retains, and protects personal information when you visit our websites, create an account, sign in with Google, connect a Microsoft email account, upload recruiting materials, use contact discovery, draft outreach, manage campaigns, or otherwise use Networker. References to Networker, we, us, or our mean the operator of the Networker service. References to you or user mean the person who visits, registers for, accesses, or uses Networker.

Networker is a finance recruiting and networking outreach platform. Users may use Networker to create a recruiting profile, identify potentially relevant finance professionals, draft personalized outreach, organize contacts, track outreach activity, connect Microsoft Outlook or Microsoft 365 for email sending, and manage recruiting workflows. This Privacy Policy applies to personal information collected through Networker and related communications. It does not apply to third-party websites, services, payment processors, identity providers, email providers, or other services that are not controlled by Networker.

This Privacy Policy is written with California residents in mind and includes disclosures intended to address the California Consumer Privacy Act, as amended by the California Privacy Rights Act, and related regulations, to the extent they apply to Networker. If a law gives you additional rights based on where you live, we will honor those rights as required by applicable law.

2. Important Definitions

Personal information means information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked with a particular person or household. Sensitive personal information may include account login credentials, contents of communications where legally protected, precise geolocation, government identifiers, financial account information, or other categories defined by applicable law.

Services means Networker's websites, web application, onboarding flow, dashboard, contact discovery tools, outreach drafting tools, campaign tools, Google sign-in, Microsoft email integration, payment and checkout flows, support channels, and related online services.

User Content means content you submit, upload, connect, save, draft, approve, import, or generate through Networker, including profile details, resume context, school or club selections, recruiting preferences, target firms, target cities, contact notes, campaign settings, email drafts, outreach status, and connected account metadata.

Service provider, contractor, processor, and subprocessor mean third parties that process personal information for Networker or on our behalf under contractual obligations. Third-party services mean services you choose to connect or use with Networker, such as Google, Microsoft, Supabase, Stripe, hosting providers, analytics providers, and communication providers.

3. Personal Information We Collect

Account information. We collect information you provide when you create or manage an account, including name, email address, password or authentication credentials handled through our authentication provider, profile information, school or program affiliation, account status, plan information, and related identifiers.

Recruiting profile and onboarding information. We collect schools, degree or program selections, clubs or student organizations, target cities, recruiting goals, bank types, groups of interest, resume filename or resume-derived context, professional interests, and other information you provide to personalize your workspace.

Resume and career materials. If you upload or provide resume details, we may process the file name, file metadata, text extracted from the resume, education, work experience, activities, skills, and other career information you submit. You

should not upload unnecessary sensitive information, Social Security numbers, financial account details, protected health information, or third-party confidential information.

Contact, outreach, and campaign data. We collect contact selections, target firms, groups, locations, school overlap, notes, status labels, draft messages, campaign configuration, scheduled or sent outreach metadata, response status, and related workflow information. This may include professional contact information about finance professionals that appears in Networker or that you add to your workspace.

Google sign-in data. If you sign in with Google, we receive basic identity information covered by the openid, email, and profile scopes, such as your Google account identifier, email address, name, profile image, and authentication information needed to maintain your session. Networker does not request Gmail, Google Drive, Google Calendar, contacts, or other Google Workspace scopes.

Microsoft email integration data. If you connect Microsoft Outlook or Microsoft 365, we receive authorization tokens, the connected account identifier and email address, basic profile information, message and draft content, provider draft or message identifiers, send status, and related metadata needed to create and update drafts, send user-approved or user-scheduled outreach, refresh the connection, track workflow status, troubleshoot issues, secure the service, comply with law, and enforce our terms. Networker requests delegated permissions only and does not request organization-wide application permissions.

Payment and transaction information. If you purchase a paid plan, our payment processor may collect payment card or financial details. Networker may receive limited billing information such as plan, transaction status, billing email, customer identifier, amount, currency, invoice or receipt metadata, and subscription status. We do not intentionally store full payment card numbers.

