

 West Mercia POLICE  John Campion Police and Crime Commissioner West Mercia		POLICY
Security Classification	OFFICIAL	
Disclosable under Freedom of Information Act 2000	Yes	

POLICY TITLE	Anti-Money Laundering
POLICY REFERENCE NUMBER	WMP182
Version	1.0

POLICY OWNERSHIP	
DIRECTORATE	OPCC
BUSINESS AREA	POLICY

INITIAL IMPLEMENTATION DATE	December 2021
NEXT REVIEW DATE:	December 2024
RISK RATING	LOW
EQUALITY ANALYSIS	LOW

1.0 POLICY OUTLINE

- 1.1 The Proceeds of Crime Act 2002, the Terrorism Act 2000 and the Money Laundering Regulations 2007 place obligations on the Police and Crime Commissioner and the Chief Constables and their employees (staff and officers) to establish internal procedures to prevent the use of their services for money laundering.
- 1.2 This policy applies to all employees of the organisations, and aims to maintain the high standards of conduct which currently exist within the organisations for preventing criminal activity through money laundering. This policy sets out the procedures for the reporting of suspected money laundering activities which will assist the organisations to comply with their legal obligations.
- 1.3 The policy should be read along side the [Anti-Fraud and Corruption Strategy](#), the [OPCC Whistle-blowers policy](#) and the [WMP Whistleblowing Policy](#)
- 1.4 Failure by an employee to comply with the procedures set out in this policy may lead to disciplinary action being taken against them. Any disciplinary action will be dealt with through the organisations disciplinary policy.

2.0 IMPLICATIONS of the POLICY

- 2.1 Money laundering is a term used which relates to offences involving the proceeds of crime or terrorism funds. The following are defined as primary acts of money laundering:
- **Concealing**, disguising, converting, transferring criminal property or removing from the UK (section 327 of the Proceeds of Crime Act (POCA) 2002).
 - To enter into or become concerned in **arranging** a transaction which you know or suspect will assist the acquisition, retention, use or control of criminal property or on behalf of another person (POCA section 328).
 - **Acquiring, using or possessing** criminal property (POCA section 329).
- 2.2 There are also two secondary offences
- the failure to disclose any of the three primary acts
 - Tipping off. Tipping off is where someone informs a person or persons involved in, or suspected to be involved in money laundering acts, in such a way as to reduce the likelihood of their being investigated.
- 2.3 Potentially any employee could be caught by the money laundering provisions if they suspect money laundering and either become involved in it or fail to do something about it. None of these offences are committed if:
- the persons involved did not know or suspect that they were dealing with the proceeds of crime

Or

- a report of the suspicious activity is made promptly to the Money Laundering Reporting Officer (MLRO).
- 2.4 While the risk to the organisation of breaching legislation is considered to be low, it is important that all employees are aware of their responsibility to report any suspicions of money laundering activity. All employees are responsible to act promptly and report any suspicions to the MLRO.
- 2.5 In support of this policy the organisation will make all employees aware of the requirements and obligations placed on the authority and on themselves as individuals by anti-money laundering legislation and give targeted training where deemed necessary.

3.0 WHAT IS MONEY LAUNDERING?

- 3.1 Money laundering is where money obtained, as a result of a crime, is used to pay for services or goods. Although the term 'money laundering' is usually associated with organised criminal activities, it can include a suspicion that someone you know, or know of, is benefiting financially from dishonest activities, e.g. non-payment of income tax.
- 3.2 People involved in handling criminal property look for ways to secure and safeguard the proceeds of their criminal activities. Although other ways exist, cash is the mainstay of criminal transactions, being the most reliable and flexible, and having little or no audit trail.
- 3.3 In the UK, the most popular method of money laundering is thought to be the purchase of property, followed by investment in front companies, or high cash turnover businesses (often legitimate businesses), or by funding a lifestyle. After property, the most significant assets bought by criminals are jewellery, artwork, antiques, cars and boats.
- 3.4 Criminals invest cash in financial products with a view to selling them quickly (if necessary at a loss). Criminals also use trusts to launder money because of their secretive nature and flexibility, often using front companies to hide identities. Gambling large amounts at relatively low odds is also used, since winnings are usually received in the form of cheque payments.
- 3.5 Criminals use 'layering' to confuse the audit trail. This involves passing transactions through several stages, often eventually banking the proceeds of business income and transferring the money overseas to a country whose regulatory regime is weaker.

Examples of money laundering can include:

- large cash payments;
- asking for cash refunds on credit card payments; or
- overpaying invoices and fees, and then asking for refunds

4.0 THE PENALTIES for MONEY LAUNDERING

- 4.1 Money laundering offences may be tried at a magistrate's court or in the Crown Court, depending on the severity of the suspected offence. Trials at a magistrate's court can attract fines of up to £5,000, up to 6 months in prison, or both.
- 4.2 In a Crown Court, fines are unlimited and with possible prison sentences of between two to 14 years.

