Financial Crime and Abuse Policy

VERSION CONTROL		
Version	**Date**	**Summary of changes made**
1.0	29 July 2021	New Financial Crime & Abuse Policy adopted

Policy owner: Chief Operating Officer

Policy approver: Christian Aid Board

Approval date: 29 July 2021

Next review date July 2024

1.0 Background and purpose

1.1 Financial Crime & Abuse is any incident of: terrorist financing, a breach of financial sanctions, trade sanctions or export controls, or money laundering. Definitions of these terms are provided in Annex 1. The purpose of this policy is to set out how Christian Aid will manage these key risks and ensure legal compliance. For risks relating to bribery and fraud, please refer to the specific policies set out in section 12.

1.2 We are a UK-registered Charity, and this Policy is therefore primarily based on UK law, specifically the UK Terrorism Acts[1] and the UK Sanctions and Anti-Money Laundering Act 2018. However, it is also informed by and intended to support compliance with obligations we have beyond UK law arising from donor contracts and our banking relationships.

1.3 These risks and associated legal and contractual obligations are complex and evolve regularly. No policy can fully anticipate all eventualities we may face as an organisation. Instead, this policy sets a risk management framework to support us to address these risks effectively.

1.4 Christian Aid works in over 20 countries, and it would not be feasible to draft a policy which addresses legal requirements across all these jurisdictions. The UK legal framework is comprehensive, and incorporates global measures imposed by the United Nations, however in the event local law exceeds this policy, local legal requirements should take precedence. When in doubt, please consult the Financial Crime Manager, who can determine whether legal advice is required.

2.0 Scope and application

2.1 This Policy applies to Christian Aid's activities worldwide, including all overseas offices and branches, and all separate legal entities owned and controlled by Christian Aid.

2.2 The Policy is applicable to and must be followed by all Christian Aid staff, Trustees and volunteers as well as consultants engaged to carry out work on behalf of Christian Aid or on behalf of all separate legal entities owned and controlled by Christian Aid.

2.3 While this is an internal policy, Christian Aid requires grant funding that it provides to partners and other organisations to be used in a manner that is consistent with our values, and with our legal and contractual obligations. Requirements in respect of managing Financial Crime & Abuse risks will therefore be included in our Funding & Reporting agreements with partners.

3.0 Policy statement

3.1 Delivering Christian Aid's mission to end poverty and our humanitarian mandate frequently requires us to work in locations where risk factors for Financial Crime & Abuse are high. For example, countries subject to sanctions, or locations controlled by terrorist organisations. At

[1] Terrorism Act 2000, Terrorism Act 2006, Counter-Terrorism Act 2008 and Counter-Terrorism and Border Security Act 2019.

the same time, failing to effectively manage Financial Crime & Abuse risks could lead to Christian Aid committing serious criminal offences, breaching donor contracts, losing access to banking services, suffering financial losses and reputational damage.

3.2 We will therefore implement effective, risk-based measures to minimise the risk of incidents of Financial Crime & Abuse occurring, and ensure we respond effectively to any incidents which do occur and report them transparently. The goal being to support our work, including in challenging environments, while meeting our legal and contractual obligations and ensure we work in a way that is consistent with our values. To further guide users of this policy, examples of incidents of Financial Crime & Abuse are provided in Annex 2.

3.3 We will not knowingly or recklessly provide funds or resources either directly or indirectly through our grant funding to partners, to any individual or entity which is subject to a terrorism or sanctions listing imposed by the United Nations Security Council or the United Kingdom government, or which appears on any other published terrorism or sanctions list that we judge relevant to meeting our obligations, as set out in Annex 3. The only exception is situations where we are authorised to do so by a licence or other legal authority and where the existence of such authorisation has been confirmed by the Financial Crime Manager. For example, this means we will not:

- procure goods or services from suppliers which are subject to sanctions; or use sanctioned financial service providers, or sanctioned airlines;
- allow “access payments” or informal “taxes” to be paid to terrorist organisations in connection with Christian Aid projects, whether in the form of money or goods;
- engage an individual who appears on a sanctions or terrorism list as a Trustee or employee; or
- provide grant funding to an organisation which is subject to a terrorism or sanctions listing or which is controlled by a terrorist organisation or its members.

