ClearPath RD

clearpathrd.com

API Specification

Version 1.0 — February 2026 — Confidential

What this document covers

- Prisma schema — complete schema.prisma for PostgreSQL / Supabase
- OpenAPI 3.1 YAML — machine-readable, works with Swagger UI, Postman, and code generators
- 35 REST endpoints across 10 groups: Auth, Homes, Kit Orders, Test Sessions, Results, Certificates, Contractors, Referral Codes, Webhooks, Admin
- Request / response schemas with field types, nullability, and business rule annotations
- HTTP status codes and the standard error envelope format
- Authentication model — Supabase Auth JWT Bearer tokens
- Webhook handling — Stripe (payment events) and Resend (email delivery events)

Stack

Node.js + Fastify · Prisma ORM · PostgreSQL (Supabase) · Supabase Auth · Stripe · Resend · Railway

1. Overview

Base URL for all endpoints:

```
https://api.clearpathrd.com/api/v1
```

> *All endpoints except /auth/register, /auth/login, /auth/password-reset, GET /contractors, and GET /verify/:id require a Supabase Auth JWT Bearer token in the Authorization header.*

1.1 Authentication

ClearPath RD uses Supabase Auth for identity. The Fastify server validates the Supabase JWT on every protected route. The sub claim in the token is the user UUID and is used to scope all database queries.

- POST /auth/register → Supabase creates auth record + app creates users row + verification email sent
- POST /auth/login → returns { accessToken, refreshToken, expiresIn }
- Client sends Authorization: Bearer <accessToken> on protected requests
- POST /auth/refresh → exchange refreshToken for new accessToken when it expires

1.2 Error Envelope

All errors return this structure regardless of HTTP status:

```
{ "error": { "code": "VALIDATION_ERROR", "message": "postalCode must match A1A 1A1 format.", "field": "postalCode" } }
```

Standard error codes:

UNAUTHORIZED: Missing or invalid Bearer token

FORBIDDEN: Authenticated but not permitted (e.g. accessing another user's home)

RESOURCE_NOT_FOUND: Entity does not exist or is not accessible to the caller

VALIDATION_ERROR: Request body or query parameter failed validation

CONFLICT: Operation blocked by current entity state (e.g. session already has a result)

PAYMENT_REQUIRED: Email not verified; cannot purchase

1.3 Endpoint Index

All 35 endpoints. Auth column: ✓ = Bearer token required, – = public.

Method	Endpoint	Summary	Auth
POST	/auth/register	Register a new user account	–
POST	/auth/login	Login with email and password	–
POST	/auth/refresh	Refresh access token	–
POST	/auth/logout	Invalidate current session	✓

GET	/auth/me	Get current user profile	✓
PATCH	/auth/me	Update current user profile	✓
PATCH	/auth/password	Change password (authenticated)	✓
POST	/auth/password-reset	Request password reset email	–
GET	/homes	List all homes for the current user	✓
POST	/homes	Create a new home	✓
GET	/homes/:homeId	Get a single home	✓
PATCH	/homes/:homeId	Update home details	✓
DELETE	/homes/:homeId	Delete a home	✓
GET	/orders	List orders for the current user	✓
POST	/orders	Create a checkout session (initiate order)	✓
GET	/orders/:orderId	Get a single order	✓
GET	/sessions	List test sessions	✓
GET	/sessions/:sessionId	Get a single test session	✓
POST	/sessions/:sessionId/activate	Activate session — confirm kit placement	✓
POST	/sessions/:sessionId/retrieve	Mark kit as retrieved from placement	✓
POST	/sessions/:sessionId/mail	Confirm kit mailed to lab	✓
POST	/sessions/:sessionId/cancel	Cancel a test session	✓
GET	/sessions/:sessionId/result	Get result for a session	✓
POST	/sessions/:sessionId/result	Submit result for a session	✓
GET	/certificates	List certificates for current user	✓
GET	/certificates/:id	Get a certificate (authenticated)	✓
GET	/certificates/:id/download	Download certificate PDF	✓
GET	/verify/:id	Public certificate verification	–
GET	/contractors	Find contractors by location	–
POST	/contractors/:id/lead	Record contractor interaction event	✓
POST	/referral-codes/validate	Validate a referral code	✓
POST	/webhooks/stripe	Stripe webhook receiver	–
POST	/webhooks/resend	Resend email status webhook	–
GET	/admin/metrics	Platform dashboard metrics	✓
POST	/admin/contractors	Create contractor listing (admin)	✓

