Bridgefolk privacy policy

Updated 1 November 2026. Bridgefolk for iOS and Android is provided by Lattice Labs Pte. Ltd., Singapore. Our developer name on Google Play is “Lattice Inc”.

Your account

We collect your chosen display name, unique username, avatar and a random player ID to identify you, let you sign in and show your profile to other players. You do not need to give your real name, email address or phone number. We do not access your address book.

Your six-digit PIN is sent over an encrypted connection for account creation, sign-in and PIN changes. The server stores only a salted hash of the PIN. Signed-in devices use separate random session credentials; the server stores their hashes. Sessions do not expire automatically. Signing out revokes that device's session. Deleting the account revokes all its sessions.

Games, friends and table chat

Cloudflare hosts our website, account service and online games. To run tables and reconnect players, the game service stores player IDs, display names, avatars, table membership, cards, bids, plays, results and table chat messages with sender details and times. Online traffic uses HTTPS and secure WebSockets. The service can read this data to run the game.

Players at your table see your display name, avatar, messages and public play. Each online player receives their own hand; dummy becomes public after the opening lead. Participants can review completed hands and keep them in their own history.

We store friendships, removed friendships, blocks, invitations, presence preferences, multiplayer ratings and rating history. These support friends, invitations, rankings and reconnection across devices. Friends can see your online or table status unless you turn it off in Settings. Players who share a table can become friends automatically; removing a friend prevents automatic re-adding.

We also store the streak count, last qualifying day and streak badge shared with friends. Daily Ten submissions include your player ID, day, board, contract, score and accuracy when available. These provide comparisons and rankings. Other players can see your profile and results in leaderboards. Your detailed streak calendar, learning progress and local game history do not sync through your account.

Block and Report

You can block a player or report a message from table chat where these controls are available in your app version. Blocking removes the friendship, hides your online status and last-seen time from each other, cancels pending invitations, and stops friend re-adding, invitations and nudges in both directions. It does not remove either player from a table, cancel the game or delete chat already shared. Hiding blocked players' chat requires support in your app version; older versions may still display their messages.

Blocks belong to your account and persist across sign-in and reinstalling the app. They have no automatic expiry. Unblocking does not restore the

friendship or old invitations. Deleting your account removes blocks you created; blocks other people placed against your player ID remain until they remove them or delete their accounts.

When you report, we store your account ID, the reported player's ID, reason, and device and server timestamps. We also store any explanation, message ID, message text or table code included in the report. We use these details to investigate abuse. Reports are stored on Cloudflare for review by authorised team members and are not shown to other players. Reporting does not automatically block a player. Reports have no automatic expiry and remain after either account is deleted.

You can also report chat or ask about deleting a report by emailing team@latticelabs.app. Include the player's username, the table code if available, and the message or a screenshot. Do not send your PIN or session credentials. Email reports include your email address. In-app reports are not automatically emailed to this address.

Nearby play and QR scanning

On iOS, nearby play uses Apple's MultipeerConnectivity over Bluetooth and Wi-Fi, with local network permission. Android uses Google Play services Nearby Connections over Bluetooth and Wi-Fi. Android 12 and below, including Android 12L, require location permission for discovery. We do not use that permission to determine your geographic location. Newer Android versions request Nearby devices permissions; Android 17 and later also request local network permission.

Nearby discovery advertises the table name, host's display name and avatar, game variant and available seats. Devices exchange player identities, seats, game state and chat. Current nearby connections are encrypted. The host can access the full game state and, when relaying an online connection, the relayed player's table credential and hand. Play nearby with people you trust. Current iOS and Android builds move a nearby table to Cloudflare only after the host explicitly chooses Play online before the first deal. Restoring internet never moves an active nearby deal. Older client versions may migrate automatically.

The camera is used when you choose Scan QR to add a friend. QR recognition runs on your device, using Apple's camera framework on iOS and CameraX with Google ML Kit on Android. Bridgefolk does not save or upload the camera frames. The decoded username is used to look up and add the friend. You can enter a username without using the camera.

Google's Nearby and ML Kit SDKs may send Google device and app information, installation or other device identifiers, usage, performance and diagnostic data. ML Kit telemetry can include image format and resolution, but not the camera images. This SDK telemetry is separate from our PostHog setting.

