

Dating App MVP

Comparable to: Tinder / Bumble

A lean consumer dating marketplace MVP for a broad adult audience. Members discover nearby profiles through swipe-based matching and chat after a mutual match.

Estimated MVP cost

\$21,300

Estimated effort

377 hours

To get your own customised cost for an app like this, visit www.chatstack.app and start a ChatStack interview describing how you want it customised.

Key Features

- Account creation, onboarding, and dating profiles with relationship-intent labels.
- Discovery based on current location, member-selected age range, and a selected distance radius.
- Swipe-based discovery, mutual matching, and one-to-one messaging immediately available to either matched member.
- Photo selfie profile verification.
- In-app blocking and reporting with admin review.

Out of Scope for This MVP

- US hosting, payments, and legal compliance.
- App-store compliance, privacy protections, and in-app account deletion.
- English-only launch.
- Nationwide launch supported by early marketing and waitlists.
- The app is a consumer marketplace MVP inspired by established swipe-based dating apps.
- Relationship intent is shown on profiles but is not a launch discovery filter.
- A broad nationwide launch may require deliberate early member acquisition to maintain profile availability.

Full Cost Breakdown

Item	Hours	Cost
The system shall allow adult visitors in the United States to create an account using supported registration credentials and shall complete age screening before account activation.	6	\$330
The system shall require users to accept applicable community terms and acknowledge required privacy disclosures during account creation.	4	\$220
The system shall allow logged-in users to create and edit a dating profile containing photos, personal details, relationship intent, and other configured profile attributes.	12	\$660
The system shall allow logged-in users to submit a selfie for profile verification and shall display the resulting verification status where applicable.	15	\$830
The system shall present nearby dating profiles based on the user's selected age range and distance radius.	14	\$770
The system shall provide a swipe-based interaction allowing users to express interest in or pass on discovered profiles.	7	\$390
The system shall create a match only when two members have mutually expressed interest and shall make the match visible to both members.	8	\$440
The system shall allow either member of a match to exchange one-to-one text messages with the other member.	16	\$880
The system shall allow a logged-in user to block another member and shall prevent further direct interaction and relevant discovery exposure between them.	8	\$440
The system shall allow users to report a profile, photo, or message with sufficient information for service administrators to review the safety concern.	9	\$500

The system shall provide service administrators with a safety-report review workflow to review, dismiss, or act on reports, including content removal and account suspension or banning.	19	\$1,050
The system shall allow logged-in users to initiate account deletion from within the app and shall remove user-facing profile data and photos immediately after deletion is confirmed.	14	\$770
The service shall provide an external account and data deletion request path required for Android distribution.	6	\$330
The system shall optionally send push notifications for relevant matches and messages when the user grants notification permission.	10	\$550
The system shall require explicit opt-in before sending promotional notifications and shall provide a user-accessible opt-out control.	6	\$330
The application shall comply with applicable Apple App Store and Google Play requirements, including user-generated-content, safety, privacy, and account-deletion policies.	9	\$500
Planning	41	\$2,260
Project Management	33	\$1,820
Testing	20	\$1,100
DevOps	16	\$880
Design & Frontend Build	49	\$2,700
AI Tokens	0	\$540
Security	20	\$1,100
Risk (10% Contingency)	35	\$1,930
Total	377	\$21,300

Estimate Assumptions

- Estimates cover base development for the specified requirements and exclude NFR overhead, project management, design discovery, and formal release operations.
- Supabase Auth, PostgreSQL, object storage, and row-level security are available and used

without
major
custom infra
structure.

- Selfie
verification
provider
selection,
liveness
detection,
biometric
processing,
and
provider-
specific
compliance
are not
included
beyond
integration-
ready
workflow
support.

- Push notif
ications
use
OneSignal
and
Firebase
Cloud
Messaging
or an
equivalent
approved
setup.

- Messaging
uses text-
only
delivery
without atta
chments,
voice,
video,
encryption
beyond
platform
transport,
or
advanced
search.

-

Moderation is primarily administrative-driven; automated content moderation, identity verification automation, and dedicated safety operations are excluded.

- The external deletion request path is a web form or equivalent lightweight service flow connected to the existing deletion process.

- The application supports agreed iOS and Android versions and uses standard device capabilities for camera, location, photo upload, and push notifications.

Risks That

Could Change This

- Selfie verification provider, liveness requirements, and biometric-data handling could materially increase implementation and compliance effort.

- Geospatial discovery performance and privacy behavior may require specialized indexing or location services beyond the assumed Supabase capabilities.

- Real-time messaging, notification delivery, moderation response times, and app-store policy reviews may require additional iteration.

- Account deletion and

retained
safety
records
require
legal and
privacy-
policy
decisions
that may
change
data
models and
workflows.

User Stories

US-1 - Visitor

As a visitor,
I want to
create an
account so
that I can
use the
dating
service.

US-2 - Logged In App User

As a
logged-in
app user, I
want to
complete a
dating
profile with
photos,
personal
details, and
relationship
intent so
that other
members
can
understand
who I am
and what I
am seeking.

