

AI app safety and launch checklist

Work through this before Week 7's assignment and before you launch in Week 8. Not legal advice; check the rules that apply to your product.

Keys and secrets

- ☐ API keys only in environment variables, used only in server code
- ☐ .env.local in .gitignore; no keys ever pushed to GitHub (rotate any that were)
- ☐ Separate keys for development and production; spending limits set in each provider console

Abuse and cost control

- ☐ Every AI route requires sign in, or has strict rate limits per IP
- ☐ Daily and monthly usage limits per user, stored in the database
- ☐ max_tokens set on every call; input length limited
- ☐ Alerts when daily spend passes your limit

Prompt injection and content

- ☐ User text is clearly separated from your instructions (tags or separate messages)
- ☐ The model can't take irreversible actions (payments, deletions, emails) without a human confirming
- ☐ Tool inputs are validated with a schema before your code runs them
- ☐ Moderation or keyword checks on user input and model output where harm is possible

Privacy (Nigeria Data Protection Act 2023, and GDPR for EU users)

- ☐ Collect only the data you need, and say why in a plain privacy notice
- ☐ Don't send names, phone numbers or ID numbers to AI providers unless essential; remove them first
- ☐ Check each provider's data retention and training settings
- ☐ Let users delete their account and data

Quality

- ☐ A test set of real-looking inputs, run before every release
- ☐ The app says 'I don't know' instead of guessing
- ☐ Citations or sources shown where answers matter
- ☐ Loading, streaming, error, empty and limit-reached states all designed

Payments (Paystack or Stripe)

- ☐ Test mode keys only until launch; never real card numbers in testing
- ☐ Subscription status checked on the server via webhooks, not the browser
- ☐ Webhook signatures verified

Launch

- ☐ Custom domain and HTTPS on Vercel
- ☐ Error monitoring and logs (without logging personal data)
- ☐ Analytics on the key actions

[] A case study written for your portfolio