

Police & Investigation Overview

Capture > Recall > Verify > Record > Share. One recognition engine, investigation-grade records, and an evidentiary chain that survives disclosure.

1. What RapidID is

RapidID is a visual identification and records platform. Licensed venues use it as a shared barring register at the door. Police, council enforcement and investigation units use the same engine pointed at different registers — persons of interest, stolen property, vehicles and number plates — with a full chain-of-custody record behind every action. The investigative module is disabled by default, is enabled per organisation under written authority, and every activation is audit-logged.

2. Evidence workflow

Capture	Photo, video, live camera or uploaded file is ingested. Device, operator, GPS, timestamp and a SHA-256 content hash are written at the moment of capture.
Recall	Vector embeddings retrieve candidate records from the active register (pgvector nearest-neighbour), scoped to the caller's clearance.
Verify	A second-pass model re-scores each candidate and returns a confidence band. Borderline results route to a human reviewer — never an automatic identification.
Record	Match run, candidate list, scores, model version, thresholds and reviewer decision are written to an immutable log with the exhibit.
Share	Disclosure packages are exported as signed bundles to named agencies. Each transfer is recorded with recipient, purpose and time.

3. Investigative capability

- **Facial recall & verification** — two-stage matching with adjustable sensitivity per organisation.
- **Number plate & vehicle recognition** — plate OCR plus make/model/colour attributes against the vehicle register.
- **Stolen property matching** — serials, engravings and visual similarity across property reports.
- **Video analysis** — frame sampling across a clip, multi-subject tracking with persistent subject IDs, and an event timeline.
- **Audio transcription** — speech extracted and transcribed, searchable alongside the visual evidence.
- **Cross-capture search** — free-text and attribute search over every capture, transcript and detection.
- **Alert rules** — standing rules fire on watch-list hits and notify the right unit with location and confidence.
- **Incident reports** — assembled narrative, exhibit list, match provenance and audit extract, exportable as PDF.

4. Records & evidentiary integrity

Content hashing	Every exhibit hashed at ingest; re-hash on export proves the file is unaltered.
Immutable audit	Every view, match run, threshold change, export and role grant is appended and cannot be edited or deleted.
Match provenance	Model, model version, threshold and score for each candidate are retained so a result can be reproduced or contested.

Human decision	Identification is always an operator decision recorded against a named user; the system produces candidates, not conclusions.
Retention	Per-register retention windows with scheduled purge and a purge log.
Disclosure	One-click export of the complete chain of custody for a capture, incident or subject.

GOVERNANCE, LEGAL BASIS AND DEPLOYMENT

5. Access control

Roles — Security, Licensee, Coordinator, Police and Admin — are granted per user and enforced in the database by row-level security, not in the interface. A police user cannot see a venue's private barring records unless the ban scope permits it, and a venue user never sees investigative registers.

Venue scope	Visible to the lodging premises only.
Accord scope	Shared with the venues in the accord group.
LGA scope	All participating premises in the local government area.
State scope	Serious matters, coordinator approval required.
National scope	Highest tier — police and administrator oversight required.

6. Legal and privacy position

- Venue screening operates under displayed conditions of entry; signage at each entrance is the operative consent mechanism, recorded per venue.
- Investigative use of the identification pipeline requires a warrant or statutory power. It is off by default and each activation is audit-logged against the authorising officer.
- Driver-licence numbers are SHA-256 hashed at capture and never stored in raw form.
- No data is forwarded to third-party or national systems unless the operating agency explicitly configures that integration.
- The platform runs on infrastructure the agency controls; data residency and retention follow agency policy.
- Automated matching is decision-support only. A refusal, stop or identification is always attributable to a named human operator.

7. Deployment

Devices	Any modern phone, tablet or desktop browser. Native iOS and Android builds available via the same codebase.
Registers	Bulk CSV onboarding with per-row validation and an import batch history.
Integration	Agency-to-agency sharing is explicit and recorded; API access is scoped per organisation.
Pilot	Typical pilot is a single unit or LGA on a read-only register, extended once audit reporting is signed off.

Enquiries and pilot requests

Request clearance through the RapidID console, or contact your accord coordinator or agency liaison. This document is an overview only and does not constitute legal advice; deployment requires local legal review.