Investigative Tool Usage Policy

Department: Case Files & Investigations
Policy ID: CFI-04
Version: 1.0
Effective Date: Upon Publication

1. Policy Title

Investigative Tool Usage Policy

2. Authority & Legal Standing

2.1 **Binding Instrument.**
This Investigative Tool Usage Policy ("Policy") is a binding operational and governance instrument governing the selection, configuration, access, and use of investigative tools within authorised Case Files.

2.2 **Condition of Tool Access.**
No investigative tool may be used in connection with a Case unless such use complies fully with this Policy.

2.3 **Legal Reliance.**
This Policy is drafted to be relied upon in judicial, regulatory, arbitral, and oversight contexts as evidence that the Organisation exercises restraint, legality, and accountability in its use of investigative technologies.

2.4 **No Implied Authority.**
Use of a tool does not confer authority to access restricted systems, collect unlawful data, bypass safeguards, or expand investigative scope. Authority arises only from Case opening, scope locking, and target definition policies.

3. Purpose

3.1 **Primary Objective.**
The purpose of this Policy is to ensure that investigative tools are used only in lawful, proportionate, transparent, and controlled ways consistent with authorised Case scope.

3.2 **Risk Control Objective.**
This Policy exists to prevent misuse of tools in ways that could constitute unlawful access, surveillance, overcollection, coercion, or technical overreach.

3.3 **Integrity Objective.**
This Policy ensures that investigative outputs are not tainted by improper tooling, undocumented automation, or uncontrolled technical processes.

3.4 **Non-Determination.**
Tool usage does not determine truth, intent, liability, or outcome. Tools are instruments of collection and examination only.

4. Scope & Applicability

4.1 **Scope.**
This Policy governs the use of investigative tools employed during investigative activity within an opened and scope-locked Case.

4.2 **Applicability.**
This Policy applies to:

All investigative tools, whether proprietary, open-source, commercial, internal, or third-party
All personnel, contractors, and systems using tools on behalf of the Organisation
All commissioned, pro bono, and public-interest investigations

4.3 **Explicit Scope Limitation Clause.**
This Policy does **not** govern investigative conduct, target selection, analytical methodology, evidentiary evaluation, publication decisions, or archival handling. It governs tool usage only.

5. Definitions (Local Only)

For the purposes of this Policy only:

5.1 **Investigative Tool.**
Any software, script, service, platform, automation, or technical mechanism used to collect, retrieve, process, or examine information for investigative purposes.

5.2 **Tool Instance.**
A specific execution, configuration, or deployment of an investigative tool.

5.3 **Automated Tooling.**
Any tool that performs actions without continuous human input once initiated.

5.4 **Tool Output.**
Any data, logs, artefacts, or results produced by a tool instance.

Definitions are local to this Policy and have no binding force outside it.

6. Permitted Activities

Within the strict scope of this Policy, the Organisation may:

6.1 Use investigative tools that rely on lawful access pathways, publicly accessible sources, or authorised credentials.

6.2 Configure tools to operate strictly within Case scope, approved targets, and proportionality constraints.

6.3 Employ automated tools where outputs are reviewable, attributable, and controllable.

6.4 Record high-level tool usage metadata sufficient to demonstrate lawful and restrained use.

6.5 Disable, suspend, or restrict tools where risk or misuse is identified.

Anything not expressly permitted under this Policy is disallowed.

7. Prohibited Activities

The following are expressly prohibited:

7.1 **Unlawful Access.**
Using tools to access systems, accounts, communications, or data without lawful authority or access rights.

7.2 **Circumvention of Safeguards.**
Using tools to bypass authentication, paywalls, rate limits, technical restrictions, or platform protections.

7.3 **Indiscriminate Collection.**
Deploying tools in a manner that collects data beyond defined targets, scope, or necessity.

7.4 **Undocumented Automation.**
Using automated tools without traceability, configuration control, or the ability to review outputs.

7.5 **Covert Surveillance.**
Using tools in a manner that constitutes covert monitoring, tracking, or profiling of individuals outside lawful scope.

7.6 **Tool Repurposing.**
Using tools for purposes other than the authorised Case, including personal use or unrelated investigations.

7.7 **Outcome-Driven Tooling.**
Configuring or selecting tools to force, bias, or manufacture a particular investigative outcome.

8. Procedural Requirements

8.1 **Tool Selection Requirement.**
Only tools suitable to the authorised investigative purpose may be selected.

8.2 **Configuration Control.**
Tools must be configured to limit collection, access, and output to what is necessary for the Case.

8.3 **Human Oversight Requirement.**
Automated tools must operate under human oversight, with the ability to pause, stop, or review execution.

8.4 **Attribution Requirement.**
Tool outputs must be attributable to a specific tool instance and Case.

8.5 **Immediate Suspension Rule.**
If a tool is suspected of operating unlawfully, excessively, or outside scope, its use must be immediately suspended.

9. Safeguards & Risk Controls

9.1 **Least-Intrusive Tooling Principle.**
Where multiple tools could achieve the same purpose, the least intrusive option must be preferred.

9.2 **Scope Enforcement Control.**
Tool configurations must reflect Case scope and target definitions and must not enable expansion by default.

9.3 **Collateral Data Minimisation.**
Tools must be used in ways that minimise incidental collection of non-target data.

9.4 **Auditability Control.**
Sufficient metadata must exist to demonstrate what tool was used, when, and for which Case, without logging substantive content.

9.5 **Third-Party Risk Control.**
Use of third-party tools must not transfer control, ownership, or unintended access to Case data.

10. Enforcement & Compliance Mechanisms

10.1 **Access Control.**
Tool access may be restricted to authorised roles and Case-assigned personnel only.

10.2 **Usage Review Authority.**
The Organisation may review tool usage patterns to detect misuse, overreach, or drift.

10.3 **Revocation Authority.**
Tool access may be revoked where misuse, risk, or non-compliance is identified.

11. Breach Handling & Remediation

11.1 **Breach Definition.**
A breach includes any prohibited activity, misuse of tools, unlawful access, or failure to comply with procedural requirements.

11.2 **Containment.**
Upon suspected breach, tool use must be suspended and affected outputs isolated.

11.3 **Remediation.**
Remediation may include exclusion of tainted outputs, restriction of access, reconfiguration, or termination of tool usage within the Case.

12. Limitation of Liability

12.1 The Organisation authorises tool use within defined limits only.

12.2 The Organisation is not liable for unauthorised or prohibited use of tools by individuals acting outside this Policy.

12.3 No liability arises from lawful refusal to deploy or continue tool usage.

12.4 Nothing limits liability where prohibited by law.

13. Non-Delegation & Non-Expansion Clause

13.1 This Policy confers no surveillance, enforcement, or statutory authority.

13.2 This Policy may not be interpreted to expand investigative scope or override other controls.

13.3 Tool usage authority is technical, not legal or adjudicative.

14. Jurisdiction & Governing Law

This Policy is governed by the laws of England and Wales.
Jurisdiction lies with the courts of England and Wales, subject to mandatory statutory obligations.

15. Amendments & Version Control

15.1 This Policy may be amended only by the Organisation.

15.2 Amendments take effect upon publication.

15.3 The policy version in force at the time of tool usage governs that usage.

16. Supremacy Within Scope

Within the domain of investigative tool usage, this Policy is authoritative.
Outside that domain, it has no force.