3.4 We will identify and comply with any sectoral sanctions, trade sanctions and export control regulations that may be applicable to our activities. We will not accept donations if we know or suspect they are the proceeds of crime, and will also take all other reasonable steps to prevent Christian Aid from being exploited for the purposes of money laundering, or from suffering other forms of Financial Crime & Abuse incidents, for example tax evasion, or robbery or extortion of project funds and resources by terrorist organisations.

3.5 Many of the threats of Financial Crime & Abuse we face are external in nature. However, Christian Aid Trustees and staff should be aware that we will not tolerate anyone abusing their position within Christian Aid to carry out criminal acts of any kind, whether or not addressed by this policy. This is serious misconduct that will lead to dismissal and a referral to the relevant authorities, in line with our policy *Reporting Criminal Wrongdoing to Statutory Authorities*.

3.6 For the avoidance of doubt, Christian Aid does not operate a “no contact” policy. This means this policy does not prohibit speaking to or meeting with members of terrorist organisations, within clearly defined limits. Further detail on this is in Section 9.

4.0 Exemptions and licences

4.1 Some sanctions regimes include general licences or exemptions which authorise transactions that are otherwise prohibited, e.g. for humanitarian purposes. This Policy does not prohibit transactions that are authorised by a general licence or exemption. Authorisation by a general licence or exemption should be confirmed by the Financial Crime Manager before Christian Aid staff take actions in reliance on the existence of a general licence or exemption, given the legal and regulatory complexities involved in this area.

4.2 In certain circumstances it may also be possible to apply for a specific licence or other legal authority to carry out transactions that would otherwise be prohibited. To support programme continuity Christian Aid is committed to seeking such licences where available and where a licence can be obtained on a timetable that would allow Christian Aid to carry out the transactions in question.

4.3 Any decision to apply for a specific licence requires approval by the Chief Operating Officer (or an appropriate delegate in their absence) and should be notified to the Financial Crime Risk Committee (see paragraph 6.2 below) at its next scheduled meeting. Christian Aid staff should be aware that the decision by a regulator to grant a specific licence is discretionary and may not be granted.

5.0 Duress

5.1 Situations may arise in which payments are made to protect against an imminent threat to the life, health, safety or liberty of Christian Aid representatives or those around them. Representatives making a payment under such extreme duress will not be subject to sanction. Similarly, payments made under duress will not be considered a breach of their Funding & Reporting agreement with Christian Aid if made by partners.

5.2 Such payments **must** be promptly reported afterwards following the reporting requirements set out in this policy. In addition, a security incident report must be filed and measures to mitigate risk of future incidents developed with advice from Corporate Security. Christian Aid will disclose all such incidents to applicable regulators and donors. Where there are concerns a payment under duress has been made to a Proscribed Terrorist Organisation, Christian Aid will file a report with the National Crime Agency under Section 21ZB of the UK Terrorism Act.

5.3 Non-reporting of incidents is exceptionally serious. It may lead to opportunities being missed to take steps which might avoid personnel being put at risk in future, it may cause Christian Aid to commit a criminal offence under UK law, and/or to breach contractual agreements with donors, and could lead to actual or perceived abuse of the duress provision. For this reason, the protection afforded by paragraph 5.1 only applies if the incident is reported in a timely and transparent manner afterwards.

6.0 Governance

6.1 Christian Aid's Audit & Risk Committee is responsible for approving this policy and providing high-level oversight of Financial Crime & Abuse risk management. Any incident of Financial Crime & Abuse will be captured on an incident register which is presented to the Audit and Risk Committee at its scheduled meetings.

6.2 Christian Aid has also established a Financial Crime Risk Committee (FCRC) of senior staff which is responsible for driving Christian Aid's anti-financial crime risk management. The FCRC is subject to documented Terms of Reference and meets not less than quarterly. It is responsible for providing an annual report to the Audit & Risk Committee on Financial Crime & Abuse risks, including the extent and nature of those risks and measures being taken to tackle them. Other specific responsibilities are set out in Section 10.

6.3 To preserve independence the Audit, Risk and Assurance Function does not internally audit its own work except where the ARC has approved an exemption on the basis it will not compromise the overall independence of the Internal Audit Function. It has been approved that testing of procedures implemented directly by the Financial Crime Manager in relation to screening is permitted to be included in the Internal Audit plan. Furthermore, the application of corporate controls to mitigate Financial Crime risk are carried out as part of Christian Aid's broader Internal Audit work and Internal Audit plan. Any review of the effectiveness of Christian Aid's approach to Financial crime risk management, including the design of policy and procedure, will however be performed by appropriately qualified, independent external consultants.

