Evidence Intake Eligibility Policy

Department: Evidence Intake & Verification Desk
Policy ID: EIV-01
Version: 1.0
Effective Date: Upon Publication

1. Policy Title

Evidence Intake Eligibility Policy

2. Authority & Legal Standing

2.1 **Binding Instrument.**
This Evidence Intake Eligibility Policy ("Policy") is a binding operational and contractual instrument governing the submission, receipt, screening, acceptance, rejection, containment, and initial handling of information, data, files, documents, statements, communications, artefacts, or other materials ("Submissions") provided to the Organisation.

2.2 **Condition of Processing; No Assent, No Processing.**
The Organisation will not process any Submission beyond preliminary receipt and routing unless and until the submitter has been provided reasonable notice of this Policy and has completed an acknowledgement step that constitutes acceptance ("Assent"). Assent is a mandatory condition precedent to eligibility assessment and any further handling.

2.3 **Accepted Modes of Assent.**
Assent is deemed valid only where captured through one or more of the following mechanisms, as applicable to the intake channel:

a) **Clickwrap/Portal Assent:** an explicit affirmative action (e.g., ticking a checkbox) confirming acceptance of this Policy at the point of submission, prior to upload or dispatch.
b) **Written Assent:** explicit confirmation by email or written message stating agreement to this Policy in response to an intake notice referencing this Policy title, ID, and version.
c) **Signed Engagement Assent:** acceptance of this Policy through a signed engagement letter, statement of work, or equivalent commissioning instrument that incorporates this Policy by reference to its title, ID, and version.

2.4 **Assent Evidence and Auditability.**
The Organisation will maintain an auditable record of Assent sufficient to demonstrate reasonable notice and acceptance, which may include timestamps, channel identifiers, submission identifiers, and the Policy version accepted. Assent records are retained as audit metadata and do not constitute publication or endorsement of the Submission's content.

2.5 **Public Submissions Without Assent.**
Where a Submission is received without Assent, the Organisation may (i) issue an automated or manual notice requiring Assent, (ii) decline to process, (iii) securely delete or quarantine the material pending Assent, and/or (iv) retain only minimal routing metadata required to evidence non-processing and manage operational risk.

2.6 **Court and Regulatory Reliance.**
This Policy is drafted to be relied upon in judicial, regulatory, arbitral, and oversight contexts as evidence of due process controls, lawful and ethical intake constraints, and systematic risk containment.

3. Purpose

3.1 **Primary Objective.**
The purpose of this Policy is to define the strict eligibility criteria under which Submissions may be accepted into the Organisation's controlled workflow for subsequent verification, investigation, analysis, archival handling, or public reporting, and to prevent the intake of unlawful, malicious, coercive, biased, irrelevant, improperly obtained, or procedurally defective material.

3.2 **Risk Containment Objective.**
This Policy exists to prevent (i) unauthorised scope expansion, (ii) intake-stage bias contamination, (iii) unlawful or unethical handling of personal data, (iv) reputational or legal harm arising from bad-faith submissions, and (v) the downstream processing of material that cannot be defended on provenance, legality, proportionality, or integrity grounds.

3.3 **Non-Determination.**
This Policy is a procedural eligibility framework. It does not determine truth, falsity, liability, guilt, innocence, intent, or wrongdoing. It determines only whether a Submission may proceed into controlled internal processes.

4. Scope & Applicability

4.1 **Scope.**
This Policy applies exclusively to the **evidence intake eligibility stage** for all Submissions received by the Organisation, irrespective of origin, format, medium, subject matter, or intended use.

4.2 **Applicability.**
This Policy applies to all parties interacting with intake processes, including but not limited to members of the public, commissioning clients, volunteers, investigators, analysts, contractors, organisational personnel, and any automated or semi-automated mechanisms that receive or route Submissions.

