

ANTI MONEY LAUNDERING POLICY & PROCEDURE

(CGN) Capital Growth Network will take measures to prevent the company and its officers being exposed to money laundering, to identify areas in which money laundering may occur and to comply with legal and regulatory requirements, especially the process for reporting actual or suspected money laundering cases to the Company's (Monitoring Officer or Chief Executive). It is the responsibility of every officer to be vigilant and act promptly in all suspected cases

1. THE POLICY

1.1 The Proceeds of Crime Act 2002, the Terrorism Act 2000 and the Money Laundering Regulations 2007 place obligations on the company and its employees with respect to suspected money laundering, the key points being:

- The reporting and detection of suspected money laundering.
- Officers must be vigilant for the signs of money laundering.
- Any employee who suspects money laundering activity must report this promptly to the (CGN)'s Money Laundering Reporting Officer (see reporting form for completion by the officer suspicious of activity).
- No payment to the company will be accepted in cash if it exceeds £5,000 and all cash serial numbers will be logged.
- Where the company is carrying out certain regulated activities during day to day business then the customer due diligence procedure must be followed, e.g. some Treasury Management activities are regulated by the Financial Conduct Authority.
- The Money Laundering Regulations are complex and detailed and should there be any doubt about the policy requirements, please request further information from line management.

2. THE POLICY

- 2.1 The policy applies to all officers and members, and sets out procedures for the reporting of suspected money laundering activities with the aim to reduce potential criminal activity. The policy defines procedures that will assist the company to comply with its legal obligations.
- 2.2 The Policy should be read alongside (CGN)'s Anti-Fraud and Corruption Policy.
- 2.3 Failure of an officer to comply with the procedures defined within this policy may lead to disciplinary action in line with (CGN)'s Disciplinary Policy Procedures.
- 2.4 Failure of a member to comply with the procedures defined within this policy would be reported to the leader for further action, e.g. a possible report to the Chief Executive Officer.

3. WHAT IS MONEY LAUNDERING?

3.1 Money laundering is a term used which relates to offences involving the proceeds of crime or terrorism funds. The following acts are defined as 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 an arrangement 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.

These are primary money laundering acts, two secondary offences are also defined which relate to the failure to disclose any of the three primary acts and tipping off (POCA section 330). 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.

3.2 While the risk to the company of breaching legislation is considered to be low, officers in all areas should be aware that they could be potentially exposed to money laundering acts. It is important that all employees' are aware of their responsibility to report any suspicions of money laundering activity as detailed within this policy (see reporting). All officers are responsible to act promptly and report any suspicions to the Money Laundering Reporting Officer to prevent any breach of legislation which can lead to serious criminal penalties.

4. AML REPORTING OFFICER / MONITORING OFFICER

4.1 The officer nominated to receive disclosures about money laundering activity is the Monitoring Officer. The Money Laundering Reporting Officer will deal with all disclosures confidentially and make decisions on reporting the activity to the Serious and Organised Crime Agency (SOCA) in the appropriate manner, all reports will be retained for five years. Contact details:

Name: Mykael Spekta
mykaelspekta@cgnequity.com
Phone: 020 8127 5021

5. REPORTING

5.1 Any employee who suspects money laundering activity should report their suspicions promptly to the Money Laundering Reporting Officer using the form attached (see reporting form for completion by the Money Laundering Reporting Officer, referenced AML Form 1), upon receipt of the report the Money Laundering Reporting Officer may contact you directly to discuss the content of the report as required.

5.2 No further enquiries should be made about the suspected money laundering after reporting to the Money Laundering Reporting Officer for action. No further steps in any transaction relating to the suspected money laundering should be made without authorisation from the Money Laundering Reporting Officer.

E.g. if repeated reported cash overpayments are received to a specific account seek guidance from the Money Laundering Reporting Officer before the amounts are refunded as a (CGN) cheque.

5.3 No disclosure should be made to others that would indicate suspicions of money laundering. Any officer reporting should not discuss the matter with others or note on file that a report has been made to the Money Laundering Reporting Officer as this may result in the suspect becoming aware of the situation.

5.4 The Money Laundering Reporting Officer will promptly evaluate any Disclosure Report to determine whether it should be reported to SOCA.

5.5 The Money Laundering Reporting Officer will, if necessary, promptly report the matter to SOCA on the standard electronic report form in the prescribed manner via www.soca.gov.uk.

5.6 Failure to report a disclosure to SOCA is considered a criminal offence without reasonable grounds. All disclosures will be retained on file for five years.

6. CUSTOMER DUE DILIGENCE

6.1 Extra care needs to be taken when (CGN) is carrying out regulated activities, this is known as customer due diligence, for example treasury management activities, charging for a service as a business or a customer other than a UK public authority. Due to the nature and stringent guidelines for regulated business, you will be aware if your duties involve regulated activities.

6.2 If customer due diligence (CDD) applies, you must seek evidence of identity, for example:

- Check the business's website to confirm their business address.
- **Conduct an on-line search via companies house to confirm the nature of business and identity of any directors.**
- Seek evidence from the key contact of their personal identity following the guidelines for identifying customers (see the council's cashiering procedure notes section seven for guidance).

