Financial Crime Compliance Policy

(AML / CTF / CPF & Prevention of Tax Evasion Facilitation)

Revision Matrix

SAFO UK Limited (company number 06478031)

Version: [2.1]. Prepared by: [Legal Department / A.C.T. London Limited]. Approved by: [Claudia Barbotto, Managing Director], [20 October 2026]. Policy owner: [Claudia Barbotto, Managing Director]. Next review: [October 2027]. Definitions: in this document, "the Company" means SAFO UK Limited. "SAFO GROUP S.p.A." is the Italian head company of the Group, and "the Group" or "SAFO Group" means SAFO GROUP S.p.A. together with the companies it controls and the Company. This document applies to the Company in the United Kingdom, its directors, employees and all persons acting on its behalf. References to the Group apply to other Group companies only to the extent of their activities in or connected with the United Kingdom.

Version	Date	Subject	Prepared by	Approved By
1.1	05.11.2025	1st Issue	Legal Department	CB
2	07.10.2026	Changed to Group Logo	Managing Director	CB
2.1	20.10.2026	Review against UK legal requirements	A.C.T. London Limited / Legal Department	CB

1. Purpose

This policy defines SAFO UK Limited's ("the company") approach to preventing financial crime, including money laundering, terrorist financing, proliferation financing, and the facilitation of tax evasion.

The company complies with all applicable laws and regulatory requirements, including:

- The Criminal Finances Act 2017 (failure to prevent facilitation of tax evasion)
- The Proceeds of Crime Act 2002 (POCA)
- Applicable Anti-Money Laundering (AML), Counter-Terrorist Financing (CTF), and Counter-Proliferation Financing (CPF) regulations in all jurisdictions in which the company operates
- Applicable financial sanctions regimes, including UK financial sanctions

The company maintains proportionate systems and controls designed to detect, prevent, and report financial crime risks.

2. Business Risk Context

As an IT development and outsourced services provider, the company recognises specific financial crime risks, including:

- Being used as a vehicle for payment flows (e.g. project billing structures)
- Working with overseas clients and subcontractors
- Providing services that could indirectly support clients engaged in financial crime
- Third-party developers or contractors acting on behalf of the company

Controls are designed to mitigate these risks proportionately and effectively.

3. Scope

This policy applies to:

- Employees, directors, and officers
- Contractors and outsourced developers
- Third-party suppliers and partners

All persons acting on behalf of the company are expected to comply with this policy and related procedures.

4. Policy Statement

The company has a zero-tolerance approach to:

- Money laundering
- Terrorist financing
- Proliferation financing
- Tax evasion and the facilitation of tax evasion
- Fraud, bribery, corruption, and other forms of financial crime

The company is committed to maintaining effective internal controls and compliance procedures designed to ensure compliance with applicable AML and financial crime legislation.

This policy should be read together with the Code of Ethics and Conduct, the Anti-Corruption, Bribery and Fraud Policy and the Whistleblowing Procedure.

5. Governance

- Senior management oversees financial crime compliance and the effectiveness of related controls
- All personnel must report concerns relating to suspected financial crime
- Compliance responsibilities are communicated throughout the organisation
- Independent monitoring arrangements are maintained to test compliance standards and assess the effectiveness of financial crime controls and procedures

6. Risk Assessment

The company conducts periodic and documented risk assessments covering:

- Client type (e.g. corporate vs individual)
- Geography (including high-risk jurisdictions)

- Nature of services (e.g. payment-related systems vs standard development work)
- Delivery model (including the use of subcontractors and outsourced resources)

Risk assessments are reviewed periodically and updated where there are material changes to the business, regulatory environment, or identified risks.

7. Client Due Diligence (CDD)

Before entering into business relationships, the company:

- Verifies client identity (including company registration and ownership where relevant)
- Screens for sanctions, politically exposed persons (PEPs), and adverse information where appropriate
- Applies enhanced due diligence for higher-risk clients or jurisdictions
- Conducts ongoing monitoring proportionate to the assessed level of risk

The company reserves the right to decline or terminate relationships where financial crime concerns cannot be satisfactorily resolved.