Communications and support. We collect information you provide when you contact us, request support, respond to surveys, submit feedback, book a demo, or otherwise communicate with us, including message contents, attachments, email address, and related metadata.

Usage, device, and log data. We collect information about how you access and use Networker, including IP address, device and browser type, operating system, referring pages, pages viewed, features used, timestamps, error logs, session information, cookie or local storage identifiers, approximate location inferred from IP address, and security events.

Information from third parties. We may receive information from authentication providers, Microsoft email services, payment processors, hosting, database, security, and analytics providers, and other services you authorize. We may also receive information from public or licensed sources used to populate firm, school, alumni, or professional contact context within the product.

4. How We Use Personal Information

We use personal information to provide, operate, maintain, secure, and improve Networker; create and authenticate accounts; personalize contact discovery and recommendations; generate and refine outreach drafts; operate Google sign-in and the Microsoft email integration; manage outreach campaigns; process payments; provide support; communicate with you; diagnose technical issues; prevent fraud, scraping, abuse, and unauthorized access; enforce our Terms of Service; comply with legal obligations; and protect the rights, safety, and security of users, Networker, and others.

We may use de-identified, aggregated, or anonymized information for analytics, product improvement, research, benchmarking, and business purposes, provided that we do not attempt to re-identify that information except as permitted by law to test whether it remains de-identified.

We do not use connected Microsoft email content or Microsoft user data to train generalized artificial intelligence or machine learning models. We do not sell email integration data. We do not use connected account data for advertising. We do not disclose connected account data except as necessary to provide the requested integration, comply with law, protect security, or as you direct.

Networker's use and transfer to any other app of information received from Google APIs will adhere to the Google API Services User Data Policy, including the Limited Use requirements. Google data is used for sign-in identity, account security, support, troubleshooting, legal compliance, and user-directed actions.

Networker does not use Google Workspace API data for advertising, retargeting, personalized advertising, data brokerage, resale, credit-worthiness decisions, or generalized AI model training. Networker does not request Gmail access.

5. AI, Drafting, and User Data Handling

Networker may use automated systems, rules, ranking logic, and AI-assisted drafting to help identify relevant contacts, summarize context, suggest talking points, draft outreach, or organize workflows. These outputs are generated to assist you. They are not professional, legal, financial, immigration, employment, or career advice, and they do not guarantee interviews, referrals, responses, offers, or outcomes.

You are responsible for reviewing, editing, and approving any draft before it is sent. Networker should not be used to send false, misleading, harassing, discriminatory, unlawful, or deceptive communications. You should not enter personal information about others unless you have a lawful basis and any required rights or permissions to do so.

We apply internal access controls, purpose limitations, and security measures to user data. Personnel, contractors, and service providers may access user data only where needed to operate, support, secure, troubleshoot, improve, or enforce Networker, or where required by law. Unauthorized browsing of user accounts, connected email content, or recruiting profile data is prohibited.

Networker does not use your resume content, connected Microsoft email content, contact notes, outreach drafts, or private recruiting workspace content to train generalized artificial intelligence or machine learning models. If we use third-party AI providers to power a requested feature, we require those providers to process user content only to provide the feature, protect security, comply with law, or as otherwise disclosed in this Privacy Policy.

AI-related processing may include sending limited prompts, profile context, selected contact context, draft text, or usage metadata to model or infrastructure providers. We design these flows to use the minimum information reasonably needed for the feature, to respect your account permissions, and to avoid exposing one user's private workspace content to another user.

6. Customer Data, Account Data, and Usage Data

Customer Data means the profile, resume, school, club, target city, recruiting preference, contact, note, campaign, draft, Microsoft email integration, and workflow content that you or your connected services submit to Networker for use in the product. You remain responsible for Customer Data and the rights needed to provide it to Networker.