7.0 Risk Management

7.1 Christian Aid's efforts to prevent incidents of Financial Crime & Abuse from occurring rest on the following key pillars. Specific roles and responsibilities are set out in Section 10.

- **Awareness:** we will deliver targeted training and provide communications of recent developments to ensure staff in relevant roles are aware of Financial Crime & Abuse risks, steps they can take to reduce the risk of incidents occurring, and how to report incidents. The Financial Crime Manger is responsible for presenting a training schedule, including roles requiring training and the type and frequency of training to be delivered, to the Financial Crime Risk Committee for approval annually.

- **Risk Appetite:** we will define and set parameters within which risks are expected to be managed, i.e. our "risk appetite", and levels of risk that would be outside of tolerance, i.e. our "risk tolerance" to inform decision making, in our Risk Appetite Statement.

- **Risk Assessment:** we will identify and assess Financial Crime & Abuse risks at both global and regional/country programme level, to ensure that relevant and proportionate risk mitigations are applied. Review of the global risk assessment will be a standing item at each of the quarterly FCRC meetings.

- **Risk & Control Mapping:** an annual Risk and Control Map will be produced mapping identified Financial Crime & Abuse risks to internal controls and programme quality requirements. Once approved by the Financial Crime Risk Committee, the Risk and Control map sets the minimum standard for mitigating Financial Crime & Abuse risks, including additional measures required where risks are high.

- **Screening:** we will carry out risk-based screening against published terrorism and sanctions lists for partners, employees, third parties and other relevant stakeholders, and where relevant will also include adverse media and politically exposed persons databases in our screening. Detailed screening requirements are set out in a separate Screening Procedure produced pursuant to this Policy.

- **Donor contracts:** we will identify Financial Crime & Abuse clauses in donor contracts. In the event they set out requirements which differ from our approach we will seek to negotiate with the donor to confirm they will accept the comprehensive, risk-based approach set out in this Policy. Where this is not possible, we will implement any additional requirements set out in the donor contract, however, we will not reduce the minimum standards set out in this Policy.

7.2 The objective of risk assessment is to minimise the risk of incidents of Financial Crime & Abuse from occurring by ensuring relevant and proportionate mitigations are applied to reduce identified risks. To facilitate this, certain programmes will be **classed as high risk** in respect of Financial Crime & Abuse based on the findings of risk assessments, requiring additional mitigations be applied to address identified risks. Risk classifications will be informed by the views of country managers and the Financial Crime Manager, however final authority for determining classifications sits with the Financial Crime Risk Committee.

8.0 Reporting

8.1 While we will make all reasonable efforts to prevent incidents of Financial Crime & Abuse from occurring, it is possible that incidents will occur in relation to our work, particularly when working in fragile and conflict affected environments. It is essential therefore that measures are in place to detect actual or suspected incidents, and ensure they are reported.

8.2 **Christian Aid staff** are required to report actual or suspected Financial Crime & Abuse incidents. They can report actual or suspected Financial Crime & Abuse incidents through the Misuse of Funds form on the intranet. Alternatively, if for any reason a staff member wishes to make a confidential report, they can do so using Christian Aid's whistleblowing process. Details of both the Misuse of Funds form and the whistleblowing process are available here on Christian Aid's intranet.

8.3 **Christian Aid partners** are required to report actual or suspected Financial Crime & Abuse incidents, and reporting channels are set out in Christian Aid's standard Funding & Reporting agreement with partners. Any Christian Aid staff member receiving a report of actual or suspected Financial Crime & Abuse from a partner is responsible for then escalating it internally, following the procedures set out in paragraph 8.2. Please note that partners or partner staff

members can also submit whistleblowing reports to Christian Aid. Details of how to do this are also included within the Funding & Reporting agreement and made available here on our website: https://www.christianaid.org.uk/about-us/reporting-serious-concerns-christian-aid

8.4 It is a legal requirement to report actual or suspected terrorist financing to the UK authorities, and failure to do so is a breach of UK law. Christian Aid will therefore report actual or suspected terrorist financing incidents to the UK National Crime Agency.

8.5 There is no equivalent mandatory reporting requirement in relation to actual or suspected sanctions or export control breaches or money laundering incidents however it is Christian Aid's Policy to make voluntary disclosures of incidents in the interests of transparency.