8. Payments and Financial Controls

Given the nature of IT services, the company applies practical controls including:

- Accepting payments only via traceable banking channels
- Avoiding cash payments
- Ensuring invoices correspond to legitimate contractual services
- Reviewing and escalating unusual payment requests, including:
    - Third-party payers
    - Offshore payment routing without reasonable justification
    - Requests designed to obscure the source or destination of funds

Internal financial controls are designed to support AML compliance and reduce the risk of financial crime.

9. Third-Party & Contractor Controls

As outsourcing forms part of the company's operating model, the company:

- Performs due diligence on subcontractors, developers, suppliers, and contractors, or appoints subcontractors/developers that belong to the same group and are subject to group compliance policies
- Uses written agreements containing:
    - Compliance obligations
    - Anti-financial crime clauses
    - Rights to terminate for non-compliance
- Monitors third-party activity proportionate to the associated risk

Where outsourced financial crime compliance activities are performed on behalf of clients, the company permits clients, their appointed representatives, and applicable regulatory bodies to inspect, audit, or commission assurance testing of those activities where contractually or legally required.

10. Prevention of Facilitation of Tax Evasion

In line with the Criminal Finances Act 2017, the company maintains reasonable prevention procedures, including:

Prohibitions

- Assisting clients, suppliers, or third parties in evading tax
- Structuring payments or transactions to conceal tax liabilities

Controls

- Due diligence on clients and intermediaries
- Clear contractual terms prohibiting tax evasion
- Review of unusual invoicing or payment structures
- Escalation procedures for concerns

Staff must immediately report any suspicion relating to the facilitation of tax evasion.

11. Suspicious Activity Reporting

Suspicions regarding potential financial crime or irregularities may be reported by employees and third parties through the dedicated online whistleblowing platform accessible via the company website: https://www.safogroup.com/uk/whistleblowing/

Reports may be submitted anonymously and are protected through secure encryption measures to ensure confidentiality and data protection.
The company undertakes to protect any individual reporting suspected or actual crime or irregularity from retaliatory action.
Employees are also required to report suspicions of money laundering in accordance with the Proceeds of Crime Act 2002 (POCA) and internal escalation procedures.
Suspicions must be reported promptly to the Managing Director [or other nominated person], who will decide whether a report should be made to the National Crime Agency. Staff must not discuss the suspicion with the person concerned or take any step that could prejudice an investigation, and must not proceed with a suspicious transaction until authorised.
Where a money laundering event or control failure is identified, the company will conduct a proportionate Root Cause Analysis (RCA) to determine underlying causes, assess control effectiveness, identify remediation actions, and reduce the risk of recurrence.

12. Record Keeping
The company maintains appropriate records relating to:

- Client due diligence
- Contracts and invoices
- Risk assessments
- Training completion
- Internal reviews and investigations

Retention periods align with applicable legal and regulatory expectations.

13. Training
All employees and relevant contractors receive regular financial crime compliance training, including training during induction and periodic refresher training thereafter.
Training covers, where relevant:

- Anti-Money Laundering (AML) obligations
- Counter-terrorist financing and proliferation financing risks
- Reporting suspicions of money laundering under the Proceeds of Crime Act 2002 (POCA)
- Recognising financial crime risks within IT and outsourced services environments
- Red flags such as unusual payment structures, shell companies, and high-risk jurisdictions
- Tax evasion facilitation risks and escalation procedures
- Internal reporting obligations and whistleblowing arrangements

Training records are maintained by the company.

14. Monitoring and Review

- This policy is reviewed at least annually or earlier where required by regulatory, legal, or business changes
- Compliance controls and procedures are subject to periodic monitoring and independent review
- Corrective actions are implemented where deficiencies or weaknesses are identified
- The company seeks continuous improvement of its financial crime compliance framework as the business evolves

15. Breaches
Breaches of this policy may result in:

- Disciplinary action in accordance with the disciplinary procedure in the Employee Handbook
- Termination of contracts or business relationships

- Reporting to relevant authorities or regulators where appropriate

All personnel are expected to cooperate fully with investigations into suspected breaches of this policy.