Account Data means information needed to create, authenticate, bill, support, and administer your account, such as name, email address, user identifiers, plan, billing status, authentication records, support communications, and security events. Usage Data means logs, device data, feature usage, diagnostics, and analytics about how the Services perform and are used.

We use Customer Data primarily to provide, secure, support, troubleshoot, personalize, and improve the Services for you. We may use Account Data and Usage Data to operate the business, prevent abuse, understand product performance, communicate with you, enforce our Terms, comply with law, and improve Networker.

7. Subprocessors, Vendors, and Operational Providers

Networker relies on service providers and subprocessors for hosting, storage, databases, authentication, security, analytics, error monitoring, email delivery, payment processing, PDF generation, support, and AI-assisted functionality. These providers may process personal information only for authorized purposes and subject to contractual or technical restrictions appropriate to the service they provide.

Before using a provider for material processing of user data, we evaluate the provider's role, data access, security posture, confidentiality commitments, and ability to support our legal and operational obligations. We may update

providers over time as our infrastructure and product change.

Where a provider processes sensitive integration data, payment data, authentication data, or AI-related Customer Data, we seek contractual terms designed to limit use of that data to providing the service to Networker, maintaining security, complying with law, and preventing abuse.

8. How We Disclose Personal Information

Service providers and contractors. We may disclose personal information to vendors that host infrastructure, provide authentication, database, storage, analytics, error monitoring, email delivery, payment processing, customer support, security, or other services for Networker. These providers are authorized to use personal information only as necessary to provide services to us or as otherwise permitted by law.

Connected services you authorize. If you use Google sign-in, connect Microsoft email, make a payment, or authorize another third-party service, we disclose and receive information as needed to operate that integration and as directed by you. Your use of those third-party services is also governed by their own terms and privacy policies.

Legal, safety, and enforcement. We may disclose personal information if we believe disclosure is required or appropriate to comply with law, subpoena, court order, law enforcement request, regulatory request, legal process, or government request; enforce our Terms; investigate fraud, scraping, abuse, security incidents, or unlawful conduct; protect the rights, privacy, safety, or property of Networker, users, or others; or establish, exercise, or defend legal claims.

Business transfers. If Networker is involved in a merger, acquisition, financing, reorganization, bankruptcy, receivership, sale of assets, or transition of service to another provider, personal information may be disclosed or transferred as part of that transaction, subject to applicable law and appropriate protections.

With consent or direction. We may disclose personal information with your consent or at your direction, including where you choose to send outreach, export information, invite another user, or connect an integration.

9. No Sale of Personal Information; Sharing for Advertising

Networker does not sell personal information for money. Networker does not sell or share connected Microsoft email content, OAuth tokens, Google sign-in data, resume content, recruiting profile data, contact notes, or outreach drafts.

Some website analytics, advertising, or measurement technologies can be considered a sale or sharing of personal information under California law if they disclose identifiers or internet activity for cross-context behavioral advertising. Networker does not currently intend to sell or share personal information for cross-context behavioral advertising. If that changes, we will update this Privacy Policy and provide legally required opt-out mechanisms.

We honor legally required opt-out preference signals, such as Global Privacy Control, where applicable and technically feasible.

10. Cookies and Similar Technologies

We may use cookies, local storage, pixels, SDKs, and similar technologies to keep you signed in, remember preferences, secure sessions, prevent abuse, measure usage, understand performance, and improve Networker. You can control cookies through your browser settings. Some cookies or storage are necessary for authentication, security, checkout, and core service functionality.

If we use analytics or advertising technologies, those providers may process device identifiers, IP address, usage activity, and similar data according to their own policies and our contracts with them. We do not use cookies to access your connected email account content.

11. Data Retention

We retain personal information for as long as reasonably necessary to provide Networker, maintain your account, operate integrations, provide support, comply with legal obligations, resolve disputes, enforce agreements, prevent fraud or abuse, maintain security, and for legitimate business purposes. Retention periods vary based on the type of data, sensitivity, legal requirements, account status, user settings, and operational needs.