8.6 Christian Aid will also make Serious Incident Reports to the Charity Commission and disclose incidents to relevant donors. We will also notify our banks where it is required or otherwise appropriate to do so.

8.7 To further guide users of this Policy, a "Question & Answer" section on reporting is included in Annex 4.

9.0 Interaction with proscribed terrorist organisations

9.1 This Policy does not prohibit speaking to or meeting with proscribed or designated terrorist organisations or their members. We recognise that in some contexts such interaction may be unavoidable, for example if a terrorist organisation is the de facto government of a location we or our partners are working in, and in some cases may even be desirable, for example, if it forms part of an acceptance strategy which helps keep Christian Aid and partner staff safe during programme delivery.

9.2 In accordance with paragraph 3.3 of this Policy Christian Aid will not knowingly or recklessly provide funds or resources to terrorist organisations, either directly or indirectly through our grant funding to partners. Therefore, any such interaction must not involve providing money, property or any material support and resources to anyone that Christian Aid employees know, suspect or believe is connected to a terrorist organisation or to the terrorist organisation itself.

9.3 "Material support and resources" means currency or monetary instruments or financial securities, financial services, lodging, training, expert advice or assistance, safehouses, false documentation or identification, communications equipment, facilities, weapons, lethal substances, explosives, personnel, transportation, and other physical assets, except medicine.

9.4 Any interaction with a terrorist organisation carries significant risks, and Christian Aid has produced a guidance document *Guidance on Operating in Areas with Proscribed Organisations* to support staff to do so safely and in accordance with Humanitarian Principles.

9.5 We recognise that we and our partners work in highly complex environments, and that the nature and extent of any required interaction with terrorist organisations and the associated risks may vary significantly. It is not possible to formulate Policy or guidance which addresses

every scenario we or partners may face. However, we do have access to internal expertise, legal advisors and external networks which we can use to support our efforts to deliver safe, legal and sustainable programming. Any staff member who is uncertain whether a proposed activity or course of action is compliant with this Policy should therefore approach the Financial Crime Manager in the first instance for advice and support.

9.6 Similarly, if a staff member becomes aware that a partner is interacting with a terrorist organisation, they should inform the Financial Crime Manager so that risks associated with this can be assessed. This applies even if the interaction is for apparently benign purposes and/or unconnected with a Christian Aid project.

10.0 Responsibilities of Christian Aid staff

10.1 Responsibilities of Christian Aid staff in relation to this Policy are as follows

- **Directors** are responsible for setting the "tone from the top" in respect of Financial Crime risk management, including by using internal communications and other measures to raise awareness of these key risks and the importance and value of Financial Crime and broader risk management as a key enabler of delivering Christian Aid's Global Strategy

- **Extended Leadership Team** is responsible for ensuring they and their teams understand and comply with the requirements of the Financial Crime and Abuse Policy

- **Financial Crime Risk Committee** determines high-risk classifications; approves the annual risk and control map; sets a 2-yearly anti-financial crime strategy; approves the Screening Procedure; is notified of licence applications; and is notified of actual or suspected incidents.

- **All staff**. Failure to apply this Policy or to report suspected Financial Crime incidents can expose Christian Aid to critical risks. All staff therefore have a responsibility to comply with this Policy and to report any actual or suspected incidents of financial crime. Any staff member can approach the Financial Crime Manager or Head of Counter Fraud for advice and support on policy compliance.

- **Country managers/Heads of Regional Programme** are responsible for identifying and assessing Financial Crime & Abuse risks as part of the country/regional programme risk assessment, and ensuring required mitigations as defined in the Risk and Control Map are applied.

- **Financial Crime Manager** is a focal point and professional advisor in respect of Financial Crime Risk within the organisation; their responsibilities in relation to application of this Policy include: leading the production of the global risk assessment, annual risk and control map, Screening Procedure; and responding to reported incidents, including to make reports to the relevant authorities; and acting as an advisor to colleagues to build awareness and capacity on prevention and detection of risks, including through implementation of appropriate training & communications.

- **Head of Counter Fraud** provides operational leadership of Financial Crime risk management through their management of the Financial Crime Manager and members of the Financial Crime Risk Committee.

- **Head of Audit, Risk and Assurance** provides overall leadership of Financial Crime risk management through their management of the Head of Counter Fraud, support for serious incidents as they emerge, and in ensuring the Fraud and Financial Crime team is adequately resourced to perform its duties.