2. Auth Endpoints

POST `/auth/register`

Register a new user account

Creates a Supabase Auth user and a corresponding users profile row. The account cannot complete a purchase until email_verified_at is set.

Request Body

Name	Location	Required	Description
`email`	string	Y	Valid email. Unique.
`password`	string	Y	Min 8 characters.
`firstName`	string	Y	Given name.
`lastName`	string	Y	Family name.
`phone`	string	N	Optional. E.164 format.
`marketingConsent`	boolean	N	CASL consent. Default false. Must never be pre-checked.

Responses

Code	Description
201	Account created. Returns user object and confirmation message.
409	Email already registered.
422	Validation error.

POST `/auth/login`

Login with email and password

Returns Supabase access and refresh tokens.

Request Body

Name	Location	Required	Description
`email`	string	Y	Registered email.
`password`	string	Y	Account password.

Responses

Code	Description
200	Returns accessToken, refreshToken, expiresIn, and user object.
401	Invalid credentials.

GET `/auth/me`

Get current user profile

Responses

Code	Description
200	Returns user object.

401	Invalid token.

PATCH /auth/me

Update current user profile

Request Body

Name	Location	Required	Description
firstName	string	N	
lastName	string	N	
phone	string	N	
marketingConsent	boolean	N	

Responses

Code	Description
200	Updated user object.
422	Validation error.

PATCH /auth/password

Change password (authenticated)

Request Body

Name	Location	Required	Description
currentPassword	string	Y	Current password for verification.
newPassword	string	Y	New password. Min 8 characters.

Responses

Code	Description
204	Password changed.
401	Current password incorrect.

3. Home Endpoints

POST /homes

Create a new home

fsa, radonZone, and regionalPrevalencePct are derived server-side from postalCode. Do not send them.

Request Body

Name	Location	Required	Description
addressLine1	string	Y	Street address. Appears on certificate.
city	string	Y	City name.
province	string	Y	Two-letter code: AB, BC, MB, NB, NL, NS, NT, NU, ON, PE, QC, SK, YT.
postalCode	string	Y	Format: A1A 1A1 (with space, uppercase).
ageRange	enum	Y	pre_1980 | 1980_2000 | 2000_2010 | post_2010 | unknown
foundationType	enum	Y	full_basement | partial_basement | crawl_space | slab | unknown
basementOccupancy	enum	Y	primary_living | occasional | storage | no_basement
nickname	string	N	Optional label.
addressLine2	string	N	Suite / unit.
roughinPresent	boolean	N	Default false.

Responses

Code	Description
201	Home created with derived radonZone and regionalPrevalencePct.
422	Invalid postal code, unknown province, or missing required field.

PATCH /homes/:homeId

Update home details

If postalCode changes, fsa, radonZone, and regionalPrevalencePct are re-derived automatically.

Parameters

Name	Location	Required	Description
homeId	path	Y	UUID of the home.

Responses

Code	Description
200	Updated home object.
404	Not found or not owned by caller.
422	Validation error.

DELETE /homes/:homeId

Delete a home

Blocked if any test session exists with status other than cancelled or expired. Returns 409 in that case.

Parameters

Name	Location	Required	Description
homeId	path	Y	UUID of the home.

Responses

Code	Description
204	Deleted.
404	Not found.
409	Active or completed sessions prevent deletion.

