The Commonwealth

ANTI MONEY LAUNDERING
and
FUNDING of CRIMINAL ACTIVITIES
POLICY

Version: 4.0

Effective Date: November 2025

1. Purpose

1.1. The Commonwealth Secretariat ('Secretariat'), as an international organisation, is not formally subject to national or international regulatory supervision or to anti-money laundering and counter financing of terrorism legislation. However, the Secretariat respects local law and is committed to combating money laundering and countering the financing of criminal (including terrorist) activities. Additionally, related legislation may apply to staff residing in the UK and other countries. It is therefore important that all Secretariat employees are aware of the potential for money laundering and the safeguards required to avoid the Secretariat unwittingly becoming exposed to, or facilitating, money laundering.

2. Scope

2.1. This Policy applies to the Secretariat's conduct both in the United Kingdom (UK) and abroad and to all employees of the Secretariat, including temporary agency staff, interns, consultants and any seconded staff (together "Staff").

2.2. It relates to both incoming funds and funds utilised and disbursed by the Secretariat.

2.3. All Staff and Counterparties are required to comply with this Policy and any anti-bribery legislation to applies in any jurisdiction in which they conduct activities.

3. Definitions

3.1. In this Policy, the following terms have the meaning set out below:

i. Money laundering: The process of legitimising funds obtained through illegal means by conducting a series of complex sequence of financial or commercial transactions designed to disguise their illicit origin.

ii. Funding of criminal activities: Providing financial support to criminal enterprises or terrorist activities (including those listed in UN sanctions list).

iii. Counterparty: Any third-party that contributes to, executes, implements, bids for, or in any way participates in Secretariat related activities, including procuring, giving or receiving of funds, services or supplies, or other form of support to or from the Secretariat.

iv. Due diligence: A process to identify, verify and validate the identity of the Counterparty. This enables the Secretariat to assess and evaluate the extent of risk related to money laundering and financing of terrorism regarding the relationship with the prospective Counterparty.

4. Core Principles

4.1. The Secretariat must make all reasonable efforts to ensure its funding comes from legitimate sources and that funds are not used to support criminal or terrorist activities.

4.2. The Secretariat should not be used as a conduit for money to be passed between two organisations.

4.3. Money laundering and the financing of criminal activities is prohibited and present substantial risks, including regulatory actions and reputational harm.

5. Procedures and Processes

5.1. All Staff should consider the likelihood of funding that is received, disbursed or otherwise utilised by the Secretariat being linked to criminal or terrorist activities. If staff have concerns, they should seek further advice from Legal Counsel, Director HRFM or Director of Corporate Compliance before taking any further steps.

5.2. All transactions with Counterparties should be made through regulated financial institutions, such as banks or building societies. Any exceptions must be approved by the Deputy Secretary-General Corporate.

Due Diligence

5.3. Staff should apply a risk-based due diligence approach to Counterparties and make proportionate checks, including with consideration to the red flags listed at Annex 1. This may include checking company website details including address and telephone numbers and ensure these are the same as stated on any documentation received. Other checks may include obtaining an Equifax report where applicable as well as an independent due diligence report, looking at industry sources, including banks, law firms and accounting firms, which have offices worldwide.

5.4. A check against the UN Sanctions list must always be conducted on Counterparties.

5.5. Staff should make reasonable efforts to ensure any Counterparty to which funding has been provided, and who sub-contracts work to a third party, conducts the appropriate downstream partner due diligence.

Record Keeping

5.6. Record-keeping is an essential component of the audit trail so all records created or obtained in relation to due diligence process and documentation regarding contractual or other arrangements with Counterparties shall be kept in accordance with the Secretariat's policies.

Reporting and Monitoring

5.7. All Staff must report to the Director Human Resources, Director of Corporate Compliance or Legal Counsel any activity which gives rise to suspicions of money-laundering or the financing of criminal or terrorist activity. Reporting can also be made via the Whistleblowing Policy which provides for anonymous reporting.

5.8. Money laundering and the funding of criminal or terrorist activities are extremely serious offences and all cases suspected or encountered by the Secretariat will be forwarded to the Police for further investigation. Staff are required to fully cooperate with investigations.

