Malicious or Bad-Faith Submission Policy

Department: Evidence Intake & Verification Desk
Policy ID: EIV-07
Version: 1.0
Effective Date: Upon Publication

1. Policy Title

Malicious or Bad-Faith Submission Policy

2. Authority & Legal Standing

2.1 **Binding Instrument.**
This Malicious or Bad-Faith Submission Policy ("Policy") is a binding operational and contractual instrument governing the identification, assessment, handling, rejection, containment, and disposition of Submissions that exhibit malicious intent, bad faith, coercive purpose, or abusive misuse of the Organisation's intake systems.

2.2 **Condition of Processing.**
No Submission may proceed beyond intake screening if it is assessed, under this Policy, to constitute or materially indicate malicious or bad-faith intent. Identification under this Policy is a hard gate that blocks onward processing.

2.3 **Reliance and Evidentiary Function.**
This Policy is drafted to be relied upon in judicial, regulatory, arbitral, oversight, and audit contexts as evidence that the Organisation actively prevents its systems from being used to facilitate harassment, extortion, reputational attacks, coercive leverage, or unlawful targeting.

3. Purpose

3.1 **Primary Objective.**
The purpose of this Policy is to prevent the Organisation from being used as an instrument for malicious activity, including but not limited to harassment, intimidation, retaliation, defamation laundering, extortion, doxxing, coercive disclosure, or strategic reputational harm.

3.2 **Protective Objective.**
This Policy exists to protect individuals, organisations, the public, and the Organisation itself from harm arising where a Submission's intent, pattern, or surrounding context demonstrates bad faith rather than legitimate evidentiary or public-interest purpose.

3.3 **Non-Determination.**
Assessment under this Policy does not determine the truth or falsity of submitted material. It determines only whether the **intent, pattern, or posture** of submission renders it procedurally unacceptable for processing.

4. Scope & Applicability

4.1 **Scope.**
This Policy applies exclusively at the evidence intake and verification stage and governs screening for malicious or bad-faith characteristics prior to investigation, analysis, archival handling, or publication consideration.

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

All Submissions received via Authorised Channels
All submitters, commissioning parties, intermediaries, and representatives
All internal personnel, volunteers, contractors, and systems involved in intake handling
All commissioned, pro bono, and public-interest submissions at intake

4.3 **Scope Limitation Clause.**
This Policy does not govern investigative findings, analytical conclusions, editorial judgement, or legal determinations. It governs intake-stage admissibility based on intent and misuse risk only.

5. Definitions (Local Only)

For the purposes of this Policy only:

5.1 **Malicious Submission.**
A Submission intended to cause harm, harassment, intimidation, retaliation, extortion, coercion, or unlawful targeting, regardless of the factual accuracy of its contents.

5.2 **Bad-Faith Submission.**
A Submission made with deceptive, abusive, manipulative, or ulterior motives inconsistent with legitimate evidentiary, research, or public-interest purposes.

5.3 **Indicator.**
Any behavioural, contextual, linguistic, relational, or procedural signal suggesting malicious or bad-faith intent.

5.4 **Patterned Abuse.**
Repeated submissions or interactions exhibiting consistent hostile or abusive indicators.

5.5 **Disposition.**
The intake-stage outcome applied to a Submission under this Policy.

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 Screen Submissions for indicators of malicious or bad-faith intent.

6.2 Assess intent based on submission context, declared purpose, metadata, interaction patterns, and conflict indicators.

6.3 Reject, restrict, contain, or refer Submissions assessed as malicious or bad-faith.

6.4 Record screening outcomes and rationale sufficient for audit and defence.

6.5 Apply submission-source restrictions where patterned abuse is identified.

No other activities are permitted under this Policy.

7. Prohibited Activities

The following are expressly prohibited:

7.1 Processing Submissions that meet malicious or bad-faith criteria.

7.2 Treating factual plausibility as justification to overlook hostile intent.

7.3 Using this Policy to suppress legitimate dissent, whistleblowing, or lawful criticism where bad-faith indicators are absent.

7.4 Escalating malicious Submissions into investigation, analysis, or publication pathways.

7.5 Providing submitters with feedback that enables refinement of abusive tactics.

7.6 Representing rejection under this Policy as a determination of credibility or truth.

8. Procedural Requirements

8.1 **Mandatory Screening Sequence.**

Each Submission must undergo the following:

a) Indicator Review — identify behavioural, contextual, and procedural signals
b) Pattern Check — assess prior interactions for repeated abuse indicators
c) Intent Classification — classify posture as neutral, concerning, or malicious
d) Disposition Assignment — apply outcome defined in Section 9
e) Audit Record Creation — record decision and rationale

8.2 **No Deviation.**
Deviation from this sequence constitutes a breach.

9. Safeguards & Risk Controls

9.1 **Malicious / Bad-Faith Indicators (Non-Exhaustive).**

Indicators may include, individually or in combination:

Explicit threats, intimidation, or coercive language
Requests for exposure, punishment, or reputational damage
Submission framed as leverage in disputes or negotiations
Repeated targeting of the same individual or entity
Inconsistent or shifting narratives indicating manipulation
Attempts to bypass safeguards or pressure intake personnel
Evidence of extortion, blackmail, or retaliatory motivation
Patterns of anonymous or serial hostile submissions

9.2 **Intent Classifications.**

Each Submission must be assigned one:

M0 — No Apparent Malice
M1 — Concerning Indicators Present
M2 — Malicious or Bad-Faith Intent
M3 — Prohibited / Abusive Use

9.3 **Default Dispositions.**

M0: Proceed subject to other intake gates
M1: Restrict, escalate, or require clarification
M2: Reject and contain; no onward processing
M3: Reject outright; consider submission blocking

9.4 **Non-Endorsement Safeguard.**
Rejection under this Policy does not validate or invalidate content; it prevents misuse.

10. Enforcement & Compliance Mechanisms

10.1 **Hard Gating.**
Workflow controls must prevent progression once a malicious disposition is recorded.

10.2 **Audit Logging.**
Records must include:

Intent classification
Disposition
Timestamp
Responsible role or system
High-level rationale (non-substantive)

10.3 **Pattern Mitigation Controls.**
Where repeated abuse occurs, the Organisation may restrict or disable submission access from the source or channel.

11. Breach Handling & Remediation

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

Processing malicious submissions
Failing to apply disposition controls
Allowing abusive progression
Suppressing indicators

11.2 **Containment.**
Affected materials are immediately contained or removed from processing pathways.

11.3 **Remediation.**
Remediation may include re-screening, rejection, deletion, access restriction, and procedural reinforcement.

12. Limitation of Liability

12.1 The Organisation assesses procedural risk, not motive certainty.

12.2 The Organisation is not liable for submitter misrepresentation or concealed intent.

12.3 No liability arises from refusal to process malicious or bad-faith Submissions.

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 cannot be used to expand organisational scope or suppress lawful engagement.

13.3 Screening determinations are procedural, 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.
Version identifiers are retained with screening records.

16. Supremacy Within Scope

Within the domain of intake-stage malicious and bad-faith submission screening, this Policy is authoritative.

Outside that domain, it has no force.