US-3 - Logged In App User

As a
logged-in

app user, I want to verify my profile with a selfie so that other members can have greater confidence that my profile is authentic.

**US-4 -
Logged In
App User**

As a logged-in app user, I want to discover nearby dating profiles using my selected age range and distance radius so that I can find relevant members in my area.

**US-5 -
Logged In
App User**

As a logged-in app user, I want to express interest in or pass on discovered profiles so that I can control which potential matches I pursue.

US-6 - Logged In App User

As a logged-in app user, I want to see when another member and I have mutually expressed interest so that I know when a connection is available.

US-7 - Matched Member

As a matched member, I want to exchange one-to-one messages with my match so that we can communicate and decide whether to continue the connection.

US-8 - Logged In App User

As a logged-in app user, I want to block another member so that I can stop unwanted interactions and reduce future contact with that member.

US-9 - Logged In App User

As a logged-in app user, I want to report a profile, photo, or message so that the service can review potentially unsafe or prohibited behavior.

US-10 - Service Administrator

As a service administrator, I want to review submitted safety reports so that I can take appropriate action to protect members and maintain community standards.

US-11 - Logged In App User

As a logged-in app user, I want to delete my account from within the app so that I can leave the service and control what happens to my associated data.

US-12 - Logged In App User

As a logged-in app user, I want to receive relevant notifications about matches and messages so that I can respond without continuously checking the app.

Requirements

FR-1 - Account Registration

The system shall allow adult visitors in the United States to create an account using supported registration credentials and shall complete age screening before account activation.

FR-2 - Terms and Privacy Consent

The system shall require users to accept applicable community terms and acknowledge required privacy disclosures during account creation.

FR-3 - Profile Management

The system shall allow logged-in users to create and edit a dating profile containing photos, personal details, relationship intent, and other configured profile attributes.

FR-4 - Profile Verification

The system shall allow logged-in users to submit a selfie for profile verification and shall display the resulting verification status where applicable.

FR-5 - Discovery

The system shall present nearby dating profiles based on the user's selected age range and distance radius.

FR-6 - Interest and Pass

The system shall provide a swipe-based interaction allowing users to express interest in or pass on discovered profiles.

FR-7 - Matching

The system shall create a match only when two members have mutually expressed interest and shall make the match visible to both members.

FR-8 - Messaging

The system shall allow either member of a match to exchange one-to-one text messages with the other member.

FR-9 - Blocking

The system shall allow a logged-in user to block another member and shall prevent further direct interaction and relevant discovery exposure between them.

FR-10 - Safety Reporting

The system shall allow users to report a profile, photo, or message with sufficient information for service administrators to review the safety concern.

FR-11 - Moderation Administration

The system shall provide service administrators with a safety-report review workflow to review, dismiss, or act on reports, including content removal and account suspension or banning.

FR-12 - Account Deletion

The system shall allow logged-in users to initiate account deletion from within the app and shall remove user-facing profile data and photos immediately after deletion is confirmed.

FR-13 - External Deletion Requests

The service shall provide an external account and data deletion request path required for Android distribution.

FR-14 - Notifications

The system shall optionally send push notifications for relevant matches and messages when the user grants notification permission.

FR-15 - Promotional Notifications

The system shall require explicit opt-in before sending promotional notifications and shall provide a user-accessible opt-out control.

FR-16 - App Store Distribution

The application shall comply with applicable Apple App Store and Google Play requirements, including user-generated-content, safety, privacy, and account-deletion policies.

NFR-1 - Performance

The system should target API response times below 200 milliseconds for normal application requests under agreed baseline load.

NFR-2 - Scalability

The system shall use a managed database architecture capable of scaling with MVP user, profile, messaging, media, and moderation workloads.

NFR-3 - Security and Access Control

The system shall enforce authenticated access, role-based administrator permissions, least-privilege access to verification data, and protection of personal, location, message, and report data.

NFR-4 - Privacy and Data Retention

The system shall document collection, use, sharing, retention, deletion, and access controls for profile, location, selfie-verification, messaging, notification-token, and safety-report data.

NFR-5 - Content Safety

The system shall support controls for objectionable content, user-generated-content reporting, moderation actions, blocking, enforcement, and prevention of prohibited interactions.

NFR-6 - Reliability and Data Integrity

The system shall preserve consistent account, match, message, block, report, moderation, consent, and deletion states across supported client sessions.

NFR-7 - Observability

The system shall provide application performance monitoring, error logging, operational metrics, and audit visibility for security and moderation actions.

NFR-8 - Usability and Accessibility

The mobile application shall provide clear, understandable flows for registration, consent, profile management, discovery, messaging, reporting, blocking, notifications, and account deletion.

NFR-9 - Platform Compatibility

The application shall support the agreed iOS and Android versions and device capabilities required for location, camera-based selfie verification, push notifications, and photo upload.

Requirements Assumptions

- The MVP is a free consumer dating service with no subscriptions, boosts, digital purchases, advertising, or external integrations specified.
- The service is initially English-only and available to adults located in the United States.
- Email, password, social login, and identity-provider choices are not specified and remain implementation decisions.

