



## **Anti-Money Laundering Policy**

### **1. Introduction**

J C Accounting Ltd is a UK registered company providing Accountancy and Bookkeeping services. The business of the Company is low risk in relation to money laundering, however in order to prevent any of our services being used (or potentially used) for any money laundering activity, as well as any of our staff being exposed to money laundering, we wish to put in place the following anti-money laundering policy which supplements the anti-money laundering training given to all members of staff.

### **2. Scope of the Policy**

The broad definition of money laundering means that potentially anyone could commit a money laundering offence, this includes all employees of the Company, all temporary staff and contractors.

Our policy is to enable the Company to meet its legal and regulatory requirements in a way which is proportionate to the risk nature of the business, by taking reasonable steps to minimise the likelihood of money laundering occurring.

All employees must be familiar with their legal responsibilities.

### **3. What is Money Laundering?**

The principal primary legislation is The Proceeds of Crime Act 2002 (POCA), which consolidated, updated and reformed criminal law with regard to money laundering, supplemented by the Terrorism Act 2000 and the Fraud Act 2006. The principal secondary legislation is the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 as amended by the Money Laundering and Terrorist Financing (Amendment) Regulations 2019.

Money laundering can be defined as the process to move illegally acquired cash through financial systems so that it appears to be from a legitimate source. Money laundering offences include: concealing, disguising, converting, transferring criminal property or removing it from the UK (Section 327 POCA); entering into 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 POCA); and acquiring, using or possessing criminal property (Section 329 POCA).

There are also several secondary offences, failure to disclose knowledge or suspicion of money laundering to the Money Laundering Reporting Officer (MLRO); failure by the MLRO to disclose knowledge or suspicion of money laundering to the National Crime Agency; and 'tipping off' whereby somebody informs a person or persons who are, or who are suspected of being involved in money laundering, in such a way as to reduce the likelihood of their being investigated or prejudicing an investigation.

Any member of staff could potentially be caught by the money laundering provisions, if they suspect money laundering and either become involved with it in some way, and/or do nothing about it. This Policy sets out how any concerns should be raised.

#### **4. Money Laundering Reporting Officer (MLRO)**

The Company will appoint a MLRO to receive disclosures about money laundering activity and be responsible for anti-money laundering activity within the Company. The officer nominated to do this is Jayne Perry.

The MLRO will ensure that appropriate training and awareness is provided to new and existing employees and that this is reviewed and updated as required.

The MLRO will ensure that appropriate anti-money laundering systems and processes are incorporated by the Company.

#### **5. Suspicions of Money Laundering**

All employees must as soon as is practical report any knowledge of or suspicion of (or where there are reasonable grounds to suspect) suspicious activity to the MLRO in the prescribed form as set out in this policy document.

Once the matter has been reported to the MLRO, must follow the directions given to and must NOT make any further enquiry into the matter.

The employee must NOT voice any suspicions to the person(s) whom they suspect of money laundering, as this may result in the commission of the offence of "tipping off". They must NOT discuss the matter with others or note on the file that a report has been made to the MLRO in case this results in the suspect becoming aware of the situation.

#### **6. Consideration of the Disclosure by the MLRO**

Once the MLRO has received the report, it must be evaluated in a timely manner in order to determine whether:

- There is actual or suspected money laundering taking place; or

- There are reasonable grounds to know or suspect that this is the case; and
- Whether the MLRO needs to lodge a Suspicious Activity Report (SAR) with the National Crime Agency (the NCA).

Where the MLRO concludes that there are no reasonable grounds to suspect money laundering then consent will be given for any on-going or imminent transaction(s) to proceed.

Where consent is required from the NCA for a transaction to proceed, then the transaction(s) in question must not be undertaken or completed until the NCA has given specific consent, or there is deemed consent through the expiration of the relevant time limits without objection from the NCA.

All disclosure reports referred to the MLRO and reports made to the NCA will be retained by the MLRO in a confidential file kept for that purpose, for a minimum of 5 years.

The MLRO must also consider whether additional notifications and reports to other relevant enforcement agencies should be made.

## **7. Customer Identification and Due Diligence**

Due diligence is performed on all clients who must provide basic information including Full Name, Address, Date of Birth, National insurance Number, Proof of ID (Passport and Driving Licence) and proof of address (a utility bill). We perform checks using Veriphy, we may send you a link to do the checks via Veriphy mobile app.

### Enhanced Due Diligence

It may be necessary for the Company to carry out enhanced due diligence on certain customers where the customer or a transaction involving the customer appears to be “high risk”. This means that there is a higher level of identification and verification of the customer’s identity required. The following non-exhaustive list of situations may indicate a “high risk”:

- a new customer;
- a customer not well known to the Company;
- customers in known high risk industries and/or jurisdictions;
- transactions that are unusual or appear to be unusual for that customer;
- highly complex transaction or payment arrangements;
- the transaction involves a politically exposed person (“PEP”) or an immediate family member or a close associate of a PEP;
- no face to face meetings take place with the customer where this is usually expected.