If you delete your account or request deletion, we will delete or de-identify personal information as required by law, subject to exceptions such as security, fraud prevention, legal compliance, backup retention, dispute resolution, transaction records, and legitimate business purposes. Backup copies may persist for a limited period before being overwritten.

Microsoft email tokens are retained only while the integration remains connected or as otherwise necessary for security, troubleshooting, legal compliance, or account recovery. Google sign-in identity information is retained while your Networker account remains active and as otherwise described in this section. Drafts, notes, campaign records, and generated content may remain in your workspace until you delete them, delete your account, or request deletion, subject to the exceptions described above.

12. Security

We use administrative, technical, and organizational safeguards designed to protect personal information, including access controls, authentication, encryption in transit where appropriate, provider security controls, logging, and vendor review. No online service is completely secure. You are responsible for maintaining the confidentiality of your account credentials, using strong passwords, limiting access to your devices, and promptly notifying us of suspected unauthorized access.

If we become aware of a data security incident affecting personal information, we will evaluate the incident and provide notices as required by applicable law.

Networker is designed to separate user accounts and workspaces logically. We use role-appropriate access controls, least-privilege practices where feasible, and provider-level security controls to reduce the risk that one user's private workspace content is exposed to another user.

You are responsible for the security of devices, browsers, Google accounts, Microsoft email accounts, and third-party services you connect to Networker. If those services are compromised, data available through the integration may also be at risk.

13. International Transfers

Networker is operated from the United States and uses providers that may process information in the United States and other countries. If you access Networker from outside the United States, your information may be transferred to, stored in, or processed in jurisdictions that may not provide the same level of data protection as your home jurisdiction.

Where required by applicable law, we use appropriate safeguards for international transfers, such as contractual commitments, provider data processing terms, or other transfer mechanisms recognized by law.

14. California Privacy Notice

This section applies to California residents. California law may provide rights to know/access categories and specific pieces of personal information, delete personal information, correct inaccurate personal information, opt out of sale or sharing, limit certain uses and disclosures of sensitive personal information, and not be discriminated against for exercising privacy rights.

Categories collected in the last 12 months may include identifiers; customer records information; commercial information; internet or other electronic network activity; approximate geolocation inferred from IP address; professional, education, or employment-related information; inferences; sensitive personal information such as account login credentials and contents of connected communications where you choose to connect an account; and user-generated content.

Sources include you, your device, your browser, connected services you authorize, payment processors, service providers, public or licensed professional information sources, and product usage. Business or commercial purposes include providing and securing Networker, personalization, contact discovery, drafting, outreach management, support, payments, analytics, compliance, fraud prevention, and enforcement.

Categories disclosed for business purposes may include identifiers, customer records, commercial information, internet

activity, professional or education information, inferences, and user-generated content, disclosed to service providers, contractors, connected services you authorize, payment processors, hosting providers, analytics providers, security providers, legal or compliance recipients, and parties involved in business transfers.

We do not use sensitive personal information to infer characteristics about you or for purposes that would require a California right to limit, unless we provide required notice and controls. We do not knowingly sell or share personal information of consumers under 16.

To exercise California rights, contact us at tanish@trynetworker.com. We may need to verify your identity and, for some requests, confirm account ownership. Authorized agents may submit requests if they provide proof of authorization and we can verify the request as required by law. We will not discriminate against you for exercising privacy rights, but some functionality may require certain information to operate.

15. User Control, Access, Correction, and Deletion

You may update certain account and profile information in Networker. You may request access, correction, deletion, export, or other privacy rights by contacting us. We may decline or limit requests where permitted by law, such as when retaining data is necessary for security, legal compliance, transaction records, debugging, fraud prevention, exercising legal rights, or completing services you requested.

You may disconnect Microsoft email through Networker settings or revoke access through Microsoft account or organization controls. Google users may revoke sign-in access through their Google Account permissions page. Disconnecting or revoking an integration may limit or disable sign-in, drafting, sending, status tracking, or related features.

