



BOG ANTI MONEY LAUNDERING POLICY

1	Introduction
	<p>Balm of Gilead World Ministries is committed to the highest standards of probity in all its financial dealings. It will therefore ensure that it has in place proper, robust financial controls so that it can protect its funds and ensure continuing public trust and confidence in it. Some of those controls are intended to ensure that the Ministry complies in full of its obligations not to engage or otherwise be implicated in money laundering or terrorist financing. This policy sets out those obligations, the Ministry's response, and the procedures to be followed to ensure compliance. Throughout this policy Ministry will be used to refer to BOG Ministries.</p> <p>Money laundering is the process of taking profits from crime and corruption and transforming them into legitimate assets. It takes criminally derived 'dirty funds' and converts them into other assets so they can be reintroduced into legitimate commerce. This process conceals the true origin or ownership of the funds, and so 'cleans' them.</p> <p>As the Ministry receives significant amounts of funds from all over the world, through donations, offerings etc. It is exposed to both risk of being unwittingly used to launder funds.</p>
1.1	Purpose
	<p>This policy supports the Ministry in its aim to comply fully with all UK legislation and all relevant legislation in relation to Anti Money Laundering and to ensure it minimises the risk of money-laundering taking place in its operations.</p> <p>For the avoidance of doubt, the Ministry will not do business or operate with anyone whom it suspects of taking part in any activity, knowingly or unknowingly, which it regards as linked with potential money-laundering.</p>
1.2	Scope
	<p>This policy applies to all staff who are engaged in financial transactions for or on behalf of the Ministry. Any failure to adhere to this policy may be dealt with under the Ministry's disciplinary procedures, as appropriate. Note that any such failure will also expose the individual concerned to the risk of committing a criminal offence under relevant UK or overseas money laundering legislation.</p>
1.3	Legislative context
	<p>The law concerning money laundering is complex and is increasingly actively enforced. It can be broken down into three main types of offences:</p> <ul style="list-style-type: none"> i. the principal money laundering offences under the Proceeds of Crime Act 2002; ii. the prejudicing investigations offence under the Proceeds of Crime Act 2002; and iii. offences of failing to meet the standards required of certain regulated businesses, including offences of failing to disclose suspicions of money laundering and failing to comply with the administrative requirements of the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017. <p>The Ministry is required to comply with the Proceeds of Crime Act 2002. The Ministry is not authorised or regulated by the Financial Conduct Authority. It therefore does not have to comply with Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017, but it is considered best practice for it to do so.</p>

2	Policy
2.1	Principles
2.1.2	Requirements of the Ministry
	In the UK, severe penalties can be imposed on both the Ministry and its employees/members (as individuals) connected with any stage of laundering money.

