CIVICGUARD FIELD DOCUMENT

Acceptable Use Policy

Mandatory boundaries for every official-fleet search, alert, export, and partner share.

CG-TRUST-204	September 2026

Visibility should work both ways.

Prepared for municipal operations, public-integrity offices, transit authorities, civic campuses, and authorized oversight partners.

REVISION HISTORY

A	September 2026	Initial release.
B	October 2026	Clarified that "checking on a colleague" counts as a search.

1. Authorized purposes

CivicGuard may be used only for documented public-operations needs involving enrolled government, municipal, executive, or contracted public fleets.

- Route integrity and continuity of public service
- Recovery of missing or misrouted official assets
- Authorized executive-protection logistics
- Fleet inventory and yard reconciliation
- Public-integrity and oversight review
- Incident reconstruction involving an enrolled official vehicle

2. Prohibited purposes

- Personal curiosity, political retaliation, harassment, or intimidation
- Searching a person rather than an enrolled official vehicle
- Immigration enforcement against private residents
- Targeting based solely on race, religion, disability, gender, or another protected class
- Exporting data outside an approved case or public-records workflow
- Sharing credentials or using another person's account

A search without a legitimate public purpose is not an informal lookup. It is a policy event.

3. Search requirements

Requirement	Minimum standard
Identity	Named user with MFA; shared accounts prohibited
Purpose	Purpose code selected before results are displayed
Scope	Narrowest plate, corridor, and time window reasonably available
Case reference	Required for investigations, exports, and partner shares
Audit	User, purpose, query, result count, and export action retained

4. Review cadence

- Supervisors review flagged searches weekly.
- Customer administrators review roles and dormant accounts monthly.
- Oversight offices receive a monthly search and export summary.
- Confirmed misuse is reported to CivicGuard Trust Operations within 24 hours.
- Audit records remain available for the contractual review period even when underlying events expire.

5. Enforcement

Finding	Default action
Incomplete purpose code	Search blocked until corrected
Repeated overbroad query	Supervisor review and retraining
Credential sharing	Immediate account suspension
Personal or retaliatory use	Immediate suspension and customer investigation
Unlawful access or disclosure	Account termination, evidence preservation, and legal escalation

6. Public accountability

Customers publish reader count, retention period, authorized-use categories, and aggregate search counts through the CivicGuard Transparency Portal. CivicGuard records the activity. The customer remains responsible for the purpose.

Questions: trust@civicguard.uk | Reports: integrity@civicguard.uk