Optional completed nearby-deal verification

On iOS and Android, completed nearby deals can be copied to Cloudflare for verification. This is off by default. In Settings, enable “Copy completed nearby deals” on iOS or “Sync completed nearby deals” on Android. Cellular/mobile data is also off by default; enable “Use cellular data” on iOS or “Allow mobile data for sync” on Android to allow it. You must be signed in. iOS requires a usable, unconstrained network with the service reachable and uses background URLSession transfers and BGTask scheduling. Android requires a validated connection, unmetered unless mobile data is allowed, and uses WorkManager. The operating system may defer transfers. Moves, chat, acknowledgements and dealing stay on the nearby link.

The signed copy includes participant account IDs and key IDs, seats and bot flags, table and deal IDs, authority generation, board and game variant, shuffle commitments and revealed seeds, all dealt cards, accepted bids, plays and claims, contract, result and score. It includes a transcript hash, the host signature and every human participant’s co-signature. Public

device keys and a signed proof of possession are sent separately to register a key with your account. PINs and session credentials are not in the transcript; requests use your account's session credential for authentication.

Devices generate P-256 signing keys. On iOS the private key uses Secure Enclave when available, with its stored representation in device-only Keychain; otherwise the private key is stored in device-only Keychain. Android uses non-exportable Android Keystore keys, trying StrongBox first where available and falling back to the normal Keystore. Hardware protection depends on the device. Private keys are never uploaded. Registered keys are bound to that account incarnation, so a recreated account cannot reuse an old key's registration proof.

Each human device checks the completed transcript against its saved shuffle commitments, original hand and observed moves before co-signing. The server checks registered keys, signatures, the committed shuffle, legal play, result and score. This verifies the signed record, not physical proximity, who tapped each move, honest play or the bot's strategy. Uploads

require all human seats to have accounts and co-signatures. At least two distinct co-signing accounts and a non-passed-out result allow ratings to change; one-account and passed-out deals provide verified history and statistics only.

Another participant can upload the shared signed deal even when your own setting is off. The setting controls transfers from this device; turning it off does not remove an accepted copy or undo ratings. Signing out keeps pending copies for later sign-in. The local queue database and saved observations are excluded from backups; other app files may be backed up. Local replay history remains on the device.

Full signed deals and private server history expire seven days after first acceptance. Reads and retries do not extend that period. Lifetime verified/rated deal counts remain until account deletion. Account deletion removes registered public keys, private nearby history, counts and throttle records. Other original participants can read a previously uploaded shared deal until its seven-day expiry and keep their own local copies or exports. Deletion removes your ratings and rating history; it does not reverse other players' rating history.

Permanent anti-replay records retain transcript hashes, hashed table/generation/deal identities, one-way participant account-incarnation fingerprints and whether rating was applied. Key-owner tombstones retain a public-key hash and one-way account-incarnation fingerprint. These records prevent duplicate scoring and reuse of old key proofs. They contain no full transcript, score, result or device public key. Successful in-app erasure removes this device's nearby signing keys, outbox, observations and cached nearby history along with local games and settings.

Product analytics and crash reports

Release builds on both platforms use PostHog, hosted in the US, to understand use and fix faults. We send events such as screen visits, game and Daily Ten results, streak changes, lesson and practice activity, friend and table actions, and use of chat. Crash reports include exception types and stack traces. Exception messages and breadcrumbs are removed.

Events are tied to your random player ID, which can be linked to your account. They are not anonymous. PostHog also receives installation and session

identifiers, device model, operating system, app version and network information such as your IP address. We disable IP-based location enrichment, session replay and automatic interaction capture. We do not add your display name, username, PIN, credentials, chat text or card contents to analytics events.

Sharing is on by default. On either platform, open Settings using the avatar and gear button on the home screen, then turn off “Share anonymous usage analytics”. This stops subsequent PostHog collection on that device, including crash reporting. It does not delete earlier data or control Google or Apple diagnostics. Your choice is saved on the device. A fresh Android install or backup restore returns this setting to its default. Debug and automated test builds do not send PostHog analytics.

We have no adverts, do not use an advertising ID, and do not sell personal data or share it for advertising.

