Personally Identifiable Information (PII) Triage Policy

Department: Evidence Intake & Verification Desk
Policy ID: EIV-05
Version: 1.0
Effective Date: Upon Publication

1. Policy Title

Personally Identifiable Information (PII) Triage Policy

2. Purpose

The purpose of this Policy is to establish a mandatory, enforceable, and auditable framework for identifying, triaging, containing, and restricting Personally Identifiable Information ("PII") and Special Category Data at the point of intake, prior to any investigation, analysis, publication consideration, or broader internal circulation.

This Policy exists to ensure that the Organisation does not become a processor, distributor, amplifier, or storage conduit of unnecessary personal data, and that any personal data that is received is handled under strict minimisation, containment, and lawful basis controls.

This Policy functions as a protective barrier to prevent the Organisation's systems, staff, volunteers, and outputs from being used to facilitate harassment, doxxing, coercion, intimidation, discrimination, reputational harm, or any outcome that could resemble extrajudicial targeting. Where PII cannot be justified as necessary, proportionate, and procedurally lawful within the Organisation's controls, it must not be processed further.

3. Binding Authority & Legal Standing

This Policy is a binding internal governance instrument and a contractual condition of engagement with the Organisation.

By submitting materials, commissioning services, or interacting with the Organisation's intake systems, all submitters and clients agree that:

The Organisation may apply strict containment, restriction, redaction, rejection, deletion, or referral decisions where PII or Special Category Data is present or suspected.

The Organisation will not process PII beyond the minimum necessary for lawful intake triage and risk containment unless and until relevant gating requirements are met, including lawful basis verification and other applicable controls.

The Organisation may require clarification, re-submission, or removal of unnecessary personal data as a condition of continued processing.

This Policy is designed to be relied upon as evidence of procedural compliance, data minimisation, and risk containment in judicial, regulatory, oversight, and audit contexts.

4. Scope of Application

This Policy applies to:

1. All submissions received through authorised intake channels, whether commissioned or unsolicited.
2. All intake-stage activities undertaken by the Evidence Intake & Verification Desk.
3. All materials that contain, appear to contain, or could reasonably be inferred to contain PII, Special Category Data, or data capable of re-identifying individuals when combined with other information.
4. All personnel, volunteers, systems, and workflows that view, route, store, label, or otherwise interact with submissions during intake triage.
5. This Policy governs PII triage only. It does not authorise investigation, analysis, enforcement, publication, or disclosure of personal data. Any onward processing must be justified and governed under the relevant policies and engagement instruments.

5. Core Principles

The Organisation operates on the following non-negotiable principles:

1. PII is toxic by default at intake unless proven necessary, proportionate, and procedurally justified.
2. Minimise first. Restrict second. Reject third. Escalate only where lawful and necessary.
3. Assent is required for processing beyond minimal routing and triage.
4. Lawful basis must be verified before any non-triage processing of PII.
5. PII must not be treated as "value". It is a liability and a harm vector.
6. Public interest does not equal public disclosure. Presence of PII increases restriction, not permissiveness.
7. The Organisation must not become a doxxing engine, harassment vector, or targeting service.
8. These principles are enforced procedurally, not aspirationally.

6. Definitions

For the purposes of this Policy:

Personally Identifiable Information (PII) includes any information relating to an identified or identifiable natural person, including direct identifiers (such as names, addresses, phone numbers, email addresses, government identifiers) and indirect identifiers (such as unique combinations of attributes that enable identification).

Special Category Data includes any data treated as special category under applicable data protection law to the extent applicable, including data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for identification, health data, sex life, or sexual orientation.

Triage means intake-stage identification and handling actions performed solely to contain risk, minimise processing, and determine whether a submission can proceed into controlled workflows.

Containment means restricting access, reducing exposure, preventing replication, and limiting processing to the minimum necessary for triage decisions.

Redaction means removal or masking of PII from a submission or any internal representation of it, with the goal of preventing unnecessary personal data processing.