- Supabase is assumed for managed database and backend services; storage, authentication, and edge-function scope require estimation.
- Firebase Performance Monitoring is assumed for application performance monitoring.
- Location permission is optional for general app access and is requested only when needed for nearby discovery.
- Selfie verification uses a third-party or internally selected verification approach; provider, liveness checks, and biometric processing scope are not specified.
- Photos and messages are text and image user-generated content; automated moderation tooling, escalation rules, and service-level targets are not specified.
- Administrator access is provided through a secured administrative interface with role-based permissions.
- Account deletion removes user-facing profile data and photos immediately, while legally or safety-required records may be retained under a documented retention policy.
- Push notifications require user permission; promotional notifications require separate explicit opt-in and opt-out handling.
- No payment processing, analytics integrations, CRM, email service, maps provider, identity provider, or moderation vendor is included unless later approved.
- Exact performance percentiles, availability targets, supported OS versions, capacity targets, and disaster-recovery objectives require definition during estimation.
- App-store policy requirements are treated as delivery constraints, including user-generated-content safety and account-deletion compliance.

Technical Specification

TS-1 - Mobile Application

Build the iOS and Android applications with Flutter and Dart, using Riverpod for state management and Material Design 3 for the UI system.

TS-2 - Web and Administration

Build the service website and secured administrator panel with Next.js, React, TypeScript, Shadcn/ui, and Tailwind CSS.

TS-3 - Authentication

Use Supabase Auth with JWT tokens for account registration, login, session management, age-screening gates, and consent-version recording.

TS-4 - Authorization and RBAC

Enforce authenticated access, member permissions, administrator roles, least-privilege verification-data access, and database row-level security where applicable.

TS-5 - Backend and APIs

Use Supabase-managed backend services with PostgreSQL, REST APIs over HTTPS, and optional edge functions for transactional or privileged workflows.

TS-6 - Data Storage

Store accounts, profiles, preferences, interests, matches, messages, blocks, reports, moderation actions, consents, and notification preferences in managed PostgreSQL.

TS-7 - Location and Discovery

Support optional device location or manually supplied location, age-range and distance-radius discovery, and privacy-conscious location handling.

TS-8 - Verification and User-Generated Content

Support selfie submission, verification-status display, photo and message content controls, reporting, blocking, moderation, and restricted verification-data access.

TS-9 - Messaging and Notifications

Provide matched-member text messaging and optional push notifications using OneSignal and Firebase Cloud Messaging, with separate promotional opt-in controls.

TS-10 - Safety Administration

Provide an administrator workflow for reviewing, dismissing, escalating, removing content, suspending accounts,

banning accounts, and recording safety actions.

TS-11 - Hosting and Distribution

Host web and administrator applications on Vercel and use Supabase managed services for backend infrastructure; distribute mobile applications through Apple and Google stores.

TS-12 - Environments and CI/CD

Maintain separate development, staging, and production environments with environment-specific secrets, database configuration, migrations, and controlled promotion.

TS-13 - Security and Privacy

Use TLS 1.2+ for APIs, encrypted storage and transport, secure token handling, secret management, access logging, and documented retention and deletion policies.

TS-14 - Observability and Reliability

Provide performance monitoring, crash reporting, structured application logs, operational metrics, alerting, and audit trails for security and moderation actions.

TS-15 - Testing and Quality

Implement unit, integration, API, security, and end-to-end tests covering core mobile, backend, administration, moderation, notification, and deletion workflows.

Technical Assumptions

- The MVP is a free, English-only dating service for adults in the United States with no payments, subscriptions, advertising, or external integrations.
- Flutter/Dart, Riverpod, Material Design 3, Next.js, React, TypeScript, Shadcn/ui, and Tailwind CSS are the default frontend technologies.
- Supabase PostgreSQL, Supabase Auth, REST APIs, and optional edge functions are the default backend approach.
- Vercel hosts web properties, GitHub Actions manages deployment pipelines, and CodeMagic supports mobile build and store delivery workflows.
- Selfie verification may use a third-party provider or selected internal implementation; biometric processing, liveness, and provider scope are not yet defined.
- Profile photos, selfie assets, messages, reports, and other user-generated content require object storage, access policies, moderation controls, and retention rules.
- Account deletion removes user-facing profile data and photos immediately; safety, legal, report, consent, and verification records may be retained under documented policy.
- Exact supported iOS and Android versions, device capabilities, capacity targets, performance percentiles, availability objectives, and disaster-recovery targets require estimation.
- Push notifications use OneSignal and Firebase Cloud Messaging or an equivalent approved configuration; promotional messaging requires separate explicit opt-in.
- The product requires HTTPS, encryption, secure token handling, least-privilege access, auditability, and applicable privacy and app-store compliance.

To get your own customised cost for an app like this, visit <https://www.chatstack.app> and start a ChatStack interview.

This is a starting estimate for a custom-built MVP, designed and built from scratch. You own all the code and IP with no platform lock-in. Tinder / Bumble are trademarks of their respective owners; ChatStack / App Developer Studio is not affiliated with, endorsed by, or sponsored by Tinder / Bumble. © 2026 ChatStack.

Created with ChatStack (www.chatstack.app)