Anti-Money Laundering (AML) Policy
For Stanford & Green Limited

1. Purpose

This Anti-Money Laundering (AML) Policy sets out the framework that Stanford & Green Limited has adopted to prevent, detect, and report any instances of money laundering, terrorism financing, or other financial crimes in connection with its enforcement activities.

We are committed to conducting our business in accordance with the UK Proceeds of Crime Act 2002, Money Laundering Regulations 2017.

2. Scope

This Policy applies to:

- All employees, agents, enforcement officers, contractors, and directors of Stanford & Green Limited.

- All activities involving the collection of payments, seizure and sale of goods, and the enforcement of court orders.

3. Policy Statement

Stanford & Green Limited is dedicated to:

- Identifying and mitigating the risk of being used for money laundering or financial crime.

- Ensuring that enforcement officers and employees remain vigilant to signs of suspicious financial behaviour.

- Complying fully with statutory reporting obligations.

- Cooperating with law enforcement and relevant authorities.

4. Roles and Responsibilities

- Money Laundering Reporting Officer (MLRO): Martin Stanford is responsible for:
  - Oversight of AML compliance.
  - Receiving internal reports of suspicious activities.
  - Reporting to authorities (e.g., the UK's National Crime Agency (NCA)).

- All Staff and Agents:
  - Must report any suspicions promptly to the MLRO.
  - Must complete mandatory AML training annually.
  - Must follow correct procedures when receiving cash or dealing with valuable assets.

5. Risk Areas for Enforcement Work

Particular attention must be paid to:

- Large Cash Payments: Payments over [e.g., £5,000] must be scrutinised and, where necessary, declined or reported.

- Suspicious Instructions: Attempts by debtors or third parties to settle debts through unusual methods (e.g., with large amounts of cash, third-party payments, foreign currencies).

- Asset Disposal: Handling and sale of seized goods must be transparent, with full documentation.

- Third Party Payments: Payments made by unrelated third parties require additional verification and assessment.

6. Customer Due Diligence (CDD)

While Enforcement Agencies primarily act on behalf of creditors, local authorities and the courts, it remains essential to:

- Verify the identity of debtors when accepting payments directly.

- Record details of any party making substantial payments.

- Understand the relationship between any third party and the debtor.

Enhanced Due Diligence (EDD) measures should be applied if:

- The payer is a Politically Exposed Person (PEP).

- The transaction is unusually complex or lacks an apparent legal purpose.

7. Reporting Suspicious Activity

- Any suspicious behaviour must be reported internally to the MLRO using the Suspicious Activity Reporting (SAR) Form.

- The MLRO will determine whether a report needs to be filed with the UK's National Crime Agency (NCA)].

- Staff must not tip off any person about a suspicion or report (offense under law).

8. Record Keeping

Records must be maintained securely for at least 5 years from:

- The date of transaction/payment.
- The end of enforcement action or debtor interaction. Records include:
- Payment receipts.
- Asset seizure documentation.
- SARs filed internally and externally.

9. Training

All staff and enforcement agents will receive AML training annually, covering:

- Recognising suspicious behaviour or transactions.
- Proper reporting procedures.
- Legal obligations and penalties for non-compliance.

New employees must complete AML induction training within 30 days of starting work.

10. Review

This AML Policy will be reviewed every 12 months and updated as needed to reflect:

- Changes in legislation or regulatory guidance.
- Emerging risks identified during operational activities.

Approved by: Martin Stanford - Director

8 January 2026