4.3 **Authorised Channels Requirement.**
This Policy governs only Submissions received via **Authorised Channels** as defined in Section 5. Submissions received outside Authorised Channels are not treated as accepted Submissions under this Policy and are not eligible for processing.

4.4 **Scope Limitation Clause.**
This Policy governs eligibility only. It does not govern investigation conduct, analytical assessment, archival procedures, publication decisions, reporting formats, tool licensing, or any other function outside initial intake eligibility.

5. Definitions (Local Only)

For the purposes of this Policy only:

5.1 **Submission.**
Any information, data, file, document, statement, message, artefact, or other material provided to the Organisation for potential consideration.

5.2 **Intake.**
The procedural process by which a Submission is received and evaluated for eligibility under this Policy.

5.3 **Eligible Submission.**
A Submission that satisfies all mandatory eligibility requirements set out in Sections 6–9.

5.4 **Ineligible Submission.**
A Submission that fails one or more eligibility requirements, triggers a prohibition, lacks required information, or presents unacceptable legal/ethical risk at intake.

5.5 **Assent.**
A recorded affirmative acknowledgement by the submitter agreeing to this Policy via one of the accepted mechanisms in Section 2.3.

5.6 **Authorised Channels.**
Controlled intake routes designated by the Organisation for acceptance of Submissions, which may include a submission portal, a dedicated intake address, or other controlled mechanisms where Assent and audit logging can be captured.

5.7 **Lawful Basis Declaration.**
A statement by the submitter describing, at minimum, how the submitter obtained the Submission and why the submitter is permitted to provide it to the Organisation.

5.8 **PII.**
Personal Identifiable Information relating to an identified or identifiable natural person.

5.9 **Special Category Data.**
Any data that would be treated as special category data under applicable data protection law, to the extent applicable.

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

6. Permitted Activities

Within the strict scope of intake eligibility, the Organisation may:

6.1 Receive Submissions through Authorised Channels for preliminary eligibility screening.

6.2 Collect and process only the minimum metadata required to (i) route a Submission, (ii) record Assent, (iii) evaluate eligibility, and (iv) generate an auditable intake decision record.

6.3 Perform non-interpretive screening to establish completeness, provenance indicators, declared lawful basis, obvious red flags, and eligibility alignment.

6.4 Identify whether PII or Special Category Data appears present for purposes of routing and risk containment only.

6.5 Accept an Eligible Submission for referral into subsequent controlled internal processes, without commenting on accuracy or truth.

6.6 Reject an Ineligible Submission and securely delete, isolate, or quarantine the material consistent with this Policy.

6.7 Issue intake-stage notices requesting missing eligibility information, including lawful basis declaration and Assent where absent.

No other activities are permitted under this Policy.

7. Prohibited Activities

The following are expressly prohibited under this Policy:

7.1 **Processing without Assent.**
Evaluating eligibility, retaining substantive content, or progressing a Submission without recorded Assent, except for minimal routing and risk-containment actions necessary to obtain Assent or decline processing.

7.2 **Processing outside Authorised Channels.**
Treating materials received through non-authorised routes (e.g., uncontrolled direct messages, informal email chains, social media inboxes, or ad hoc file drops) as accepted Submissions eligible for processing.

7.3 **Intake-stage analysis or judgement.**
Forming opinions, inferences, conclusions, or determinations regarding the truth, intent, wrongdoing, or significance of a Submission at intake.

7.4 **Acceptance of unlawful or coercive material.**
Accepting Submissions where the declared provenance indicates coercion, intrusion, deception, unlawful access, or other acquisition methods inconsistent with lawful and ethical handling.

7.5 **Harassment, defamation, or targeting intent.**
Accepting Submissions that are manifestly intended to harass, intimidate, stalk, extort, defame, or otherwise target individuals unlawfully or in bad faith.

7.6 **Retention of ineligible substantive content.**
Retaining substantive content of rejected submissions beyond what is strictly necessary for intake auditability, risk containment, and legal defence, as limited by this Policy.