	<p>The Ministry therefore has to consider the risks that its activities will expose it to potential money laundering and devise suitable controls that protect it and its employees against being the victim of money laundering. It must document these risks and monitor them on a regular basis. The Ministry also has to consider how it trains its staff to spot potential signs of money laundering activity, and how to report it according to UK law.</p> <p>The Ministry also needs to ensure it complies with all local money laundering regulations when it operates overseas.</p>
2.1.2	<p>Risk Areas</p> <p>There are three stages in money laundering: placement, layering and integration.</p> <ul style="list-style-type: none"> - Placement is where the proceeds of criminal activity enter into the financial system - Layering distances the money from its illegal source through layers of financial transactions - Integration involves the re-introduction of the illegal proceeds into legitimate commerce by providing an apparently genuine explanation for the funds. <p>There are many types of risk. Overseas payments often pose higher risk as they can often be made via a third party, can involve the movement of money through multiple bank accounts or involve high risk countries as outlined in 2.1.3. The Ministry has identified the following key areas which could be exploited by those trying to carry any or all of the three stages of money laundering, above.</p> <ul style="list-style-type: none"> - Receiving funds/donations from potentially criminal business entities - Making refunds to members, and third parties (donors and sponsors) - Receiving cash transactions (if applicable) - Receiving donations - Overseas operations
2.1.3	<p>Money Laundering Warning Signs</p> <p>It is not possible to give a definitive list of ways to spot money laundering. The following are types of risk factors which may, either alone or collectively, suggest the possibility of money laundering activity.</p> <ul style="list-style-type: none"> - A new partner, donor or sponsor not known to the Ministry - A donor or member from a country known to carry a high level of risk (such as a sanctioned country, or country with known high levels of financial fraud or corruption) - A secretive person or business e.g. that refuses to provide requested information without a reasonable explanation. - A request to pay a substantial sum in cash to the Ministry - Concerns about the honesty, integrity, identity or location of the people involved. - Involvement of an unconnected third party without a logical reason or explanation. - Overpayments for no apparent reason, and requests to pay the difference back to a third party - Absence of any clear legitimate source for the funds received. - Significant changes in the size, nature, frequency of transactions with a donors that are without reasonable explanation - Cancellation, reversal or requests for refunds of earlier transactions. - Requests for account details outside the normal course of business. - A history of poor business records, controls or inconsistent dealing - A receipt of funds from an unconnected third party (i.e. not a members, family member or sponsor) - Any other facts which tend to suggest that something unusual is happening and give reasonable suspicion about the motives of individuals.

2.2	Controls
2.2.1	Due Diligence
	<p>Due diligence is the process by which the Ministry assures itself of the provenance of funds it receives and that it can be confident that it knows the people and organisations with whom it works. In this way the Ministry is better able to identify and manage risk.</p> <p>Due diligence should be carried out before the funds are received. Funds must not be returned before due diligence has been carried out.</p> <p>In practical terms this means:</p> <ul style="list-style-type: none"> i) identifying and verifying the identity of a payer or a payee, typically a members or a donor; ii) where the payment is to come from or to be made by a third party on behalf of the members or donor, identifying and verifying the identity of that third party; iii) identifying and verifying the source of funds from which any payment to the Ministry will be made; and iv) identifying and in some circumstances verifying the source of wealth from which the funds are derived. <p>Source of funds refers to where the funds in question are received from. The most common example of a source of funds is a bank account. Source of wealth refers to how the person making the payment came to have the funds in question. An example of a source of wealth is savings from employment.</p>
2.2.2	Transactional Controls
	<p>The Ministry has a robust "know your customer" process for members and other donors.</p> <p>Members are requested to register their details with the church especially if they are going to participate in gift aid as well.</p> <ul style="list-style-type: none"> - Suspicious payment reports from the Ministry's card payment gateway provider (WPM) are monitored daily and investigated where necessary - No refunds can be made other than to the original payer - Suspicious payments purporting to be from members are returned to source if found to be fraudulent - Other than in exceptional circumstances, refunds are only made using the original mode of payment - Any potential breaches of this policy must be flagged up to the Ministry's Money Laundering accountant or designated person.
2.2.4	Training
	<p>Where possible on joining the Ministry any staff whose duties will include undertaking a finance function may receive appropriate anti-money laundering training. This could be as simple as directing them to the government website or as the church sees fit.</p> <p>All staff undertaking a finance function will receive regular refresher anti-money laundering and counter-terrorist finance training. Again this will be made from any publicly available training.</p> <p>The Ministry's anti-money laundering training will include the applicable law, the operation of this policy and the circumstances in which suspicions might arise.</p>