- **Policy owners** are responsible for responding to recommendations made following approval of the annual Risk and Control Map to amend policies in order to address identified gaps in risk mitigation.

- **Chief People Officer** is responsible for ensuring appropriate screening measures in relation to Christian Aid staff is incorporated into HR policies and procedures, and that the required screening set out in the Screening Procedure is applied.

- **Chief Finance Officer** is responsible for ensuring adequate controls are in place in respect of Christian Aid's bank accounts and payment processes to protect against the risk of money laundering.

- **Heads of Geographic Division** are responsible for reporting significant changes in risk in programmes within their division to the Financial Crime Risk Committee, as well as to the Financial Crime Manager for consolidation into committee papers

- **Signatories to donor contracts** as set out in Christian Aid's Contracting Statement of Authority are responsible for confirming with the CA staff member who is submitting the contract for approval that they have carried out the required steps in respect of identifying and reviewing any counter-terrorism and sanctions clauses set out in section 2.5.2 of the Restricted Funds Policy. Country Managers/ Heads of Regional programmes are responsible for ensuring any donor requirements, over and above this policy, are performed.

11.0 Record Keeping

11.1 Record keeping is a key element of the risk-based approach, providing the necessary audit trail to assist in any financial investigation if required. The provision of evidence to support decision making, and monitoring activity, is key to protecting the reputation of CA if it becomes a victim of financial crime. Record keeping also demonstrates to regulators and law enforcement that CA has complied with the law.

11.2 The Financial Crime manager is responsible for identifying appropriate record-keeping requirements related to this policy and ensuring these are captured in Christian Aid's data retention schedule. This is likely to include: screening records; training records (including attendance and materials used); incident management including internal disclosures and external reports.

11.3 Once the data retention period has expired, Christian Aid will continue to preserve records if they are necessary for the prevention, detection or investigation of money laundering or terrorist financing, for example if CA becomes aware that the authorities are investigating the affairs of Christian Aid, a partner or supplier. When Christian Aid becomes aware of an investigation relating to work undertaken by Christian Aid, a notice will be issued to applicable CA staff requesting that all relevant documents and communications be retained until further notice.

12.0 Related policies and procedures

- Fraud & Misuse Policy
- Anti-Bribery Policy
- Code of Conduct
- Serious Incident Reporting Policy

Annex 1 – Definitions

Terrorist financing:

The UK Terrorism Act 2000 contains several terrorist financing offences set out in sections 15-18 of the Act. The UK maintains a list of Proscribed Terrorist Organisations and providing money or property to any organisations on this list would generally be considered terrorist financing offence under the Act. This list is available here. Under Section 19 of the Act there is also a criminal offence for failing to report suspicions of terrorist financing. Christian Aid therefore will not provide funds or resources to any proscribed organisation. In addition, to meet our contractual obligations with donors and to respect the legal and regulatory obligations of our banks we will not provide funds or resources to organisations listed as terrorist organisations by various other governments or multilateral bodies, as set out in Annex 3. The term "**Terrorist organisation**" used throughout this policy refers to any organisation appearing in the UK list of Proscribed Organisations, or any organisation designated as terrorist under any of the lists in Annex 3.

Financial Sanctions:

Financial sanctions can be administered against individuals, countries or regimes by bodies such as the United Nations, the European Union, the UK Office of Financial Sanctions Implementation and the US Office of Foreign Assets Control. The UK government maintains a consolidated list of individuals and entities designated under sanctions imposed by the UK. [2]

There are two types of financial sanction measures under UK law. Targeted sanctions freeze the funds and assets of specified people or organisations. These sanctions targets appear on publicly available sanctions lists and it is a criminal offence under UK law to transact with them, or with entities they own (i.e. more than a 50% stake, including shares or voting rights) or control. Sectoral sanctions prohibit dealings with an entire economic sector or market within a specified country. Again, to meet our contractual obligations with donors and to respect the legal and regulatory obligations of our banks, we will not provide funds or resources to organisations listed as sanctions targets by various other governments or multilateral bodies, as set out in Annex 3. We will also comply with targeted, sectoral or whole-country sanctions imposed by the US Government (in practice Christian Aid will often qualify for humanitarian exemptions or general licences built into these US measures).

