TRUST & SAFETY

Security, Privacy & Data Protection.

Last updated: June 15, 2026 · 10thmuses.com/security

10th Muses serves a community with a real interest in discretion and safety. This document describes, in concrete terms, how the platform is built and operated to protect member identity and data — how we verify who joins, how access is restricted, how information is stored and retained, the service providers involved, and the member controls and legal posture that govern it all. It is maintained alongside the system it describes and updated when our practices change.

1. Scope and principles

This document covers the 10thmuses.com web application, its backend services, and the third-party providers that support them. Our practices are organized around four principles:

- **Data minimization** — we collect only what membership and safety require, and decline data we do not need.
- **Least privilege** — every actor, whether a member, an administrator, or an automated job, can reach only the data its role requires.
- **Verifiable identity, not surveillance** — we confirm members are real, unique people without building a facial-recognition or identity-tracking apparatus.
- **Member control** — members can view, correct, hide, export, and permanently delete their data.

2. Information we collect — and what we deliberately do not

To join, we require a name, a verified email address, a verified phone number, a date of birth (used to confirm members are adults), a neighborhood or address, a profile photo, and a one-time identity verification (see Section 4).

Members may optionally provide pronouns, a bio, interests, education, industry and role, social handles, and matchmaking preferences. These are supplied at the member's discretion and can be edited or removed at any time.

We deliberately do not do the following:

- We do not request, store, or scan government identification.
- We do not require a legal name to attend events.
- We do not run one-to-many facial recognition and do not match member faces against any external or surveillance database. Verification is a one-to-one check against the member's own enrollment photo, and the facial scan is deleted immediately afterward (see Section 4).
- We do not sell member data, and we do not share member lists with anyone outside the team operating 10th Muses.
- We do not store payment card numbers — payments are handled entirely by Stripe (see Section 6).

3. Identity and access control

Accounts are managed through Supabase Auth, and each member's application identity is bound one-to-one to their authenticated account, which prevents account confusion or impersonation across the system.

Both email and phone are confirmed with one-time codes during onboarding. Returning members sign in with a single-use, time-limited link rather than a stored password.

Access to member data is enforced at the database layer through Row-Level Security, not in the application alone. Database policies ensure a member can read and modify only their own record, plus the limited, opt-in directory fields other members are permitted to see. These policies are audited and version-controlled.

Administrative functions require separately granted privileges and are isolated from member-facing access paths. Privileged service credentials are never exposed to the browser.

4. Identity verification

Membership requires a one-time liveness verification at signup, provided by Amazon Rekognition. Liveness detection confirms a live person is present at enrollment — not a photo, video, or synthetic image — and a one-to-one comparison matches that capture against the member's own submitted profile photo to confirm they are the same person.

This is identity assurance, not surveillance. We do not search faces against any external database, watchlist, or other members. The image captured during the check is held only transiently to complete the one-to-one comparison and is then deleted; we do not retain biometric facial data afterward, and it is never used to identify a member later.

A member becomes active only after every required gate is met — waiver accepted, email and phone verified, liveness passed, and profile complete — and this is enforced by a database-level guardrail, not by application code alone.

5. Data protection in transit and at rest

All traffic is served over HTTPS/TLS, and HTTP Strict Transport Security (HSTS) is enforced with preload, so browsers refuse insecure connections. Member data in the primary database and files in object storage are encrypted at rest by our infrastructure providers using industry-standard, AES-256-class encryption.

In the browser, a strict Content-Security-Policy restricts what code and resources the site may load and reports violations back to us in real time. We additionally enforce X-Frame-Options (clickjacking protection), X-Content-Type-Options, a restrictive Referrer-Policy, and a Permissions-Policy that limits device access such as camera and microphone to first-party use only.

All credentials and API keys are held as server-side environment secrets and are never committed to source control. Our continuous-integration pipeline fails the build if a secret or hardcoded token is detected.

