

Finance Department

Anti-Money Laundering Policy

Version: 1.0
Date: 24 November 2022

Version control

Owner:	Finance Manager
Author:	Data Protection Officer
Approved by:	General Manager
Date of Approval of this Version:	24 November 2022
Next Review Date:	24 November 2025
Version Number:	1.0
Applicable Statutory, Legal or National Best Practice Requirements:	<p>The Proceeds of Crime Act 2002 Money Laundering and Terrorist Financing (Amendment) Regulations 2019 The Terrorism Act 2000 (as amended by The Anti-Terrorism Crime and Security Act 2001 and the Terrorism Act 2006) Criminal Finances Act 2017</p>

This document can only be considered valid when viewed via the itSMF UK website. If this document is printed into hard copy or saved to another location, you must check that the version number on your copy matches that of the one on the itSMF UK website. Approved documents are valid for use after their approval date and remain in force beyond any expiry of their review date until a new version is available.

Contents:

Version control	2
Contents:	3
1. Introduction and Purpose	4
2. Scope	4
3. Definitions and Legal Context	4
4. Responsibilities	5
5. Anti-Money Laundering Procedures	6
6. Implementation and Training	7
7. Enforcement of this Policy and Sanctions	7
8. Monitoring and Review	7
9. Appendices	8
10. Appendix A: AML Reporting Form	9
11. Appendix B: MLRO Report	10
12. Appendix C: Examples of Suspected Money Laundering	11

1. Introduction and Purpose

- 1.1 itSMF UK is committed to upholding the highest level of ethical conduct whilst undertaking business activity that falls within scope of the legislative obligations associated with antimoney laundering (AML). At the itSMF UK, our values are embodied in everything we do and trust, underpinned by integrity in our work, is a particular focal point of this policy.
- 1.2 Like all businesses, itSMF UK must regularly review and update processes and procedures to protect itself and its stakeholders against money laundering attempts and in recent years legislation has broadened the definition of money laundering and its associated activity. This policy has been implemented to meet legislative requirements, assist with mitigating money laundering risk and update procedures to address suspected cases.
- 1.3 Part 7 of the 2002 Proceeds of Crime Act defines the full scope of money laundering activity and includes:
 - Concealment or disguising of criminal property.
 - Converting, transferring, or removing criminal property from the UK.
 - Acquiring, using or having possession of criminal property.
 - Failure to disclose activity that is suspected, or knowingly committing an offence relating to acquisition, retention, use, control or disguising of criminal property.

2. Scope

- 2.1 The policy applies to all staff undertaking business on behalf of itSMF UK. The policy outlines responsibilities and procedures to follow in the event of suspected money laundering activity.

3. Definitions and Legal Context

- 3.1 The legislation that sets out the requirements on Anti-Money Laundering, with which the itSMF UK must comply is:
 - The Proceeds of Crime Act 2002 – Primary regulations in the UK which define activity and offences.
 - Money Laundering and Terrorist Financing (Amendment) Regulations 2019 – Enhancing on the 2017 regulations, the 2019 regulations apply primarily to financial services companies but provide the key principles around transaction monitoring and customer due diligence that the itSMF UK apply.
 - The Terrorism Act 2000 (as amended by The Anti-Terrorism Crime and Security Act 2001 and the Terrorism Act 2006).
 - Criminal Finances Act 2017.
- 3.2 Money Laundering is the process of taking illegitimate proceeds from criminal activity and transforming them through various stages into what appear to be legitimate assets. Money Laundering has three stages:
 - **Placement:** Movement of criminal property/proceeds from their source i.e. cash paid into a bank account.