PII Present means that PII is confirmed to exist within the submission.

PII Suspected means that PII may exist within the submission but cannot be confirmed without greater exposure or processing than is justified at intake.

7. Mandatory PII Triage Requirements

7.1 Default Intake Posture Where PII Is Present or Suspected

Where PII is present or suspected, the default posture is:

1. Contain the submission immediately.
2. Restrict access to the minimum number of authorised roles required to perform triage.
3. Minimise handling and avoid copying, exporting, or reformatting.
4. Prevent onward routing beyond intake triage until a PII triage outcome is recorded.
5. This posture applies regardless of whether the submission is commissioned or public.

7.2 Minimum Necessary Handling Only

At intake, the Organisation may perform only the minimum handling required to:

1. Confirm whether PII is present or suspected.
2. Determine whether the PII appears necessary for the stated purpose.
3. Determine whether the submission can be processed without the PII.
4. Determine whether the submission must be rejected, restricted, or returned for re-submission without unnecessary PII.
5. Triage must not expand into investigative analysis, profiling, inference, or judgement.

7.3 PII Categorisation for Triage Decisions

The intake desk must categorise PII into one of the following triage categories, and this categorisation must be recorded:

Category P1 — Unnecessary PII
PII is present but not necessary for eligibility, classification, or lawful processing. This triggers minimisation actions and may trigger rejection if the submitter refuses to minimise.

Category P2 — Potentially Necessary PII
PII may be necessary but cannot be justified at intake without lawful basis verification and downstream constraints. This triggers restriction and gating.

Category P3 — High-Risk PII
PII indicates heightened risk of harm if mishandled (e.g., home address, phone number, government identifiers, sensitive location data, intimate material, protected characteristics, or any material likely to enable targeting). This triggers strict containment and conservative disposition.

Category P4 — Special Category Data
Special Category Data is present or suspected. This triggers maximum restriction, conservative triage, and heightened lawful basis scrutiny.

7.4 Commissioned vs Public Submissions

Commissioned submissions may still be rejected or restricted where PII is unnecessary, excessive, unlawful, or high-risk. Payment, commissioning status, or claimed urgency does not override triage controls.

Public submissions containing PII are treated as higher-risk by default, particularly where the submission appears to target or identify individuals, includes contact details, or indicates harassment intent.

8. Prohibited PII Handling Conduct

Under this Policy, the Organisation must not:

1. Treat PII as a default intake requirement or encourage submitters to provide additional personal details.
2. Process, enrich, correlate, compile, or profile individuals at intake.
3. Create a searchable index of individuals from intake-stage PII.
4. Publish, disclose, or externally share PII received at intake.
5. Use PII triage as a pretext for investigative activity.
6. Retain unnecessary PII where redaction, deletion, or return for re-submission is feasible.

7. Facilitate doxxing, harassment, intimidation, discrimination, or reputational punishment through handling choices or downstream routing.
8. Any breach of these prohibitions is a material policy violation.

9. PII Triage Outcomes (Mandatory)

Each submission where PII is present or suspected must receive one triage outcome, recorded as the intake desk's controlling decision for the purposes of routing:

Outcome T1 — Proceed Without PII (Redaction/Minimisation Required)
PII is unnecessary. The submission may proceed only if PII is removed, masked, or otherwise minimised before onward processing.

Outcome T2 — Restrict & Hold Pending Lawful Basis Verification
PII may be necessary. The submission is held in restricted access until lawful basis verification is completed and recorded, and until any additional gating conditions are satisfied.

Outcome T3 — Reject for Unnecessary/Excessive PII
PII is unnecessary, excessive, or unjustified, and the Organisation will not accept the submission as provided. The Organisation may request resubmission without PII, but is not obligated to do so.

Outcome T4 — Reject for High-Risk Targeting Indicators
PII presence indicates targeting, harassment, intimidation, coercion, or other unacceptable risk. The submission is rejected without onward processing.