16. Children's Privacy

Networker is not directed to children under 13, and we do not knowingly collect personal information from children under 13. If you believe a child has provided personal information to Networker, contact us so we can take appropriate steps. Users under 18 may use Networker only with appropriate permission and supervision where required by law.

17. International Users

Networker is operated from the United States. If you access Networker from outside the United States, your information may be processed in the United States and other jurisdictions where our service providers operate. Those jurisdictions may have data protection laws different from where you live.

18. Changes to This Privacy Policy

We may update this Privacy Policy from time to time. The updated version will be indicated by an updated effective date. If changes are material, we will provide notice as required by law. Your continued use of Networker after an updated Privacy Policy becomes effective means you acknowledge the updated policy.

19. Google and Microsoft OAuth Data Addendum

Google OAuth scope. When you sign in with Google, Networker requests openid, email, and profile permissions only. Networker uses Google access to identify the signed-in account, maintain the authenticated session, protect account security, comply with law, and carry out user-directed support. Networker does not request Gmail sender scopes, does not request <https://mail.google.com/>, and does not use Google access for outreach drafting or sending.

Google Limited Use. Networker's use and transfer to any other app of information received from Google APIs will adhere to the Google API Services User Data Policy, including the Limited Use requirements. Networker uses Google user data only to provide or improve prominent user-facing features in Networker, maintain security, prevent abuse, comply with law, or act on your direction. Networker does not transfer Google user data to advertising platforms, data brokers, information resellers, surveillance providers, or credit or lending decision-makers. Networker does not sell Google user data, use it for serving ads, use it for retargeting or personalized advertising, use it to determine credit-worthiness, or use it to train generalized AI or machine learning models.

Human access to Google user data is limited. Networker personnel, contractors, and service providers may access Google user data only with your affirmative permission for support, where necessary for security or abuse investigation, where necessary to comply with law, or where the data is aggregated and used for internal operations in accordance with applicable privacy requirements.

Microsoft OAuth and Microsoft Graph scopes. When you connect Microsoft Outlook or Microsoft 365 as a sender, Networker requests openid, email, profile, offline_access, User.Read, Mail.ReadWrite, and Mail.Send. User.Read identifies the signed-in Microsoft account and reads the profile information needed to connect the sender.

Mail.ReadWrite allows Networker to create, read, update, and delete messages in the signed-in user's mailbox and is used for draft creation, draft updates, draft and message metadata, send workflow status, troubleshooting, security, and user-directed actions. Mail.Send allows Networker to send outreach from the signed-in account when you approve, schedule, or direct sending. offline_access allows Networker to refresh access tokens so the integration can keep working until you disconnect it or revoke access.

Networker uses Microsoft email data only for connected sender features, workflow tracking, support, troubleshooting, security, legal compliance, and user-directed actions. Networker does not request Microsoft Graph application permissions to access all mailboxes in an organization, does not use Microsoft email data for advertising, data brokerage, surveillance, credit or lending decisions, or generalized AI model training, and does not disclose Microsoft email data except as needed to provide the requested integration, comply with law, protect security, or as you direct.

OAuth token storage, revocation, and deletion. Microsoft OAuth access tokens and refresh tokens are encrypted server-side and retained only while the Microsoft email sender remains connected or as otherwise necessary for security, troubleshooting, legal compliance, or account recovery. Campaign drafts, provider draft identifiers, provider message identifiers, send status, audit records, and workflow logs may be retained as described in this Privacy Policy. You may disconnect Microsoft in Networker settings, revoke Google sign-in access through your Google Account permissions, revoke Microsoft access through your Microsoft account or organization controls, or contact tanish@trynetworker.com to request access, correction, or deletion.

20. Contact

For privacy questions, data requests, or concerns, contact Networker at tanish@trynetworker.com. Please include enough information for us to understand and verify your request.