

Consent & Lawful Basis Verification Policy

Department: Evidence Intake & Verification Desk

Policy ID: EIV-04

Version: 1.0

Effective Date: Upon Publication



1. Policy Title

Consent & Lawful Basis Verification Policy

2. Purpose

The purpose of this Policy is to establish a mandatory, enforceable, and auditable framework governing the verification of consent, assent, and lawful basis prior to any processing of submitted materials beyond minimal intake routing.

This Policy exists to ensure that the Organisation does not process personal data, sensitive data, or any submission-derived information without a clearly identified, verified, and procedurally defensible lawful basis, and that such verification is performed prior to any investigative, analytical, or evaluative activity.

This Policy functions as a **legal firewall**. Where lawful basis or valid consent cannot be established to a defensible standard, processing must not proceed.

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:

- No processing beyond minimal routing will occur without verification under this Policy.
- The Organisation may refuse, suspend, restrict, or terminate processing where lawful basis or consent is absent, defective, withdrawn, or unverifiable.
- The Organisation's verification determinations under this Policy are final for intake-stage purposes.

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

4. Scope of Application

This Policy applies to:

- All submissions received through authorised intake channels;

- All materials containing or potentially containing personal data;
- All intake-stage actions prior to investigation, analysis, reporting, or publication;
- All personnel, volunteers, systems, and workflows operating within the Evidence Intake & Verification Desk.

This Policy governs **verification only**. It does not itself authorise investigation, analysis, enforcement, publication, or disclosure.

5. Core Principles

The Organisation operates on the following non-negotiable principles:

1. **No lawful basis, no processing.**
2. **Consent is never assumed.**
3. **Assent is not consent.**
4. **Lawful basis must be declared, assessed, and recorded.**
5. **Verification precedes action.**
6. **Withdrawal or invalidity halts processing.**

These principles are enforced procedurally, not aspirationally.

6. Distinction Between Assent, Consent, and Lawful Basis

6.1 Assent

Assent refers to contractual acceptance of the Organisation's policies and terms. Assent is required for engagement but **does not constitute consent for data processing** under data protection law.

Assent enables eligibility screening only.

6.2 Consent

Consent, where relied upon, refers strictly to consent as defined under applicable data protection law. Consent must be freely given, specific, informed, unambiguous, and capable of withdrawal without detriment.

Consent is treated as an **exceptional lawful basis**, not a default.

6.3 Lawful Basis

Lawful basis refers to the legal justification under applicable law permitting processing of personal data.

The Organisation does not rely on implied or assumed lawful basis. A lawful basis posture must be **explicitly declared and verified** prior to processing.

7. Mandatory Lawful Basis Declaration

All submitters or commissioning parties must provide a lawful basis declaration at intake where submitted materials contain, may contain, or may reasonably be inferred to contain personal data.

The declaration must include, at minimum:

- The asserted lawful basis relied upon;
- The relationship of the submitter to the data subject(s);
- The manner in which the data was obtained;
- The purpose for which the data is being submitted;
- Any known restrictions, duties, or prohibitions attached to the data.

Absence of a lawful basis declaration results in automatic suspension of processing.

8. Verification Obligations of the Organisation

The Organisation must verify lawful basis declarations to a standard proportionate to risk, sensitivity, and potential harm.

Verification does **not** require the Organisation to prove the declaration true in fact. It requires the Organisation to determine whether the declaration is:

- Coherent;
- Plausible;
- Non-contradictory;
- Not facially unlawful;
- Not incompatible with known constraints or prohibitions.

Where verification cannot be achieved to a defensible standard, processing must not proceed.

9. Consent Verification Requirements

Where consent is asserted as the lawful basis, the Organisation must verify that:

- Consent is specific to the processing requested;
- Consent was not obtained through coercion or imbalance of power;
- Consent is capable of withdrawal;

- Withdrawal would not create retaliatory, punitive, or coercive effects;
- Evidence of consent exists or can be reasonably demonstrated.

Where any of the above cannot be verified, consent is deemed invalid for intake-stage purposes.

10. Withdrawal of Consent or Lawful Basis Failure

Where consent is withdrawn or lawful basis is invalidated at any stage:

- Processing must immediately cease;
- Materials must be restricted pending disposition under applicable policies;
- No adverse inference may be drawn from withdrawal;
- No continued processing may occur under alternative bases without fresh verification.

Withdrawal does not retroactively legitimise prior unlawful processing.

11. Prohibited Processing Activities

Under this Policy, the Organisation must not:

- Process personal data on the basis of assumed or implied consent;
- Convert contractual assent into data protection consent;
- Proceed where lawful basis is unclear, disputed, or unverified;
- Reframe unlawful material as “public interest” without verification;
- Pressure submitters to recharacterise lawful basis;
- Continue processing after withdrawal or invalidation.

Any such activity constitutes a policy breach.

12. Interaction with Other Policies

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

- Evidence Intake Eligibility Policy;
- Source Classification Policy;
- Personally Identifiable Information Triage Policy;
- Intake Audit Logging Policy;
- Evidence Rejection & Referral Policy.

Where conflict arises, the most restrictive processing posture applies.

13. Auditability & Recordkeeping

All lawful basis and consent verification actions must be recorded in accordance with the Organisation's audit requirements, including:

- Declared lawful basis;
- Verification outcome;
- Date and time of verification;
- Responsible role or system;
- Any conditions, limitations, or restrictions applied.

Failure to record verification renders processing non-compliant.

14. Enforcement & Breach Handling

Non-compliance with this Policy results in:

- Immediate suspension of affected processing;
- Mandatory internal review;
- Corrective action or termination of access where required;
- Referral to governance or disciplinary mechanisms where applicable.

Repeated or deliberate breaches are treated as material governance failures.

15. Limitation of Responsibility

The Organisation verifies procedural defensibility, not factual truth.

The Organisation is not responsible for inaccuracies, omissions, or misrepresentations in submitter-provided declarations, provided that verification under this Policy was conducted in good faith and to the required standard.

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 consent and lawful basis verification, this Policy is authoritative and controlling. Outside that domain, it has no force.