Intake Audit Logging Policy

Department: Evidence Intake & Verification Desk
Policy ID: EIV-09
Version: 1.0
Effective Date: Upon Publication

1. Policy Title

Intake Audit Logging Policy

2. Authority & Legal Standing

2.1 **Binding Instrument.**
This Intake Audit Logging Policy ("Policy") is a binding operational and contractual instrument governing the creation, retention, protection, and use of audit records documenting intake-stage actions, decisions, and procedural compliance.

2.2 **Condition of Processing.**
No Submission may proceed beyond intake-stage handling unless all required audit records have been created in accordance with this Policy. Absence of audit logging renders processing non-compliant and voids eligibility for onward handling.

2.3 **Evidentiary Reliance.**
This Policy is expressly drafted to be relied upon in judicial, regulatory, arbitral, oversight, and audit contexts as evidence that the Organisation operates structured, consistent, and defensible intake procedures and does not engage in informal, undocumented, or discretionary processing.

3. Purpose

3.1 **Primary Objective.**
The purpose of this Policy is to ensure that all intake-stage actions are documented in a manner that is sufficient to reconstruct procedural events, demonstrate compliance with governing policies, and defend the Organisation against allegations of misuse, bias, selective handling, or unlawful processing.

3.2 **Integrity Objective.**
This Policy exists to ensure that intake audit records serve as evidence of *process integrity*, not as a secondary content store, intelligence database, or surveillance mechanism.

3.3 **Non-Determination.**
Audit logging under this Policy does not assess truth, merit, intent, or outcome. It records only that defined procedures occurred and what procedural decisions were taken.

4. Scope & Applicability

4.1 **Scope.**
This Policy applies exclusively to audit logging associated with evidence intake and verification activities prior to investigation, analysis, archival processing, or publication consideration.

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

All Submissions received via Authorised Channels
All intake-stage policies and gates
All personnel, volunteers, contractors, and systems performing intake functions
All commissioned, pro bono, and public-interest Submissions at intake

4.3 **Scope Limitation Clause.**
This Policy does not govern investigative logs, analytical working notes, editorial records, employment monitoring, or system surveillance beyond intake-stage procedural logging.

5. Definitions (Local Only)

For the purposes of this Policy only:

5.1 **Audit Log.**
A structured record capturing intake-stage procedural events, decisions, and metadata sufficient to evidence compliance.

5.2 **Audit Metadata.**
Non-substantive data elements documenting process execution without recording content meaning or analysis.

5.3 **Event Record.**
A discrete log entry representing a single procedural action or decision.

5.4 **Submission Identifier.**
A unique reference assigned to a Submission to link audit records without repeating content.

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 Create audit logs documenting intake-stage events and decisions.

6.2 Record timestamps, identifiers, policy gates applied, and disposition outcomes.

6.3 Retain audit logs for compliance, defence, and oversight purposes.

6.4 Restrict access to audit logs to authorised governance roles.

6.5 Produce audit extracts in response to lawful oversight, regulatory, or judicial requests.

No other activities are permitted under this Policy.

7. Prohibited Activities

The following are expressly prohibited:

7.1 Recording substantive content of Submissions within audit logs.

7.2 Using audit logs as investigative notes, intelligence repositories, or profiling tools.

7.3 Logging speculative commentary, opinions, or analysis.

7.4 Allowing unauthorised access to audit records.

7.5 Altering, deleting, or retroactively editing audit records except as permitted under version control rules.

7.6 Creating parallel or informal intake records outside the audit logging system.

8. Procedural Requirements

8.1 **Mandatory Audit Logging Sequence.**

For every Submission, the following events must be logged where applicable:

a) Submission Receipt — channel, timestamp, submission identifier
b) Assent Capture — method and policy version accepted
c) Eligibility Screening Outcome — accept / reject / pending
d) Source Classification Assignment — labels applied
e) Lawful Basis Verification Outcome — verified / failed / withdrawn
f) PII Triage Outcome — category and triage decision
g) Conflict of Interest Screening Outcome — category and disposition
h) Malicious or Bad-Faith Screening Outcome — intent classification
i) Final Intake Disposition — proceed, reject, refer, contain

8.2 **Atomic Event Logging.**
Each event must be logged as a discrete record. Bundled or retrospective logging is prohibited.

8.3 **No Deviation.**
Failure to log a required event constitutes a breach.

9. Safeguards & Risk Controls

9.1 **Data Minimisation.**
Audit logs must contain only the minimum metadata necessary to evidence procedural compliance.

9.2 **Immutability Controls.**
Audit records must be protected against unauthorised alteration. Where corrections are required, they must be appended as new records, preserving the original. Audit logs are maintained in an append-only manner with controls designed to prevent undetected alteration.

9.3 **Access Restrictions.**
Audit logs are restricted to authorised governance, compliance, or legal roles and must not be accessible for investigative or analytical use.

9.4 **Separation from Content.**
Audit logs must be logically and technically separated from substantive content repositories.

9.5 **Non-Interpretive Safeguard.**
Audit records must not include interpretive or evaluative commentary.

9.6 **Identification Safeguards.**
Audit records must not be combined, correlated, or enriched for the purpose of identifying submitters or third parties beyond what is strictly necessary for compliance or abuse prevention.

10. Enforcement & Compliance Mechanisms

10.1 **Hard Gating.**
Workflow systems must prevent progression where required audit events are missing.

10.2 **Automated Validation.**
Where technically feasible, systems should validate completeness of audit records before allowing stage transitions.

10.3 **Periodic Integrity Checks.**
The Organisation may perform internal checks to confirm audit completeness and detect logging gaps or anomalies.

11. Breach Handling & Remediation

11.1 **Breach Definition.**
A breach includes:

Failure to log required events
Logging substantive content

Unauthorised access or alteration
Parallel off-system records

11.2 **Containment.**
Affected Submissions are suspended pending audit correction.

11.3 **Remediation.**
Remediation may include retroactive append-only logging, access restriction, procedural reinforcement, and system hardening.

12. Limitation of Liability

12.1 Audit logs evidence procedure, not outcome.

12.2 The Organisation is not liable for external misinterpretation of audit records.

12.3 No liability arises from reliance on audit logs outside their defined scope.

12.4 Nothing limits liability where prohibited by law.

13. Non-Delegation & Non-Expansion Clause

13.1 This Policy confers no investigative, analytical, or surveillance authority.

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

13.3 Audit logging is evidentiary, not 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

This Policy may be amended only by the Organisation.
Amendments take effect upon publication.
Audit records retain the policy version in force at time of logging.

16. Supremacy Within Scope

Within the domain of intake-stage audit logging, this Policy is authoritative.
Outside that domain, it has no force.