- **Layering:** Transactions involved in concealing the origin i.e. cash transferred to several other accounts overseas.
 - **Integration:** Movement of laundered proceeds into the economy i.e. a 'front' company issues what appears to be a legitimate invoice and invoice is paid with 'layered' cash.
- 3.3 Any individual found to be connected with money laundering activity, at any stage, in the UK, could face 2 to 14 years imprisonment and unlimited fines.
- 3.4 It is important that all staff be aware of 'Relevant Circumstances', which are situations where the AML regulations would typically apply, relevant to itSMF UK's business activity.
- 3.5 There is no monetary limit on suspicious business activities that might give rise to money laundering concerns, which should be reviewed and risk assessed.
- 3.6 In terms of itSMF UK business activity, all of the following examples would be considered relevant circumstances:
- Members paying large amounts of membership and/or event fees.
 - Sponsor/third party (not known to the itSMF UK or knowingly connected to the member) paying the membership/event fees on behalf of the member organisation.
 - Overpayment of funds for no apparent reason, including subsequent requests for refunds of overpaid amounts, as well as payments received from unknown customers who then suggest an administrative error and require funds to be refunded.
- 3.7 Further examples of suspected Money Laundering can be found under Appendix C of this policy.

4. Responsibilities

- 4.1 To comply with the AML regulations and to ensure the itSMF UK has appropriate internal controls to mitigate the risk associated with money laundering activity, itSMF UK must satisfy the following key requirements:
- Obtain, and retain for the duration of the relationship plus five years, evidence of the identity of our customers and details of the business relationship (KYC).
 - Appoint a Money Laundering Reporting Officer (MLRO) for whom will assess disclosures before potentially reporting to authorities such as the National Crime Agency (NCA).
 - Ensure disclosure processes are in place allowing reporting of suspicious or suspected activity to the MLRO.
 - Ensure training is provided to assist all staff, particularly those with finance related roles, in understanding AML, including what processes are in place internally to facilitate disclosure and what they can do to help mitigate risk.

Employees

- 4.2 Money Laundering regulations apply to all staff, not just those in finance facing roles. Should any member of staff become aware that money laundering activity has or is taking place, or concerned about their own involvement in a situation, they must disclose this at the earliest opportunity to the MLRC. Failure to do so could result in the employee

committing an offence and becoming personally liable to prosecution. In addition, the employee could become subject to internal investigation under the itSMF UK Disciplinary Policy. Employees should use the 'AML Disclosure Report' (Appendix A) to notify the MLRO and guidance in doing so is provided under Section 5.6 of this Policy 'Disclosure Procedure'.

Money Laundering Reporting Officer (MLRO)

- 4.3 itSMF UK's Money Laundering Reporting Officer is the designated individual within the itSMF UK who will evaluate all disclosures and determine next steps.
- 4.4 itSMF UK's MLRO is the Data Protection Officer and can be contacted via email: data@itsmf.co.uk.
- 4.5 The MLRO's key responsibilities include:
- Oversight of itSMF UK's compliance with AML regulations.
 - Review of all disclosures including assessing the need to escalate to NCA.
 - Retention of all disclosures, actions taken and annual reporting to audit committee.

5. Anti-Money Laundering Procedures

Know your Customer

- 5.1 Know Your Customer (KYC) is the principle of establishing the true identity of the person/business that itSMF UK is entering into a transactional relationship with. Evidence in relation to businesses and third parties should include official Purchase Orders, letter headed documents, companies house checks and formal confirmation of bank details via publicly published contact information.
- 5.2 itSMF UK prohibits engaging in business activity with any individual or entity listed on the HMRC UK Sanctions List or the HMRC UK Financial Sanction Target List. All staff within scope of this policy must consult the MLRO where these sanctions list become of concern to any forthcoming business engagement.

Due Diligence

- 5.3 During procurement, itSMF UK will always undertake due diligence where the value of a business-to-business engagement is valued at over £25,000. This would include a credit check and minimum insurances.

Cash Handling

- 5.4 itSMF UK does not accept cash payments for any of its services.

Processing of Refunds

- 5.5 Any approved refund, for whatever reason, will only be returned to the original payer via the same payment route it was received to the same account that it was paid from. This includes all credit/debit card payments both domestic and international plus all direct bank transfers received into the itSMF UK account.

