Patchwork

Privacy Policy

Last updated: 10 June 2026

Your privacy matters deeply to us. Patchwork is built around the principle that your system data belongs to you — not to us. This Privacy Policy explains what data we collect, why, and how we protect it. This policy applies to the Patchwork web application and the website patchwork.work.

1. Definitions

The following terms are used throughout this document:

- **"Faen Laud"** refers to Niles McCrystal, the individual developer and operator of Patchwork, operating under the trading name Faen Laud. Faen Laud is the data controller for the purposes of applicable data protection law. Where this policy refers to "we", "us", or "our", this means Faen Laud.
- **"Patchwork"** refers to the web application and associated server infrastructure developed and operated by Faen Laud.
- **"You"** or **"User"** refers to any person who accesses or uses Patchwork.

2. Who We Are

Patchwork is developed and operated by Faen Laud. For privacy enquiries, contact: **legal@patchwork.work**

3. Our Core Privacy Principles

- **Encrypted-first:** Your system data (members, fronting history, categories) is encrypted on your device before it ever leaves it. The server stores and routes only sealed, encrypted blobs it cannot read.
- **Minimal server data:** The server stores only what is strictly necessary to provide backup, sync, and friend-notification features.
- **End-to-end encryption:** Content shared between users is encrypted so we cannot read it.
- **No telemetry:** We do not collect analytics, crash reports, or usage statistics.
- **No advertising:** Patchwork is free and contains no ads. We do not sell or share your data for commercial purposes.

4. What Data We Collect and Why

4.1 Encrypted backup data stored on our server

To support syncing across devices and data recovery, Patchwork continuously uploads an encrypted backup of your full system to our server. This backup contains:

- System member profiles (names, pronouns, custom fields)
- Fronting history and session logs
- Category structure

This data is encrypted on your device using AES-256-GCM before upload. We cannot read, access, or decode it. The server stores it as an opaque encrypted blob and returns it to you on sign-in so your data is available across devices.

4.2 Encrypted member records stored on our server

Individual member records are also pushed to the server as encrypted blobs, identified only by a SHA-256 digest of the member's internal ID. We cannot link these records to real identities or read their contents.

4.3 Account and routing data stored on our server

We store the following minimal account data on the Patchwork server:

- Your user ID (derived from your Discord identity via Logto)
- Your RSA public key (so your friends can encrypt messages to you)
- Your friend associations (which user IDs you are connected with, for message routing)
- Encrypted fronting notifications: temporarily stored as ciphertext until you fetch them. We cannot read these.

We do not store your email address, your Discord username, your system name, or any unencrypted member information.

4.4 Web Push subscription data

If you enable notifications, your browser's Web Push subscription — comprising the push endpoint URL and cryptographic keys issued by your browser — is sent to our server. This is used solely to deliver fronting notifications from your friends. You can unsubscribe at any time via your browser or by signing out.

4.5 Data processed during sign-in

When you sign in with Discord via Logto OIDC, the following occurs:

- Discord shares your basic profile (username and avatar) with the app to authenticate you.
- Logto processes your Discord user ID and issues a JWT token for Patchwork.
- Patchwork receives only the token. We do not store your Discord username or avatar.

Your Discord user ID is used as the basis for deriving your AES backup key (via PBKDF2). This derivation happens entirely on your device; the raw Discord ID is never sent to us.

4.6 Website (patchwork.work)

The patchwork.work website is a static informational site. We do not use tracking cookies, advertising networks, or analytics tools on the website.

4.7 Data that stays on your device only

The following data is held in your browser's local storage (IndexedDB) and is never sent to us in unencrypted form:

- Your RSA private key (generated locally on first sign-in; never transmitted)
- Your AES encryption key (derived locally; never transmitted)
- App settings and preferences

- Your PluralKit API token (stored encrypted; cannot be read back)

5. Legal Bases for Processing

Where data protection law (such as UK GDPR or EU GDPR) requires us to identify a legal basis for processing, we rely on:

- **Contractual necessity:** processing your user ID, public key, and encrypted backups is necessary to provide the sync and friend messaging features you request.
- **Legitimate interests:** storing friend associations and Web Push subscriptions is necessary for message routing and notification delivery, and represents a minimal, proportionate use of data.

6. Your Rights

Depending on where you live, you may have the following rights regarding your data:

- **Access:** request a copy of the data we hold about you.
- **Deletion:** delete your account and all associated server-side data via Settings → Delete Account. This removes your public key, encrypted backup, friend associations, push subscriptions, and any pending encrypted messages from our server.
- **Correction:** if you believe any server-stored data about you is inaccurate, contact us.
- **Portability:** your local data is already under your full control inside your browser's IndexedDB. You can export or delete it at any time.

Because your system data is encrypted before it reaches us, we are unable to read, provide access to, or modify its contents on your behalf. To exercise any of these rights, contact us at: **legal@patchwork.work**

7. Data Retention

We retain server-side data (your user ID, public key, encrypted backup, and friend associations) for as long as your account exists. Encrypted fronting notifications are stored temporarily and deleted once delivered. Web Push subscriptions are retained until you unsubscribe or delete your account. When you delete your account via Settings → Delete Account, all server-side data is permanently removed.

8. Security

Your system data is encrypted on your device using AES-256-GCM with a key derived from your Discord ID via PBKDF2 (200,000 iterations) before being uploaded. Content shared between users uses hybrid encryption: RSA-OAEP-2048 key encapsulation with AES-256-GCM payload encryption. Your private RSA key and AES key never leave your device.

The server stores and routes only sealed, encrypted blobs that it cannot open. While we take security seriously, no system is perfectly secure. We cannot guarantee absolute security.

9. Children

Patchwork does not have a minimum age requirement. We do not knowingly collect additional personal data from children beyond what is described in this policy. If you believe a child's data has

been shared with us inappropriately, please contact us.

10. International Transfers

Patchwork's server infrastructure may be hosted in various locations. By using Patchwork, you acknowledge that your server-side data (user ID, public key, encrypted backups, friend associations, push subscriptions) may be stored and processed in countries other than your own. We take steps to ensure that any such transfers are conducted with appropriate protections in place.

11. Third-Party Services

Discord (discord.com) and Logto act as third-party processors during authentication. Their own privacy policies govern how they handle your data. We encourage you to review them.

12. Changes to This Policy

We may update this Privacy Policy from time to time. We will update the "Last updated" date when we do. Continued use of Patchwork after changes are posted means you accept the updated policy.

13. Contact

For any privacy-related questions or requests, please contact: **legal@patchwork.work**