4. Kit Order Endpoints

POST `/orders`

Create a checkout session

Creates a KitOrder with payment_status = pending and returns a Stripe Checkout URL. Redirect the user to this URL. On payment success, the Stripe webhook sets payment_status = paid, creates the TestSession(s), and triggers the order_confirm email.

Request Body

Name	Location	Required	Description
`homeId`	string	Y	UUID of the home this kit is for.
`productSku`	enum	Y	standard_long | real_estate_short | twin_pack
`shippingAddressLine1`	string	Y	Shipping street address.
`shippingCity`	string	Y	Shipping city.
`shippingProvince`	string	Y	Province code.
`shippingPostalCode`	string	Y	Postal code.
`referralCode`	string	N	Optional promo or referral code.
`successUrl`	string	Y	Stripe redirects here on successful payment.
`cancelUrl`	string	Y	Stripe redirects here if user cancels.

Responses

Code	Description
201	Returns order object and checkoutUrl.
402	Email not verified.
422	Invalid referral code or missing required field.

5. Test Session Endpoints

> *Sessions follow a strict state machine: ordered → active → retrieval_due (auto) → mailed → results_pending → complete. Terminal states: expired and cancelled. The API rejects invalid transitions.*

POST `/sessions/:sessionId/activate`

Activate — confirm kit placement

Sets activated_at, calculates expected_completion_date (+ 91 days long_term / + 4 days real_estate_short) and retrieval_due_at (expected_completion_date − 3 days). Schedules the Day 30, 60, 80, and 88 emails.

Parameters

Name	Location	Required	Description
`sessionId`	path	Y	UUID of the session.

Request Body

Name	Location	Required	Description
`placementRoom`	string	Y	e.g. Basement.
`placementDescription`	string	N	Optional notes on exact placement.
`activatedAt`	date	N	YYYY-MM-DD. Defaults to today if omitted.

Responses

Code	Description
200	Session updated to active.
409	Session is not in ordered status.

POST `/sessions/:sessionId/retrieve`

Mark kit as retrieved

Parameters

Name	Location	Required	Description
`sessionId`	path	Y	UUID of the session.

Request Body

Name	Location	Required	Description
`retrievedAt`	date	Y	Date kit was retrieved from placement.

Responses

Code	Description
200	Session updated.
409	Session not in active or retrieval_due status.

POST `/sessions/:sessionId/mail`

Confirm kit mailed to lab

Sets mailed_at and transitions to mailed. Schedules the results_prompt email for 10 days after mailed_at.

Parameters

Name	Location	Required	Description
sessionId	path	Y	UUID of the session.

Request Body

Name	Location	Required	Description
mailedAt	date	Y	Date kit was mailed.

Responses

Code	Description
200	Session updated to mailed.
409	Session not in retrieved state.

POST /sessions/:sessionId/result

Submit a result

zone is derived server-side from valueBqm3. Never accept zone from the client. Transitions session to complete. Triggers certificate generation (async). If the home already has a valid certificate, the old one is superseded automatically.

Parameters

Name	Location	Required	Description
sessionId	path	Y	UUID of the session.

Request Body

Name	Location	Required	Description
valueBqm3	number	Y	Radon concentration ≥ 0.
recordedAt	timestamp	Y	ISO 8601 UTC.
labReference	string	N	Lab internal reference number.

Responses

Code	Description
201	Result created and certificate generation triggered. Returns result and certificate objects.
409	Session already has a result, or not in mailed / results_pending status.

6. Certificate Endpoints

GET `/verify/:certificateId`

Public certificate verification (no auth required)

Returns minimal public information only — no numeric Bq/m³ value, no personal information. This is the endpoint behind the QR code on the printed certificate.

Parameters

Name	Location	Required	Description
`certificateId`	path	Y	The certificate UUID from the QR code.

Responses

Code	Description
200	Returns certificateNumber, certType, status, zone (not Bq value), city, province, validFrom, validUntil.
404	Certificate not found.