Trade sanctions and embargoes:

These prohibit the exporting of certain types of goods to specified countries. Many are focused on the arms trade, but also can encompass broader categories of goods such as technology (e.g., computers and telecommunications), chemicals, and nuclear power. Christian Aid's partnership model means we are only involved in relatively limited imports of goods to the countries we work in. However, trade sanctions also cover the financing of imports, so we could be held legally responsible for goods imported by one of our partners. In certain circumstances, Christian Aid may also have obligations in respect of US trade sanctions, particularly when transacting in US origin goods or US dollars owing to the responsibility our banks have to ensure they do not facilitate transactions that

[2] https://www.gov.uk/government/publications/financial-sanctions-consolidated-list-of-targets/consolidated-list-of-targets

would be a breach of US trade sanctions. Using non-US banks does not necessarily avoid transactions in dollars or through US financial institutions.

Export controls:

The UK government controls the export of certain types of good from the UK. Any goods which appear on the UK Strategic Export Control List therefore require a licence in order to be exported legally. As with trade sanctions these measures are heavily focused on military goods and technology.

Money laundering:

This is attempting to conceal, convert or disguise property obtained through criminal activities. One technique used in money laundering is to try and cycle the funds through legitimate organisations, including charities. To be effective, money laundering through legitimate organisations relies on a cyclical flow of funds, i.e. the money launderer must be able to place funds and then recover at least part of the funds again or receive some other benefit. The benefit to the money launderer can be direct or indirect. For example, the donor's receipt of a charitable tax deduction, positive publicity by virtue of the donation, or jobs for friends or relatives are examples of benefits that would be sufficient for purposes of money laundering.

Knowingly or recklessly: for the purposes of this policy, to do something knowingly means an individual possesses knowledge that means they are certain or near-certain that a transaction would lead to a breach of this policy, and proceeds anyway. To do something recklessly, simply means that it would have been obvious to any reasonable person (and therefore should have been obvious to the person performing the action) that a transaction was going to lead to a breach of the policy. An example of "recklessness" would be if someone deliberately avoided knowledge of facts that might lead them to believe that a transaction would be a breach of this policy.

Annex 2 – What is an incident of Financial Crime & Abuse?

Examples of incidents of Financial Crime & Abuse which may occur in relation to aid programming are included below. Any of these incidents or similar types of incident, would be reportable under this policy, whether or not the incident involves a violation of law by CA staff or partners. This list is not exhaustive and is intended for illustrative purposes only.

Examples of terrorist financing incidents:

- A partner makes an "access payment" to a terrorist organisation to gain access to a project location in connection with a Christian Aid project (regardless of whether CA grant funds were actually used or not).
- A partner agrees to hand over a percentage of food aid being distributed in the locality to a terrorist organisation as a "tax" for operating in an area they control in connection with a Christian Aid project (regardless of whether the goods were purchased with CA grant funds or not).
- Robbery or extortion of Christian Aid or our partners in connection with a CA funded project by members of a proscribed or designated terrorist organisation. While we/our partners are clearly the victim in this situation, it is crucial such incidents are reported as failure to do so could be itself a criminal offence under UK law.

Examples of breaches of financial sanctions:

- Christian Aid procures goods or services from a supplier which appears on a sanctions list, i.e. the supplier contracts with or invoices us in the same name that appears on the sanctions list.
- Christian Aid procures goods or services from a supplier which is more than 50% owned by a person on a sanctions list, i.e. the company is not on a sanctions list, but it is owned by someone who is.
- Christian Aid provides goods or services to a partner who is subject to sanctions, or to a partner who used Christian Aid funding to provide goods or services to an individual or entity that is subject to sanctions or is more than 50% owned by a person on a sanctions list.
- A partner purchases goods or services from a sanctioned supplier in connection with a Christian Aid project.
- A financial service provider (e.g. bank, FX bureau or cash agent) which is subject to sanctions is used during cash programming.

Examples of breaches of trade sanctions:

- Christian Aid imports goods into a country which are subject to trade sanctions measures.
- A partner imports goods into a country which are subject to trade sanctions measures using grant funding provided by Christian Aid.

Examples of breaches of export controls:

- Christian Aid exports radios which have a potential military use from the UK to a country programme for security purposes, without obtaining the required licences.

