



Anti Money Laundering Policy

KN-POL-038-02

Version #	Issue Date	Initials
01	02/12/2021	MM
02	21/10/2022	ES

Anti Money Laundering Policy

1. Purpose

The Anti-Money Laundering Policy is used to prevent criminals attempting to hide and change the identity of the proceeds of their crime, so they appear legitimate. There are various stages as outlined below:

- placement – “dirty money” is placed directly into the financial system
- layering – the proceeds are moved through a series of financial transactions, making it harder to establish their origin
- Integration – the money launderer creates a legitimate explanation for the source of the funds allowing them to be retained, invested into the legitimate economy or to acquire assets.

2.Scope

This policy applies to all KubeNet employees, contractors, and affiliates.

3.Version Control & Access Control Team

The below members of the KubeNet Team have been assigned to the Access Control Team.

Version	Date
2	21/02/2022

Members	Role
Julie Inglis	Operations and Finance
Elaine Syme	Digital Transformation
David Gray	IT Infrastructure

4. Policy Elements

Money Laundering Reporting Officer – David McDermott

The following constitute the act of money laundering:

- Concealing, disguising, converting, transferring criminal property, or removing it from the UK (section 327 of the 2002 Act); or
- Entering or becoming concerned in an arrangement which you know, or suspect facilitates the acquisition, retention, use or control of criminal property by or on behalf of another person (section 328); or
- Acquiring, using or possessing criminal property (section 329);
- Becoming concerned in an arrangement facilitating concealment, removal from the jurisdiction, transfer to nominees or any other retention or control of terrorist property (section 18 of the Terrorist Act 2000).

No payment to KubeNet should automatically be accepted in cash (including notes, coins, or travellers' cheques in any currency) if it exceeds £1,000. This does not, however, mean that cash transactions below these 4 values will be valid and legal and should not raise suspicion. Professional scepticism should be retained.

Staff who collect cash payments are asked to provide the details of any cash transaction over £1,000 to the MLRO so that precautionary checks can be performed.

If a member of staff has reasonable grounds to suspect money laundering activities or proceeds of crime, or is simply suspicious, the matter should still be reported to the MLRO. If the money offered is £1,000 or more in cash, then payment must not be accepted until guidance has been received from the MLRO even if this means the person must be asked to wait.

Any employee who becomes concerned that their involvement in a matter may amount to a prohibited act under the legislation, must disclose this promptly to the MLRO or deputy. The disclosure should be at the earliest opportunity of the information coming to your attention, not weeks or months later. Should you not do so, then you may be liable to prosecution

5. Policy Compliance

If any user is found to have breached this policy, they may be subject to KubeNet disciplinary procedure. If a criminal offence is considered to have been committed further action may be taken to assist in the prosecution of the offender(s).

If you do not understand the implications of this policy or how it may apply to you, seek advice from your line manager.