GET `/certificates/:id/download`

Download certificate PDF

If PDF generation has not yet completed (typically within 5 seconds of result submission), returns HTTP 202. Client should retry after 3 seconds.

Parameters

Name	Location	Required	Description
`id`	path	Y	UUID of the certificate.

Responses

Code	Description
200	PDF file. Content-Type: application/pdf.
202	Still generating. Retry in 3 seconds.
404	Not found or not accessible.

7. Contractor Endpoints

GET `/contractors`

Find contractors by location (public)

Returns active contractors matching the FSA or province. FSA-level matching takes priority. Featured contractors appear first. No auth required — this endpoint is callable from the public-facing site.

Parameters

Name	Location	Required	Description
`fsa`	query	N	Forward Sortation Area e.g. T2J.
`province`	query	N	Province code e.g. AB. Fallback if no FSA match.
`services`	query	N	measurement | mitigation | both

Responses

Code	Description
200	Array of active contractors, featured first then alphabetical.

POST `/contractors/:contractorId/lead`

Record a contractor interaction event

Call on profile_view, phone_click, email_click, or contact_click. Used for billing and funnel analytics.

Parameters

Name	Location	Required	Description
`contractorId`	path	Y	UUID of the contractor.

Request Body

Name	Location	Required	Description
`eventType`	enum	Y	profile_view | contact_click | phone_click | email_click
`resultId`	string	N	UUID of the result that prompted this interaction.

Responses

Code	Description
201	Lead event recorded.
404	Contractor not found or not active.

8. Webhook Handlers

> *Webhooks are verified by provider signature, not Bearer token. Invalid signatures return HTTP 400. Stripe signature uses STRIPE_WEBHOOK_SECRET; Resend uses RESEND_WEBHOOK_SECRET.*

8.1 POST /webhooks/stripe

Stripe webhook handler. Verifies Stripe-Signature header. Handled events:

- payment_intent.succeeded → set order payment_status = paid, set paid_at, transmit to lab, create TestSession(s), schedule order_confirm email
- payment_intent.payment_failed → set order payment_status = failed
- charge.refunded → set order payment_status = refunded, cancel associated TestSession(s)

All other event types are acknowledged with HTTP 200 and silently ignored.

8.2 POST /webhooks/resend

Resend delivery status handler. Updates email_log.status.

- email.delivered → status = delivered
- email.bounced → status = bounced. Three consecutive bounces on same address flags the user for admin review.
- email.complained → treated identically to email.bounced

9. Admin Endpoints

> *All /admin/* endpoints require role = admin in the authenticated user record. Non-admin requests return HTTP 403 FORBIDDEN.*

9.1 User Management

GET /admin/users returns a paginated list of all users. Supports search (email, name) and role filter. PATCH /admin/users/:userId can update role.

9.2 Contractor Management

POST /admin/contractors creates a new listing. PATCH /admin/contractors/:id updates it (status, certification dates, service areas). DELETE /admin/contractors/:id removes it.

9.3 Certificate Supersession

POST `/admin/certificates/:id/supersede`

Manually supersede a certificate (admin)

Used when a lab error requires a result correction. Sets certificate status = superseded, unlocks the result (is_immutable = false), allowing a corrected result to be submitted on the same session.

Parameters

Name	Location	Required	Description
`id`	path	Y	UUID of the certificate.

Request Body

Name	Location	Required	Description
`reason`	string	Y	Audit reason. Stored in admin audit log.

Responses

Code	Description
200	Certificate superseded. Result unlocked.
404	Not found.
409	Certificate is already superseded or expired.

9.4 Platform Metrics

GET /admin/metrics returns a dashboard snapshot: totalUsers, totalHomes, activeSessionCount, completedThisMonth, resultsByZone (4 zone counts), certificatesIssued, revenueThisMonthCad, contractorLeadsThisMonth.

— End of API Specification —

ClearPath RD | clearpathrd.com | Version 1.0 | February 2026