5.0 MONEY LAUNDERING POLICY

- 5.1 Cash Transactions - Where possible West Mercia Police will implement digital payment methods. These payments should be promoted and the acceptance of cash transactions should be discouraged where possible.
- Employees must report any cash transactions over £5,000 to the Chief Financial Officer (or nominated deputy) for consideration of legitimacy of the transaction.
 - To help prevent money laundering, a cash payment limit of £7,500 has been set. No cash payments above this level will be accepted.

This is not designed to prevent customers making payments for fees and services, but to minimise the risk of money laundering to protect both employees and the organisation.

- 5.2 Digital Transactions - Where a transaction has been made via a card payment and a refund is requested then the refund can only be made to the original Payment Card that was used. Refunds cannot be made to any other bank accounts than the original payment method, or as a separate cheque payment.
- 5.3 Purchase of Assets - If the matter involves a proposed transaction (eg the sale of property) you should not proceed with the transaction without following the procurement rules regarding authorisation of sale of asset. The transaction for the sale of the asset should comply with the policy in 3.1 & 3.2 above.
- 5.4 Designated in Financial Regulations (7.6.25), the Treasurer to the Police and Crime Commissioner is designated as the Money Laundering Reporting Officer for West Mercia. In the absence of the Treasurer, the Finance Manager to the Police and Crime Commissioner is authorised to deputise.
- 5.5 Undertaking Regulated business – These are categorised as accountancy, audit and tax services and legal services regarding financial, company or property transactions. Where any of these services are being provided and as part of this:
- Forms an ongoing business with a client
 - Undertakes a one-off or occasional transaction amounting to 15,000 euros or more whether carried out as a single transaction or several linked ones.
 - Suspects money laundering or terrorist activity

Then the Customer Due Diligence (CDD) procedure must be followed before any business is undertaken with that client. Due to the nature and stringent guidelines

for regulated business, employees will be aware if their duties involve regulated activities.

6.0 RESPONSIBILITIES OF EMPLOYEES

6.1 Any employee who suspects money laundering activity is taking place or that their involvement in a matter may be prohibited under the legislation should take the following actions.

- Do not tell the customer about your suspicions.
- Report your suspicions immediately to West Mercia's MLRO
- Keep all records relating to the transaction(s). If you are unsure about what records or information to keep, please ask the MLRO.

6.2 The employee must follow any subsequent directions from the MLRO or deputy and must not make any further enquiries themselves into the matter. Additionally, they must not take any further steps in the transaction without authorisation from the MLRO or deputy.

6.3 The employee should not disclosure or otherwise indicate their suspicions to the person(s) suspected of money laundering. They must not discuss with others or note on a file that suspicions have been raised with the MLRO in case this makes the person(s) aware.

7.0 RESPONSIBILITIES OF THE MRLO

7.1 The MLRO or deputy must promptly evaluate any Disclosure Report to determine whether it should be reported to the National Crime Agency (NCA).

7.2 The MLRO or deputy must, if they so determine, promptly report the matter to the NCA on their standard report form and in the prescribed manner. The latest forms can be found at www.nationalcrimeagency.gov.uk.

7.3 All disclosure reports referred to the MLRO or deputy and reports made to NCA must be retained by the MLRO in a confidential file for a minimum of 5 years.

7.4 If the MLRO or deputy fail to disclose as soon as practicable that they know or suspect, or have reasonable grounds to do so, through a disclosure being made to them, that another person is engaged in money laundering they will have been considered to have committed a criminal offence without reasonable grounds.

8.0 CONSULTATION

<i>Business Lead Consulted</i>	<i>Date Consulted</i>
Andy Champness	November 2021

Consultation has taken place with the Force Chief Financial Officer, Critical Friends group and approved at the October 2021 WMGB.

9.0 DOCUMENT HISTORY

The history and rationale for change to policy will be recorded using the below chart:

Date	Author / Reviewer	Amendment(s) & Rationale	Date of Approval / Adoption
Oct 2021	Paul Benfield	To review and update the policy unique to WMP/OPCC	Published in advance of JNCC final approval in Feb 2022

10.0 ASSESSMENT AND ANALYSIS

The Equality Analysis (EA), Health & Safety Assessment (HAS) and Risk Assessment (RA) associated with this document are available on request.

11.0 DATA PROTECTION IMPACT ASSESSMENT

- Is a DPIA required? – No, Agreed with Audit, Risk and Compliance on 8th Nov 2021

12.0 MONITORING / EVALUATION

The monitoring and review of this policy is the responsibility of the policy owner.