6.3 Identification must be retained for five years after the end of the business relationship.

7. GUIDANCE & TRAINING

7.1 (CGN) will make all officers aware of the requirements and obligations placed on the company and on themselves as individuals by anti-money laundering legislation and give targeted training to those most likely to encounter money laundering. See Appendix A at the end of this document.

8. FURTHER INFORMATION

Further information can be obtained from the following sources:

- "Proceeds of Crime (Anti-Money Laundering) – Practical Guidance for Public Service Organisations" – CIPFA
- www.soca.gov.uk

APPENDIX A

All officers should be vigilant to suspicious activity, in particular when handling cash and other monetary transactions and when procuring works.

The Chartered Institute of Public Finance and Accountancy (CIPFA) have issued the following examples for situations which may give rise to money laundering or the suspicion of it:

- Those involved in the handling of 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.
- Criminals often transport cash out of the UK using couriers, usually through airports, to pay into banks overseas, to purchase property abroad, or to pay to their families.
- In the UK, the most popular method of laundering money is thought to be the purchase of property, followed by investment in front companies (these are companies used as a front or 'decoy' for illegal activities) or high cash turnover businesses (frequently legitimate businesses), or funding a lifestyle.
- After property, the most significant assets bought by criminals are jewellery, artwork, antiques, cars and boats.
- The investment of cash in financial products with a view to selling them quickly (if necessary at a loss) is used.
- Criminals use trusts to launder money because of their secretive nature and flexibility, often using front companies to hide identities.
- Gambling large amounts of cash at relatively low odds is used, since winnings are usually received in the form of cheque payments
- Criminals use 'layering' to confuse the audit trail – this involves passing transactions through several stages, often eventually banking the proceeds as business income, and transferring the money

Any transaction involving an unusually large amount of cash should cause questions to be asked about the source. This will particularly be the case where cash paid exceeds the amount necessary to settle a transaction, and the person(s) concerned request a non-cash refund of the excess. This will include double payments.

The reason for the use of trusts or offshore funds for handling the proceeds or settlement of a transaction should be questioned.

Care should be exercised and further enquiries may be needed where:

- a third party intermediary becomes involved in a transaction
- the identity of a party is difficult to establish or is undisclosed
- a company is used by a third party and the ultimate ownership is concealed or difficult to establish
- a party is evasive as to the source or destiny of funds.

It should be remembered that the money-laundering regime adopts an 'all-crimes' approach. Whilst the above examples are largely concerned with significant transactions which organisations may effect with third parties, the offences under the Proceeds Of Crime Act (notably sections 327-329) may apply to a very wide range of more everyday activities within an organisation. For example, being complicit in crimes involving the falsification of claims, benefiting from non-compliance with the conditions attaching to a grant, or facilitating employment on which tax is not paid.

HOW COULD MONEY LAUNDERING OCCUR WITHIN (CGN)?

Money laundering may occur during day to day business activities within the council; these are issues all officers should be aware of:

CREDIT UNION

- Completing regulated cash transactions, large cash deposit, identity of customer withdrawing cash, are you satisfied they are the account holder?
- Processing account applications and identifying new customers, accept only original documents and ensure identification is in line with credit union guidance.

ACCOUNT MANAGEMENT

- Are business relationships documented for loans and investments?
- Are customers identified and information retained for five years after the transaction?

REPUTATION

- Use local knowledge. Local knowledge is invaluable, this increased knowledge may increase suspicions, if in doubt, report it!
- Think about the impact on the company if lack of awareness is identified and inappropriate relationships are formed.

BUSINESS RATES (NNDR)

Consideration of the following examples of best practice:

- Are business directors identified as bona fide?
- Is the business legitimate and have we confirmed this?
- Is information retained?

LICENSING

- Have we identified the customer requesting a licence?
- Has the nature of the relationship been clearly defined and is the application viable and legitimate?

TRAINING

- Officers must be vigilant at all times.
- If in doubt, report it.
- The Money Laundering Policy should be adhered to and further guidance requested from the Money Laundering Reporting Officer where needed.
- Access further information via the sources in section eight of this document, for detailed guidance.

OFFICERS VISITING BUSINESSES AND PROPERTIES

- If suspicious activity is suspected during a property visit, officers should report the matter via the money laundering reporting procedure.

IDENTIFICATION

- Only original forms of valid identification and verification should be accepted in line with the cashiering procedure notes.
- Identification should be retained for reference for five years after the relationship has ended, reference to the transaction to which the identification relates should also be clearly documented.

PROCUREMENT

- Are tender documents clear and is it stipulated that employees performing contract works are legitimate?
- Are new suppliers/clients identified as bone fide?

DEBTORS

- Cash overpayments are repeatedly received to a debtor account without reasonable explanation, and refunds are given in the form of a (CGN) cheque, this may be a means to conceal the source of money obtained from illegal activities.