Examples of money laundering:

- A criminal poses as a donor and makes a donation and shortly afterwards claims it was a mistake and requests a refund in the form of a payment into a bank account.
- A criminal poses as a donor, and tries to persuade us to accept funds and make a grant to a partner we have never worked with before. Subsequent due diligence raises concerns about whether the partner is a genuine organisation or whether it is controlled by a friend or associate of the donor.
- A criminal poses as another charity, and asks if we will make a fund transfer on their behalf to a conflict zone where access to banking services are challenging.
- A criminal poses as a donor and offer to make a payment through a third-party bank account or some other non-traditional method of payment.
- A criminal posing as a donor makes a donation that seems inconsistent with the donor's known sources of legitimate wealth.
- A criminal posing a donor is identified in public reporting as related to a government official who is involved in official corruption.

Annex 3: Applicable Lists

Christian Aid is a UK-registered Charity. This means we are subject to UK law across all our activities globally. In addition, sanctions or counter-terrorism measures imposed by the United Nations are automatically transposed into UK law, meaning UN-designated terrorists and sanctions targets also appear within the UK lists. Compliance with UK law also achieves compliance with UN measures.

However, as an organisation with a variety of donors including governments, foundations and multilateral bodies, and which regularly transacts internationally using US dollars we have additional obligations to our donors and banks which extend beyond UK requirements. For that reason, we will not knowingly transact with any individual or entity appearing on the following lists.

The UN Security Council Sanctions List

The UK List of Proscribed Terrorist Organisations

The UK List of Consolidated Financial Sanctions Targets

The EU List of Consolidated Sanctions

The US List of Specially Designated Nationals

The Australian Criminal Code List and Sanctions List

The Switzerland List of Sanctions

We may screen against other lists where we feel this is necessary for the purposes of legal or regulatory compliance or to manage other risks.

Annex 4: Incident Reporting Q&A

Can reports be made anonymously?

In the interest of fostering a positive and open financial crime compliance culture, we encourage all staff to use the Misuse of Funds form to report any financial crime concerns.

However, we appreciate that some individuals may wish to raise concerns anonymously, and so they can do so using the whistleblowing process on the website.

What is the benefit of reporting incidents?

Reporting actual or suspect incidents is a key component of effectively managing Financial Crime & Abuse risks and a requirement for all CA personnel, as well as for partners and other recipients of CA grant funding (with reporting requirements set out in the Funding & Reporting agreement). It allows steps to be taken to protect against further incidents occurring, supports timely and transparent notification of incidents to statutory authorities and donors, banks and other relevant parties, and supports our ongoing risk management by allowing lessons to be learned.

What are the risks of failing to report incidents?

Delayed reporting, or a failure to report Financial Crime & Abuse incidents exposes Christian Aid to significant risks, including the risk of committing criminal offences under UK law by failing to make mandatory reports to relevant statutory authorities, breaching donor contracts and regulatory duties. It also poses a significant programme risk if funds are diverted from target beneficiaries and used to support the activities of armed organisations that are likely causing harm to affected communities.

What are the implications for partners in reporting incidents?

Timely and transparent reporting of incidents by partners is seen by Christian Aid as a sign of a strong partnership and a healthy approach to risk management and compliance. We recognise that when working in complex environments incidents of Financial Crime & Abuse are possible, even if effective risk mitigation has been applied. If a partner reports an incident, we will seek to work with the partner in a collaborative way to fully establish the facts and reduce risk of future incidents occurring. It is probable that we will also need to notify our back donors and may also need to inform statutory authorities in the UK. We understand partners may be concerned about the impact of reporting an incident on their partnership with Christian Aid. In rare cases, we may need to review our ongoing relationship with a partner in response to an incident. However, this is the exception and our preferred approach is to seek to work with partners to resolve the issue, support programme continuity and reduce the risk of future incidents.

How does Christian Aid respond to reports?

All reports received will be assessed. This process will usually be coordinated by Christian Aid's Financial Crime Manager, Head of Counter Fraud or another member of the Audit, Risk & Assurance team if they are unavailable. Generally, this assessment will include the following steps

- Evaluating whether an incident has occurred, or if there are credible suspicions that one has. Further fact finding or an investigation may be needed to support this evaluation.

- Determining if an actual or suspected incident is ongoing, and whether immediate steps need to be taken to avoid further breaches of law or regulation.
- Determining whether external notifications need to be made to statutory agencies or donors
- Identifying what steps can be taken to support programme continuity, in compliance with the law.
- If it is determined an incident or “near miss” has occurred, ensuring lessons are learned which can inform ongoing risk management.
- Steps taken in response to a report of Financial Crime or Abuse will be documented and retained in accordance with CA retention policies.