Notifications, local storage and backups

With permission on iOS, we store your Apple Push Notification service (APNs) token and notification preference to send friend nudges. The notification includes the sender's display name. You can turn nudges off in Settings or disable notifications in iOS settings. Android does not currently register a push token or receive friend push notifications. Daily Ten reminders are scheduled locally on both platforms.

Games, history, settings, learning and practice progress, and detailed streak records stay in the app's storage on your device. They can include other players' names and IDs. History remains until you remove it or it reaches the app's history limit. Exports can include names, cards, bids, plays and results; the recipient you choose receives the file.

On iOS, session and table credentials are stored in Keychain. Keychain data can survive uninstalling the app. Local app data may be included in iCloud or computer backups, depending on your settings.

On Android, credentials are encrypted using Android Keystore and stored outside backups. Only the app's

local game, history, settings, learning, practice and streak files are allowed in backups and device transfers. Account caches, shared preferences, analytics identifiers and queues are excluded. Restoring a backup does not restore a signed-in session. Backup availability depends on your device and provider settings. Android 12 and later require encryption capabilities for cloud backup.

Retention and account deletion

Your account remains until deleted. Delete your Bridgefolk account explains the in-app steps and how to request deletion by email without the app. Successful in-app deletion removes the online profile, username, PIN hash, active sessions, friendships, blocks you created, invitations, push token, shared streak, multiplayer ratings and your rating history. It also erases local game data and settings on that device.

In-app deletion does not erase PostHog data. To delete your PostHog person profile and events, email team@latticelabs.app with your Bridgefolk username before erasing the account. Wait for us to confirm

analytics deletion. We need the existing account to match your username to the player ID used for analytics; a former username alone cannot reliably identify those records after account deletion. Do not send your PIN. You can also request deletion of both analytics and the online account by email without the app. We use the username to locate the account and its analytics records, handle analytics deletion first, then delete the online account and confirm completion. We may need more information to verify the request; never send credentials. Turning analytics off does not erase earlier events. PostHog data otherwise follows our project's retention settings; there is no automatic expiry set by the app.

Table records, including game state and chat, expire after seven days without a retention-extending game action or seat change. Continued play can extend this period. Chat and reconnection alone do not extend it. Account deletion does not immediately erase these shared table records. Daily Ten submissions remain until 32 days after midnight UTC at the start of the relevant game day; deleted accounts are removed from public rankings immediately.

Invitations expire after ten minutes. Nudge cooldown records expire after 15 minutes and are removed during subsequent server housekeeping. We retain the deleted account's random ID and revoked credential hashes without automatic expiry to reject old credentials. These are session credential hashes, not the PIN hash. Rating event IDs and one-way event fingerprints also remain without automatic expiry to prevent duplicate scoring. Other players' rating history is not undone.

In-app deletion does not remove other devices' local data, recipients' exports or existing backups. Anonymised aggregate statistics may remain. Server logs are kept for up to 30 days. Google and Apple SDK records follow their providers' retention policies; the app's table expiry does not apply to them. Contact us about earlier deletion of table data, analytics, support correspondence or abuse reports. Include the table code where relevant, never credentials.

Service providers and support

Cloudflare processes hosting, account and online game data for us. PostHog processes product analytics and crash reports. Apple provides iOS networking, camera, Keychain, backups, APNs, the App Store and TestFlight. Google provides Android services, Nearby Connections, ML Kit and Google Play. Providers may process data outside Singapore or your home country. Their policies explain their own processing: Cloudflare, PostHog, Apple and Google.

Apple and Google may provide store, testing and diagnostic information according to your settings and their services. TestFlight can share crash logs, device details and feedback or screenshots you submit. We use these to fix problems. If you email support, we receive your email address, message and attachments and use them to answer your request. Contact us to ask for access, correction or deletion of your data.

Children and earlier versions

Bridgefolk is for people aged 13 and over. It is not directed at children under 13. If you believe a child under 13 has provided personal data, contact us so we can investigate and delete it.

Older versions may lack the features described here. The contract-only iOS version 1.0 (build 2) had no online accounts or analytics and used unencrypted nearby connections. Its behaviour is described in the 18 October policy. The 30 October policy covers the previous public version. We update this policy when our handling of data changes.

Contact

Lattice Labs Pte. Ltd., 51 Penjuru Road, #4-00, Singapore 609143. Google Play developer name: Lattice Inc. Email team@latticelabs.app.