Outcome T5 — Contain & Escalate for Special Category Risk Review
Special Category Data is present or suspected. The submission is contained and restricted, and cannot proceed unless and until an explicit risk review decision authorises limited onward processing under strictly controlled conditions.

No submission containing PII may proceed beyond intake triage without one of the above outcomes recorded.

10. Redaction and Minimisation Requirements

Where minimisation is feasible and consistent with intake controls:

1. PII must be removed or masked in any internal working representation.
2. Only the minimum retained personal data necessary for legitimate processing may remain, and only under restricted access.
3. Redaction must not be performed in a way that introduces interpretive commentary or changes meaning beyond removal of identifiers.
4. Where redaction cannot be performed without unacceptable exposure or risk at intake, the Organisation must prefer restriction, rejection, or re-submission rather than attempting complex handling.

5. The Organisation is not obligated to provide redaction services to submitters, and may require submitters to provide a compliant version as a condition of processing.

11. Access Restrictions and Containment Controls

Where PII is present or suspected:

1. Access is limited to authorised intake roles only, with no general volunteer visibility.
2. Any onward routing must enforce least privilege and must be consistent with the triage outcome.

Copying, exporting, external forwarding, or out-of-band sharing is prohibited.

Internal communication about the submission must avoid repeating PII unless strictly necessary, and must prefer identifiers (case number, submission identifier) over personal names or details.

Containment measures must remain in place until triage outcome execution is complete and any required gating checks have been satisfied.

12. Interaction with Other Policies

This Policy operates in conjunction with, and does not override:

1. Evidence Intake Eligibility Policy (EIV-01)
2. Source Classification Policy (EIV-02)
3. Consent & Lawful Basis Verification Policy (EIV-04)
4. Conflict of Interest Screening Policy (if relevant to who can access PII)
5. Malicious or Bad-Faith Submission Policy (where targeting intent is suspected)
6. Evidence Rejection & Referral Policy (for final disposition and external signposting)
7. Intake Audit Logging Policy (for procedural evidencing)
8. Where any conflict arises, the most restrictive and risk-containment posture applies.

13. Auditability & Recordkeeping

All PII triage actions must be recorded in accordance with the Organisation's audit requirements, including:

1. Whether PII was present or suspected.
2. The PII category (P1–P4) assigned.
3. The triage outcome (T1–T5) assigned.
4. The date and time of the decision.
5. The responsible role or system.

6. Any minimisation actions required or executed.
7. Failure to record triage outcome renders onward processing non-compliant.
8. Audit records must be limited to the minimum necessary metadata and must not become a secondary store of PII.

14. Enforcement & Breach Handling

Non-compliance with this Policy results in:

1. Immediate suspension of affected processing.
2. Containment of the relevant submission(s).
3. Internal review of access and handling events.
4. Corrective action including deletion of improperly retained PII or reversal of unauthorised routing.
5. Restriction or termination of access for personnel, volunteers, or submitters who breach PII handling controls.
6. Repeated or deliberate breaches are treated as material governance failures.

15. Limitation of Responsibility

The Organisation's role at intake is procedural triage and risk containment, not determination of truth, wrongdoing, or entitlement.

The Organisation is not responsible for submitter misconduct, including unlawful acquisition or provision of PII, provided the Organisation applied triage controls in good faith and to the standard required by this Policy.

Nothing in this Policy limits liability where such limitation is prohibited by law.

16. Jurisdiction & Governing Law

This Policy is governed by the laws of England and Wales.

All disputes arising in connection with this Policy fall within the jurisdiction of the courts of England and Wales, subject to mandatory statutory obligations.

17. Amendments & Version Control

This Policy may be amended only by the Organisation.

Amendments take effect upon publication of a revised version. Continued engagement constitutes acceptance of the amended Policy.

18. Supremacy Within Scope

Within the domain of PII identification, triage, containment, minimisation, and restriction at intake, this Policy is authoritative and controlling.

Outside that domain, it has no force.