3	Reporting
2.3.1	Internal Reporting
	<p>It is best practice for the Ministry to appoint a nominated officer or Money Laundering Reporting Officer (MLRO) to be aware of any suspicious activity in the business that might be linked to money laundering or terrorist financing, and if necessary to report it through channels described below. The nominated officer at the Ministry of Balm of Gilead will be the change admin for now due the position they carry with the church/ministry.</p> <p>Where a member of staff knows or suspects that money laundering activity is taking, or has taken place, or becomes concerned that their involvement in a transaction may amount to a breach of the regulations, they must disclose this immediately to church administrator or the senior Pastor of the church. If in consultation with their line manager reasonable suspicion is confirmed a disclosure report must be made to the MLRO. This disclosure should be made by email and should be completed as soon as possible after the information came to their attention.</p> <p>The report should include as much detail as possible including:</p> <ul style="list-style-type: none"> - Full available details of the people, companies or other entities involved, including the individual making the disclosure and other members of staff if relevant. - Full details of transaction and nature of each person's involvement in the transaction. - Suspected type of money laundering activity with exact reasons as to why the individual making the disclosure is suspicious. - The dates of any transactions, where they were undertaken, how they were undertaken and the likely amount of money or assets involved. - Any other information that may help the MLRO judge the case for knowledge or suspicion of money laundering and to facilitate his or her report to the relevant authorities. <p>Once this suspicion has been reported to the MLRO any instructions provided by the MLRO must be followed.</p> <p>Further enquires must not be made unless instructed to do so by the MLRO. At no time and under no circumstances should any suspicions be voiced to the person(s) suspected of money laundering.</p> <p>If appropriate the MLRO will refer the case to the UK authorities who will undertake any necessary investigation. This may include consent to continue with a particular transaction and care should be taken not to 'tip off' the individuals concerned, otherwise this may be committing a criminal offence.</p> <p>Reports made by a member of staff to the MLRO under the above procedures will be considered for treatment as a disclosure under the Ministry's Public Interest Disclosure Policy.</p>
2.3.2	External reporting
	<p>On receipt of a disclosure report the MLRO will:</p> <ul style="list-style-type: none"> - Note the date of receipt and acknowledge receipt of it. - Assess and advise the individuals concerned when a response can be expected. - Consider the report and any other relevant information, undertaking further enquires necessary to decide if a report should be made to the National Crime Agency (NCA). <p>Once the MLRO has evaluated the case a timely determination will be made as to whether:</p> <ul style="list-style-type: none"> - There is actual or suspected money laundering taking place - There are reasonable grounds to know or suspect that is the case - Consent is required from NCA for a particular transaction to proceed.

	<p>Where the MLRO concludes that the case should be disclosed to NCA this needs to be done:</p> <ul style="list-style-type: none"> - In a timely manner - In the prescribed manner on a standard report format provided by NCA <p>Where the MLRO concludes that there are no reasonable grounds to suspect money laundering then consent will be given for transactions to proceed, and the disclosure report will be marked accordingly.</p> <p>Where the MLRO considers a potential breach has taken place, the Ministry may be obliged to report serious incidents to the authorities.</p> <p>Details of the reporting to the NCA can be found at: https://www.gov.uk/guidance/money-laundering-regulations-report-suspicious-activities</p>
2.4	Monitoring
	To enable monitoring to be conducted and compliance with this policy to be evidenced, the Ministry will retain all anti-money laundering and counter-terrorist finance records securely for a period of at least five years.
3	Governance Requirements
3.1	Responsibility
	The church administrator has overall responsibility for this policy. Members are expected to be familiar with this policy and to contribute to its effective implementation.
3.2	Implementation / Communication Plan
	Members and donors will be notified of the policy via church website the policy will be available on the policies page of the Ministry website.
3.3	Exceptions to this Policy
	Any exceptions to this policy require approval from the Senior Pastor
3.4	Review and Update
	Minor changes such as change of a role title or other titles or name which do not change the meaning of the policy may be made by the operational owner. Major changes which alter the meaning of the policy or are substantial re-writes will be submitted via the full approval route.

Version History

Version	Author	Revisions Made	Date
1	R Utete	First Draft	16/08/202

Approval History

Committee Sign Off

Version	Name	Date of Sign Off
1	Senior Pastor – M Cox	17/08/2022