7.7 **Assurances to submitters.**
Providing commitments or representations regarding outcomes, acceptance, investigation, publication, or any action beyond the intake decision.

8. Procedural Requirements

8.1 **Mandatory Intake Sequence.**
All Submissions must undergo the following procedure:

a) **Receipt:** Submission received only via an Authorised Channel.
b) **Assent Capture:** submitter is presented with this Policy and Assent is recorded via an accepted mechanism.
c) **Eligibility Data Capture:** submitter provides a lawful basis declaration and minimal provenance details required for eligibility evaluation.
d) **Completeness Screening:** intake desk checks whether required eligibility information is present.
e) **Risk Triage:** intake desk identifies presence of PII / Special Category Data for containment routing only.
f) **Eligibility Determination:** intake desk records an eligibility outcome: Accept / Reject / Pending (Assent or missing declarations).
g) **Intake Audit Record:** a decision record is created containing the minimum auditable metadata required to evidence due process and compliance.
h) **Disposition:** material is progressed (Accepted) or disposed/contained (Rejected/Pending) in accordance with Sections 9–11.

8.2 **No Deviation.**
No deviation from the mandatory intake sequence is permitted. Any deviation constitutes a breach under Section 11.

9. Safeguards & Risk Controls

9.1 **Data Minimisation at Intake.**
The Organisation will minimise processing at intake. Eligibility evaluation is performed using the minimum information necessary, and the Organisation will not solicit additional personal data beyond what is required to assess eligibility and route the Submission appropriately.

9.2 **PII and Special Category Data Handling at Intake.**
Where a Submission appears to contain PII or Special Category Data, the intake desk will apply heightened containment controls. Intake does not legitimise such material. Eligibility may be denied on risk grounds even where the submitter asserts a lawful basis.

9.3 **Retention Controls for Rejected Submissions.**
For Ineligible Submissions, the Organisation will, as a default position, retain only minimal audit metadata sufficient to evidence the intake decision and to defend against misuse allegations. Substantive content of rejected materials will be securely deleted or quarantined pending resolution of legal-risk concerns, as determined under Section 11.

9.4 **Authorised Channel Controls.**
The Organisation will operate intake routes that support Assent capture and audit logging. Material received outside Authorised Channels may be deleted without review, or may be redirected to an Authorised Channel prior to any processing.

9.5 **Intake Role Separation.**
Eligibility assessment under this Policy is separated from investigative or analytical functions. Personnel performing eligibility screening are not authorised, under this Policy, to conduct investigation, analysis, or publication.

9.6 **Bad-Faith and Malicious Submission Controls.**
Indicators of bad faith—such as repeated anonymous targeting, inconsistent provenance statements, coercive intent signals, or requests for unlawful outcomes—trigger rejection and may trigger restriction of further submissions from the same source or channel.

9.7 **Non-endorsement Safeguard.**
Acceptance under this Policy is procedural and does not constitute endorsement, validation, or confirmation of accuracy, truth, or completeness.

10. Enforcement & Compliance Mechanisms

10.1 **Hard Gating.**
The Organisation enforces intake gating such that Submissions cannot progress to subsequent stages without an eligibility outcome recorded under this Policy.

10.2 **Assent Evidence Controls.**
The Organisation maintains verifiable records of Assent to support enforcement and defence. Absence of Assent blocks processing.

10.3 **Audit Logging.**
The Organisation records intake decisions and supporting metadata in a manner designed for audit and evidentiary review, including timestamps, channel identifiers, decision outcomes, and applicable Policy version.

10.4 **Operational Compliance Checks.**
The Organisation may conduct periodic internal compliance checks to confirm intake behaviour aligns with this Policy and to identify procedural drift.

