

Evidence Rejection & Referral Policy

Department: Evidence Intake & Verification Desk

Policy ID: EIV-08

Version: 1.0

Effective Date: Upon Publication



1. Policy Title

Evidence Rejection & Referral Policy

2. Authority & Legal Standing

2.1 Binding Instrument.

This Evidence Rejection & Referral Policy (“Policy”) is a binding operational and contractual instrument governing the lawful rejection, containment, disposal, retention-limitation, and referral of Submissions that are determined to be ineligible for further processing at the intake and verification stage.

2.2 Condition of Processing.

Where a Submission fails to satisfy one or more mandatory intake requirements, or is blocked under any applicable intake-stage policy, the Organisation must apply a rejection or referral disposition in accordance with this Policy. No discretionary continuation is permitted.

2.3 Evidentiary Reliance.

This Policy is drafted to be relied upon in judicial, regulatory, arbitral, oversight, and audit contexts as evidence that the Organisation applies structured, proportionate, and non-punitive handling of rejected materials and does not retain, exploit, or repurpose ineligible content.

3. Purpose

3.1 Primary Objective.

The purpose of this Policy is to ensure that Submissions rejected at intake are handled in a manner that is lawful, ethical, proportionate, auditable, and defensible, and that prevents the Organisation from becoming a repository, amplifier, or recycler of unlawful, harmful, or procedurally defective material.

3.2 Protective Objective.

This Policy exists to protect submitters, third parties, the public, and the Organisation by ensuring that rejection decisions do not result in unnecessary data retention, covert processing, retaliatory handling, or informal onward disclosure.

3.3 Non-Determination.

Rejection or referral under this Policy does not constitute a determination of truth, falsity, legality, wrongdoing, liability, or credibility. It is a procedural disposition only.

4. Scope & Applicability

4.1 Scope.

This Policy applies exclusively to the handling of Submissions that are rejected, blocked, or deemed ineligible at the intake and verification stage.

4.2 Applicability.

This Policy applies to:

All Submissions received via Authorised Channels

All rejection decisions arising under intake-stage policies

All personnel, volunteers, contractors, and systems involved in intake disposition

All commissioned, pro bono, and public-interest submissions rejected at intake

4.3 Scope Limitation Clause.

This Policy does not govern investigation, analysis, publication, disciplinary action, or external enforcement. It governs rejection and referral handling only.

5. Definitions (Local Only)

For the purposes of this Policy only:

5.1 Rejected Submission.

A Submission determined to be ineligible for further processing under one or more intake-stage policies.

5.2 Referral.

A procedural signposting action directing a submitter to an external authority, support body, or appropriate channel without transferring substantive content.

5.3 Disposition Record.

The auditable record documenting the rejection or referral outcome.

5.4 Minimal Audit Metadata.

The smallest set of non-substantive data required to evidence that a Submission was received and disposed of lawfully.

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 Reject Submissions that fail intake eligibility, conflict screening, lawful basis verification, PII triage, or bad-faith screening requirements.

6.2 Dispose of rejected Submissions through secure deletion, containment, or minimal retention consistent with risk posture.

- 6.3 Retain only minimal audit metadata necessary for compliance and defence.
- 6.4 Provide neutral, non-substantive notices of rejection to submitters.
- 6.5 Refer submitters to external bodies where appropriate, without transferring content.
- 6.6 Restrict future submissions where patterned abuse has been identified.

No other activities are permitted under this Policy.

7. Prohibited Activities

The following are expressly prohibited:

- 7.1 Retaining substantive content of rejected Submissions beyond what is strictly necessary for auditability or legal defence.
- 7.2 Repurposing rejected materials for investigation, analysis, training, publication, or internal reference.
- 7.3 Informally sharing rejected materials internally or externally.
- 7.4 Providing feedback that could enable submitters to refine harmful, coercive, or abusive tactics.
- 7.5 Reframing rejected Submissions under alternative pathways to bypass intake controls.
- 7.6 Treating rejection as punitive, retaliatory, or adversarial.

8. Procedural Requirements

8.1 Mandatory Rejection Sequence.

Every rejected Submission must undergo the following steps:

- a) Rejection Trigger Identification — identify the policy basis for rejection
- b) Disposition Determination — select reject, reject-and-refer, or contain
- c) Content Handling Decision — delete, quarantine, or minimise retention
- d) Disposition Record Creation — log outcome and rationale
- e) Submitter Notification (where appropriate) — issue neutral notice

8.2 No Deviation.

Deviation from this sequence constitutes a breach.

9. Safeguards & Risk Controls

9.1 Default Deletion Posture.

The default posture for rejected Submissions is secure deletion of substantive content as soon as practicable following disposition.

9.2 Minimal Retention Exception.

Where necessary for legal defence, regulatory compliance, or abuse-pattern management, the Organisation may retain minimal audit metadata only. This metadata must not include substantive content.

9.3 Containment Controls.

Where immediate deletion is not appropriate due to legal-risk considerations, rejected content must be quarantined under strict access controls pending resolution.

9.4 Referral Safeguards.

Referrals must be informational only. The Organisation must not transfer content, endorse allegations, or imply investigative findings.

9.5 Non-Endorsement Safeguard.

Rejection or referral does not imply validation, dismissal, or judgement of content.

10. Enforcement & Compliance Mechanisms

10.1 Hard Gating.

Rejected Submissions must be technically and procedurally blocked from all onward workflows.

10.2 Audit Logging.

Disposition Records must include:

- Policy basis for rejection

- Disposition type

- Timestamp

- Responsible role or system

- Retention or deletion action taken

10.3 Periodic Review.

The Organisation may review rejection patterns to detect misuse or systemic intake risks.

11. Breach Handling & Remediation

11.1 Breach Definition.

A breach includes:

- Retention of rejected substantive content

- Informal sharing of rejected materials

- Failure to apply deletion or containment

- Bypassing rejection controls

11.2 Containment.

On detection, affected materials are immediately contained or deleted.

11.3 Remediation.

Remediation may include corrective deletion, access restriction, retraining, and procedural reinforcement.

12. Limitation of Liability

12.1 The Organisation's role is procedural disposition, not adjudication.

12.2 The Organisation is not liable for consequences arising from rejection or referral decisions.

12.3 The Organisation is not responsible for submitter reliance on referral signposting.

12.4 Nothing limits liability where prohibited by law.

13. Non-Delegation & Non-Expansion Clause

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

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

13.3 Disposition decisions are procedural, not legal determinations.

13.4 Referral does not imply severity, credibility, urgency, or merit; it is procedural signposting only.

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.

Version identifiers are retained with Disposition Records.

16. Supremacy Within Scope

Within the domain of intake-stage rejection and referral handling, this Policy is authoritative.

Outside that domain, it has no force.