6. Service providers

We rely on a small set of established providers, each receiving only the data needed for its function. We do not sell data to any of them.

- **Supabase** — primary database and authentication (profile data, credentials).
- **Cloudflare** — image storage and delivery for active member photos, and bot/abuse prevention at signup.
- **Amazon Web Services** — one-time identity (liveness) verification.
- **Twilio** — SMS verification codes and notifications (phone number).
- **Resend** — transactional email such as codes and account notices (email address, name).
- **Mailchimp** — opt-in newsletter and event announcements (email, name).
- **Stripe** — event ticketing and payments; card details are held by Stripe and never by us.
- **Sentry** — error monitoring, with personal data minimized or redacted.

We also use privacy-respecting analytics to understand which pages work, and AI-assisted tooling to support photo review at signup; neither is used for advertising or sold to third parties.

7. Data retention and deletion

Profile data is retained while an account is active. A member may request deletion at any time: the account is hidden immediately and enters a seven-day grace period during which the request can be cancelled. After seven days, an automated job permanently removes the member's record and all associated content — messages, matches, tickets, RSVPs, and notifications — and deletes the underlying authentication record so the account cannot be resurrected. The deletion is logged as a tamper-evident audit entry containing only a one-way hash of the email; no readable personal data is retained.

Incomplete signups are automatically swept and removed after a short window. Identity-verification captures are deleted immediately after the one-to-one comparison completes. When a member opts out of SMS, a minimal do-not-contact record is intentionally retained so the opt-out is honored permanently — this is the only personal datum kept after deletion, and it exists solely to respect the member's choice. Payment and tax records held by our payment processor are retained as required by law, independent of profile deletion.

8. Member privacy controls

The member directory is gated to verified, active members only and is never public; each member can hide their own profile from the directory at any time. Members can review and correct their information and request a copy of their data.

Marketing and newsletter email is opt-in and every message carries an unsubscribe link. SMS is opt-in at signup and can be stopped at any time by replying STOP. Transactional messages — verification codes and account or security notices — are limited to what is operationally necessary.

9. Application and operational security

Authorization rules live in the database through Row-Level Security, so a bug in the application cannot silently expose data it should not. Sign-in and verification endpoints are rate-limited and lock out after repeated failures, and signup is protected by a privacy-preserving bot challenge and a disposable-email blocklist.

Every change runs through automated security linting with repository-specific rules drawn from real incidents, plus automated code review, before it ships. Each deployment must pass build, security, and secret-scanning checks; the build fails on any policy violation.

10. Monitoring and incident response

Application and database errors, and security-policy violations, are captured centrally with personal data minimized or hashed. Database logs are polled on a short interval, and defined critical patterns — for example permission errors or integrity violations — page an operator automatically. Synthetic health checks run daily against core systems and alert on failure.

When an issue is detected it is triaged against this telemetry, root-caused, and fixed forward, with verification that the fix holds.

11. Regulatory and legal compliance

The platform is for members eighteen and older; date of birth is verified at signup, and we do not knowingly collect data from minors, consistent with the Children's Online Privacy Protection Act (COPPA).

We comply with the California Consumer Privacy Act (CCPA/CPRA) and the General Data Protection Regulation (GDPR): members may request access to, correction of, and deletion of their data, and may opt out of marketing communications and of the sale of personal information, which we do not engage in.

SMS is sent only to members who have given express consent, with timestamped consent records and a permanent opt-out mechanism, consistent with the Telephone Consumer Protection Act (TCPA). Card data is processed entirely by Stripe, a PCI-DSS Level 1 provider, so 10th Muses never receives or stores card numbers.

Our infrastructure is United States–based. We disclose member data only where legally compelled, and we maintain a warrant canary on our privacy page.

12. Reporting a concern

Security or privacy concerns can be reported to abh@10thmuses.com. We acknowledge reports promptly and investigate every credible report of a vulnerability or data concern.