Parental Monitoring Web Tool – Development Plan

0) Guardrails, consent, scope
- Intended use: parental supervision on devices they administer for minors with disclosure.
- Local only: no cloud calls by default. Optional local LLM.
- Tamper-resistance: password required to disable.

1) Architecture
- Watcher daemon/service
- Browser extensions (Chrome/Firefox)
- Network capture (optional DNS/proxy)
- OCR/ASR sidecars
- Safety analyzer (rule + ML + LLM)
- Policy engine
- Parent UI (localhost)
- SQLite+SQLCipher storage

2) Data model
Tables: child_profile, event, analysis, decision, settings.

3) Capture Layer
- Browser extensions: URLs, searches, DOM text, screenshots, video audio (optional)
- DNS/proxy (optional advanced)

4) Safety Analysis
- Pre-filters: blocklists, regex, URL categories
- ML classifiers: toxicity, sexual content, NSFW image, violence
- LLM judge (via Ollama, JSON output)

5) Real-time Enforcement
- Content script for warn/blur/block
- Search interception
- Async upgrade of decision

6) Parent Dashboard
- Views: Home, Alerts, Searches, Sites, Policies, Models, Audit
- Security: PIN login, local only

7) Local APIs
- gRPC/HTTP2 endpoints for event, analyze, decision, control

8) Pause Monitoring
- Child requests pause → parent approves via PIN
- Tamper prevention: watcher restarts killed processes

9) Models & Performance
- Default small models (text toxicity, NSFW image)
- Optional Whisper OCR/ASR
- LLM judge optional

10) Milestones

M0 scaffold → M1 browser monitoring → M2 fast rules → M3 classifiers → M4 LLM → M5 OCR/ASR → M6 DNS/proxy → M7 QA → M8 Packaging

11) Policy Logic Example
- Allow educational
- Block adult/NSFW
- Warn supervision-needed
- Apply LLM judge

12) Privacy by Design
- Redact PII
- Ephemeral logs option
- Export/delete per child