Fraud, Bribery, and Corruption Policy

1. Purpose

Fraud, bribery, and corruption, and other related illegal matters (**hereon referred to under the label of 'fraud')** undermine our efforts to help people in need. This policy is our approach to preventing, detecting, and managing the risk and incidents of fraud, both in the UK and internationally.

2. Scope

This policy applies to all staff, volunteers, and third parties representing the British Red Cross and its operations in the UK and internationally.

In this policy the term fraud includes risk and incidents of fraud, bribery, corruption, financial abuse, money laundering, funding terrorism, violating financial sanctions and other related illegal financial matters. See the definitions for more information.

3. Policy Statement

BRC does not accept acts of fraud. This means we have a strict, uncompromising approach to the application of the law, and we act accordingly where risks and issues are identified.

BRC is committed to maintaining a culture where such behaviours and actions are unacceptable. We expect our people and partners to act with the highest standards of integrity.

BRC will investigate and seek to take appropriate disciplinary and / or legal action against those who commit, or assist in committing, fraud or other improper activities in our operations.

3.1. Counter Fraud

BRC's leadership is committed to countering wrongdoing in the following ways:

3.1.1. An anti-fraud culture across the British Red Cross through the championing of ethics and integrity in all our activities and decisions.

3.1.2. Minimising opportunities for fraud by ensuring that we have effective systems, procedures, and controls to prevent, detect, and deter wrongdoing.

3.1.3. Protecting the people that we support from fraud perpetrated by those acting on behalf of our Organisation.

3.1.4. Assessing our exposure to the risk of fraud.

3.1.5. Carrying out risk assessment and due diligence checks on partner organisations, suppliers, and contractors to ensure they work to the same or equivalent standards.

3.1.6. Ensuring our people understand the risks and their obligations to prevent, identify, and report any actual or suspected incidents of fraud through training and awareness.

3.1.7. Taking all reported incidents seriously and investigating them proportionately and appropriately, while protecting those who report in good faith.

3.1.8. Using learning and insights to strengthen systems and address weaknesses.

3.1.9. Meeting our obligations to inform relevant external authorities of incidents of fraud.

Training and Communication

3.1.10. We will provide mandatory training and ongoing communication to support compliance with this policy.

3.1.11. We will monitor and report to ELT on training completion rates.

Reporting Issues and Concerns

3.1.12. Concerns or suspicions of fraud or irregularities must be reported and those who report in good faith will be protected.

3.1.13. Fraud investigations will maintain confidentiality and communication will be restricted.

3.1.14. The following reporting routes are available, all of which are secure and confidential: Datix Cloud IQ (incident management), Safecall, or through directly contacting internal audit and counter fraud. For information refer to RedRoom.

Fraud Response

3.1.15. Fraud reports will be triaged and investigated in accordance with the BRC fraud response plan managed by internal audit and counter fraud and overseen by the Safecall Group.

3.1.16. Internal audit and counter fraud maintain a record of all incidents and provides an annual report to the Board of Trustees via sub-committees.

3.2. Lessons Learned from Policy Evaluation

3.2.1. The language of this policy was refined as part of a review from internal stakeholders and Gartner's external benchmarking.

4. Responsibilities

4.1. The **Board of trustees** has overall responsibility for our approach to fraud.

4.2. The **Executive Leadership Team (ELT)** is responsible for establishing and maintaining a sound system of internal control that is designed to

identify and manage key risks, including those related to ethics and integrity. Specific fraud responsibilities within the ELT are as follows:

4.2.1. Chief Operating Officer (policy owner) is responsible for ensuring that this policy allows achievement of external and internal standards. They are also responsible for counter fraud measures, transaction processing, and the personnel (i.e., disciplinary) aspects of fraud. The post holder responsibilities include taking/facilitating the actions to improve processes, systems, and management of any disciplinary or legal action.

4.2.2. Chief Finance Officer is responsible for the financial aspects of fraud. This covers consideration of the materiality of the fraud and actions relating to write-off of funds. They are consulted on the actions to improve controls following an investigation.