Training and Awareness

5.9. All Staff must complete the Whistleblowing Mandatory training course within six months of joining the Secretariat and complete a refresher course every two years. This training includes fraud and the code of conduct.

Risk Assessments

5.10. The annual risk assessment seeks to identify, evaluate and manage all the potential risks, which may exist within the Secretariat in relation to money-laundering and the funding of criminal or terrorist activities.

5.11. This process ensures that fit for purpose controls are in place and that action plans are in place to deliver an effective and proportionate response when there are suspicions of money laundering or the funding of criminal or terrorist activities.

6. Non-Compliance with this Policy

6.1 Non-compliance with any of the provisions of this Policy may constitute a disciplinary offence and may be dealt with in accordance with the disciplinary procedure set out in the Staff Handbook.

6.2. As far as Counterparties are concerned, a breach of this Policy could lead to the suspension or termination of any relevant contract, sub-contract or other agreement as applicable.

7. Supporting Documents

7.1. This Policy should be read in conjunction with the Secretariat's policies, including:

- Prevention and Investigation of Fraud and Corruption Policy
- Anti-Bribery Policy
- Whistleblowing Policy
- Gifts & Hospitality Policy
- Staff Handbook
- Code of Conduct and Ethics
- Downstream Partner Due Diligence Guidance

8. Roles and Responsibilities

8.1. Responsibility for maintaining this Policy is with the Director of Corporate Compliance.

9. Policy Review

9.1. This Policy will be reviewed at least every three years or earlier if required.

9.2. This Policy and any changes to it are approved by the Corporate Affairs Committee.

10. Implementation / Communication

10.1. This Policy will be implemented via an announcement on Compass.

11. Version Control

Version	Date	Description of changes	Reason	Approved By
1.0	Oct 2012	Initial release		Director, CSD
2.0	Jun 2015	Updated changes to names of job titles in line with current structure Inclusion of Code of		Director, CSD
		Conduct and Ethics as a supporting policy Formatting changes in line with standard policies and procedures.		
3.0	Apr 2021	Policy review.		

3.1	Jan 2023	Formatting changes in line with Policy Template.		
4.0	Nov 2025	Convert from guidelines to policy. Change of policy owner, inclusion of sub headings under procedures (reporting, due diligence, risk assessments, training), change in reporting lines, inclusion of red flags.	Periodic review	CAC

Red Flags for Money Laundering

Red flags do not confirm the existence of money laundering or financing of terrorism activity; they signal a need for further review, checks and verification. The red flags for money laundering and financing of terrorism vary depending on the type of scheme. Some red flags include:

1. The source of funds from a donor is suspicious - such as funds received from a high-risk entity (dubious reputation, unverified identity) or country with weak financial infrastructure, or donor with links to those that engage in or support money laundering activities or financing of terrorism, or large contributions in cash, not through the financial system.
2. Counterparty provides false or inconsistent information during the due diligence verification – this may include fake documents, email accounts that cannot be found on the internet.
3. Counterparty is reluctant to provide needed information or data for due diligence verification. This could include refusal to provide details of principals or key management or those with majority interest in the entity.
4. Counterparty is overly secretive of the entity's business or evasive regarding their clienteles, beneficial owners among others.
5. Counterparty is using an agent or intermediary without adequate or logical justification or uses email address with unusual domain part.
6. Counterparty requests for partnership or services or transactions not compatible with those declared or not typical for that type of entity.
7. Counterparty requests to be paid in cash instead of bank-to-bank transfer.
8. Frequent changes of vendor's bank accounts by Counterparty without adequate justification.
9. Multiple bank accounts belonging to the same supplier or implementing partner without good reasons.
10. Request to pay a supplier or implementing partner through a third party.
11. Structuring transactions to avoid government reporting, tax compliance or record keeping requirements.
12. Refunds from implementing partner using unusually complex structures that bear no connection with the implementing partners registration.
13. Refunds of programme funds in cash – programme refunds should be done through the bank.
14. Wire transfer activity that is not consistent with the business activities of a vendor, or which originates or terminates with parties unrelated to the transaction.
15. An unauthorised person acting as representative or signatory of a Counterparty, or a person claiming to be a representative but not ever listed or introduced as a formal party to the transaction or relationship.