



Saving a Generation

OPS · RUNBOOK

Demo → production Go-live checklist

Use this when green light is given. Portals UX and online training are ready; remaining work is identity, data hygiene, domains, and the email / Paybill flips. Do **not** execute flips until PO + ops approve.

Live today: [Marketing + portals](#) · [Training manuals](#) · [Partner login](#)

API: Railway Postgres · <https://api-production-92a5.up.railway.app/v1>

Status: Demo / workshop mode — seed users and simulate forms/payments until flipped.

A. Must-do before inviting real partners

Security and data — complete before real CSR/Host invites.

	Item	Notes
☐	Kill or rotate demo accounts	Disable <code>*@sag.local</code> / <code>*@acme.local</code> / <code>*@sigona.local</code> or change every password off Password123!
☐	Turn off auto-seed	Ensure <code>SEED_ON_BOOT</code> is unset on Railway prod
☐	Invite real ops users	Create real <code>ops_admin</code> (+ optional <code>ops_readonly</code>); stop shared seed password for invites
☐	Confirm JWT + CORS	Strong unique <code>JWT_SECRET</code> ; <code>CORS_ORIGINS</code> locked to marketing + portal origins (not *)
☐	Confirm Postgres is SoT	Health shows <code>store: postgres</code> ; no <code>MemoryStore</code> / <code>.data/submissions.json</code> in prod
☐	Backups	Railway Postgres daily backup on; document one restore drill
☐	Delete leftover Netlify site	<code>sag-portals-unused-delete-me</code> if still present

B. Domains & deploy posture

	Item	Notes
☐	Custom domains	Apex → Netlify; <code>api....</code> → Railway (TLS)
☐	Env matrix filled	<code>NEXT_PUBLIC_SAG_API_URL</code> / <code>SAG_PLATFORM_API_URL</code> → prod API; no demo secrets in client
☐	Preview ≠ prod	Separate DB + JWT for preview environments
☐	Deprecate <code>/ops/inbox</code>	Redirect or banner; Admin inbox under <code>/portal/admin</code> is canonical
☐	Demo logins stay hidden	Keep <code>NEXT_PUBLIC_SHOW_DEMO_LOGINS</code> unset in production

C. Non-tech gates

	Item	Notes
☐	NGO / board registration	Clear for sponsor diligence conversations
☐	Child safeguarding policy	Published; hosts can acknowledge in portal
☐	MoU template	Ready for first Host Node

☐	Named ops owner	Inbox triage hours owned
☐	First real partners	Named CSR + Host contacts (not seed fixtures)

D. Live flips (only with PO + ops approval)

Until flipped, keep `SAG_FORM_CHANNEL=simulate` and `SAG_PAYMENT_MODE=simulate` even on the production URL.

Forms (email)

	Item	Notes
☐	Provider ready	Resend/SMTP + secrets
☐	Flip <code>SAG_FORM_CHANNEL=email</code>	On Netlify
☐	Smoke public forms	CSR / contact / need-support → email + Admin inbox copy
☐	Fail-closed check	Behaviour if provider is down

Payments (Paybill)

	Item	Notes
☐	Real Paybill / bank details	<code>SAG_MPESA_*</code> / <code>SAG_BANK_*</code>
☐	Flip <code>SAG_PAYMENT_MODE=live</code>	On Netlify
☐	Donate UI no longer sim	No simulation rails shown as live
☐	Admin labelling	Leftover <code>payment_sim</code> still labelled; no fake settled funds

E. Soft-launch hardening (first week)

	Item	Notes
☐	Invite password hygiene	Reset / forced change, or unique per invite
☐	Login rate-limit smoke	Confirm throttle against brute force
☐	Audit spot-check	After first real invites / triage
☐	Staff use /training/	Paths already online
☐	Error tracking (optional G4)	Sentry on API + Next; scrub PII

F. Explicitly not required for first production

- Daraja ledger / dollar-for-dollar receipts
- Hub Manager PWA / offline sync
- WhatsApp clinical triage
- Angular portal migration / separate `admin.csr.host.apps`
- Donor portal / SSO / full document upload

Suggested order when green light lands

1. **A + B** — secure the running stack
2. **C** — ops can staff it
3. Soft launch with **simulate still on** for forms/payments if needed
4. **D** — email flip, then Paybill flip
5. **E** — first-week polish

Pause here

Checklist captured for later execution. Do not flip email/Paybill or delete seed users until green light + owners are assigned.