11. Breach Handling & Remediation

11.1 **Breach Definition.**
A breach of this Policy includes, without limitation:

a) processing eligibility without Assent
b) treating non-authorised channel materials as eligible Submissions
c) conducting analysis or judgement at intake
d) retaining substantive rejected material contrary to retention controls
e) bypassing the mandatory intake sequence

11.2 **Containment.**
Upon detection or credible allegation of a breach, the Organisation will apply immediate containment measures appropriate to the breach type, which may include quarantine of materials, suspension of processing, and restriction of access pending review.

11.3 **Corrective Action Record.**
The Organisation will create an internal breach record sufficient to evidence detection, containment, corrective action, and closure. This record is maintained as an operational defence artefact and does not constitute publication.

11.4 **Remediation.**
Remediation may include re-performing intake under correct procedure, secure deletion of improperly retained materials, retraining or access restriction for personnel, and review of intake channel controls.

11.5 **Engagement Consequences.**
The Organisation reserves the right to void or suspend engagement activities that depend upon a breached intake pathway until procedural integrity is restored.

12. Limitation of Liability

12.1 **Scope-Limited Allocation of Responsibility.**
Within the scope of intake eligibility, the Organisation's role is to apply procedural acceptance criteria and risk controls. The Organisation does not warrant that Submissions will be accepted, investigated, analysed, or published, and does not guarantee any outcome.

12.2 **No Liability for Non-Acceptance or Non-Progression.**
The Organisation is not liable for decisions to reject, quarantine, decline, suspend, or not progress a Submission under this Policy.

12.3 **No Liability for Submitter Misconduct.**
The Organisation is not liable for consequences arising from a submitter's unlawful acquisition, provision, misrepresentation, or misuse of materials, including where the submitter has misdescribed provenance or lawful basis.

12.4 **No Liability for Reliance Beyond Stated Scope.**
The Organisation is not liable for any reliance by submitters or third parties on anticipated outcomes, implied assurances, or uses of intake-stage status beyond the strictly procedural meaning of eligibility.

12.5 **No Exclusion Where Prohibited by Law.**
Nothing in this Policy limits liability to the extent such limitation is prohibited by applicable law.

13. Non-Delegation & Non-Expansion Clause

13.1 **No Delegation.**
This Policy does not confer investigative, analytical, archival, publication, enforcement, or decision-making authority beyond intake eligibility screening.

13.2 **No Expansion.**
This Policy may not be interpreted to authorise activity outside its defined scope, to override other organisational controls, or to create any entitlement to services beyond procedural eligibility evaluation.

13.3 **No Legal Determination.**
Eligibility decisions under this Policy are risk-based procedural decisions and do not constitute determinations of legality, wrongdoing, or liability as a matter of law.

14. Jurisdiction & Governing Law

14.1 **Governing Law.**
This Policy is governed by the laws of **England and Wales**.

14.2 **Forum.**
Subject to mandatory legal requirements that cannot be excluded, disputes arising from or materially connected to this Policy shall fall within the jurisdiction of the courts of **England and Wales**.

14.3 **Mandatory Compliance Carve-Out.**
Nothing in this section is intended to disapply mandatory statutory obligations that may apply based on the location of processing, the location of data subjects, or other non-excludable legal requirements.

15. Amendments & Version Control

15.1 **Amendment Right.**
This Policy may be amended solely by the Organisation.

15.2 **Publication and Effect.**
Amendments take effect upon publication of an updated version number and effective date.

15.3 **Acceptance of Updates.**
Continued engagement, commissioning, submission, or use of intake channels after publication of an amended version constitutes acceptance of the amended Policy.

15.4 **Version Evidence.**
The Organisation will retain the version identifier associated with recorded Assent and intake decision records.

16. Supremacy Within Scope

16.1 **Authoritative Within Scope.**
Within the domain of evidence intake eligibility, this Policy is authoritative and controls intake eligibility decisions.

16.2 **No Force Outside Scope.**
Outside the domain defined in Section 4, this Policy has no force and may not be construed to govern other organisational functions.