Sanctioned Countries

- 5.6 See section 5.2. Should you require advice before entering into proposed activity involving a sanctioned country, please consult the MLRO.

Disclosure Procedure

- 5.7 Any staff member who has suspicions of potential money laundering activity must complete the Suspected Anti-Money Laundering Reporting Form (Appendix A) at the earliest opportunity. Submit the reporting form to the MLRO listed in section 4.4 of this policy. The report can be submitted confidentially (password protected) by email, or by post, but any post must be enclosed in an envelope marked “Confidential – to be opened by addressee only” and placed within another envelope that bears no confidential marking. You can enclose any evidence you think may assist the MLRO in their investigations. It may be necessary to request further information from other individuals and their details should be noted in the ‘Other information’ section of the AML reporting form for the MLRO to take forward. Do not make any further enquiries yourself as to avoid inadvertently alerting anyone who may be involved, unless specifically asked to do so by the MLRO.
- 5.8 Where there are suspicions around the MLRO’s involvement in potential money laundering activity, the report should be directed to the itSMF UK Chair, whose contact details can be obtained via email: membership@itsmf.co.uk.

6. Implementation and Training

- 6.1 The Policy is available on the itSMF UK website (Board & Governance page) and internally on the itSMF UK SharePoint site.
- 6.2 All staff members should familiarise themselves with this policy and the procedures, which have been implemented to support itSMF UK’s compliance with AML regulations.

7. Enforcement of this Policy and Sanctions

- 7.1 The approval of the Policy will be communicated through operations team meetings.
- 7.2 The General Manager will work with the MLRO to identify appropriate provision of training, guidance and support to staff on the implementation of this Policy.
- 7.3 It is imperative that staff follow the guidance within this Policy as failure to do so may result in disciplinary action and/or personal liability via legal proceedings.

8. Monitoring and Review

- 8.1 The impact of this Policy shall be reviewed by the Money Laundering Reporting Officer (MLRO).

9. Appendices

Appendix A - AML Reporting Form

Appendix B - MLRO Report

Appendix C – Examples of Suspected Money Laundering

10. Appendix A: AML Reporting Form

Suspected Anti-Money Laundering – Reporting Form			
Name		Position	
Tel		Email	
Details of suspected offence & offender(s)			
Name(s), address(es) & relationship with itSMF UK			
Value & timing of activity involved			
Nature of suspicions			
What investigation /enquiries have been undertaken to date & if anything, what has been established?			
Have you discussed your suspicions with anyone?			
If so, who, when and on what basis?			
Is any aspect of the transaction(s) outstanding and requiring consent to progress? (details)			
Other information (additional evidence, enclosures or commentary that may assist the MLRO)			
Signed		Dated	

11. Appendix B: MLRO Report

Money Laundering Report by MLRO (Retain for 5 years)			
Date Received			
Consideration of disclosure			
Key points identified			
Reasonable grounds of suspected money laundering?			
Will Suspicious Activity Report be submitted to NCA? If yes, date submitted. If no, reason(s) for non-disclosure			
Do we require NCA consent to proceed with a potentially illegal transaction(s) if yes, date consent received and date consent given to staff member (s) involved			
Signed		Dated	

12. Appendix C: Examples of Suspected Money Laundering

This list should not be considered exhaustive as money laundering can present itself under many different guises. The following are examples which could suggest money laundering activity or raise reasonability suspicion about the integrity of the activity.

- A member, sponsor or third party not known to itSMF UK attempt to engage in a transaction.
- Unreasonable secrecy when requesting information.
- Unexplained involvement, or insistence of the involvement, of an apparent unconnected third party without reasonable explanation.
- Overpayments without reason.
- Noticeable change in usual business activity, i.e. size/frequency of payments.
- The insistence for refunds to be credited to alternative bank accounts.
- Knowledge of alleged improper business conduct by a third party.
- Payment of an invoice to a bank account not connected to the business name.
- Refusal to put business terms in writing.
- The offer of a gift in exchange for facilitation.