4.3. Internal audit and counter fraud (policy lead) together with the policy owner, is responsible for the development, monitoring, and review of this policy. The function provides assurance on the management of risk and the effectiveness of the control framework. They provide advice on processes and procedures for the prevention and detection of irregularities and will undertake investigations of allegations of potential fraud.

4.4. The Safecall Group meets periodically and is made up of CEO office, Internal Audit, Compliance, People Services, and Communication leads. It provides oversight of fraud arrangement and investigation in the organisation.

4.5. Managers will promote a culture of fraud awareness and education within their teams and ensure fraud risks are considered periodically.

4.6. All our people are responsible for ensuring they are compliant with our controls and reporting suspected, actual, or attempted irregularity as soon as possible. Our people are also encouraged to suggest improvements to our systems, processes, and culture to mitigate the risk of irregularities.

5. Governance

Associated policy document/s	**BRC Wide**: Code of Conduct; Conflicts of Interest and Gifts & Hospitality Policy; Confidentiality policy; Disciplinary policy; Grievance Resolution policy; Raising a Concern policy; Information Security policy; Information Governance policy; Safeguarding policy; Procurement and purchasing policy. **Retail**: Retail field managers reporting theft and fraud; and shop guidance reporting theft and fraud.

	IFRC: Policy on the Protection of Integrity of National Societies and Organs of the International Federation; Movement Statement on Integrity.	
Policy(ies) superseded	N/A	
Legislation/ regulatory requirements and standards	Theft Act 1968 and 1978; Fraud Act 2006, Bribery Act 2010, Money Laundering Regulations 2007, Proceeds of Crime Act 2002, Terrorism Act 2000, Sanctions and Anti-Money Laundering Act 2018.	
Equality impact assessment	No equality impact identified	
Data Protection impact assessment	No data protection impact identified	
Environmental impact assessment	No environmental impact identified	
Endorsing Authority; Endorsement date	Executive Leadership Team, 04 2024	
Approval Authority; Approval date	BoT, 07 2024	
Policy Owner	Chief Operating Officer	
Policy Lead	Head of Internal Audit & Counter Fraud	
Date effective	07 2024	
Interim update date	N/A	
Review date	07 2027	
Version	Version number 5.0	
Keywords	Counterfeit, fake, imposture, sham, lying, dishonesty, crime, theft, safecall, whistleblowing, reporting line, internal audit, investigate, investigation, reporting, fraud, corruption,	
Revision history	**Version**	**Summary of change (s)**
	5.0	Scheduled review into the new format. Wording simplified. Addition of the Safecall oversight group and reference to fraud response.
	4.0	Interim update to check and confirm the policy is fit for purpose until a full review is finalised, Change of ownership (CFO to COO).
	3.0	Scheduled review. Policy revised to aid clarity
	2.0	Interim update, Part of DFID improvement plan, add reference to BRC Code of Conduct

	1.0	Scheduled review. Strengthened policy and inclusion of Bribery Act requirements
	0.0	New policy on ‘Anti-fraud and corruption’.

Appendix: Definitions

Fraud: A dishonest act intended to result in a gain or advantage for the individual, or cause BRC a loss. This may include, but is not limited to, theft of money or property including theft from the people we support, the misuse of funds, assets or other resources, fabrication of expense claims and false accounting perpetrated by those acting on behalf of our organisation. In this policy the term fraud includes risk and incidents of fraud, bribery, corruption, financial abuse, money laundering, funding terrorism, violating financial sanctions and other related illegal financial matters.

Bribery: Offering, giving, receiving, or asking for an incentive to achieve a favourable behaviour or outcome. This includes, but is not limited to, receiving a payment from a supplier for awarding them a contract, offering, or making a payment to an official to induce them to perform their duties more quickly or in favour of the individual or BRC. The Bribery Act 2010 makes it an offence if an organisation fails to take reasonable steps to prevent bribery. Whilst bona fide hospitality is acceptable, the conflicts of interest policy and procedure provides further detail on how declarations of gifts and hospitality must be made.

Corruption: Abuse of a position of trust to gain an undue advantage. This could include, but is not limited to, favouritism in the appointment or reward of external consultants or members of staff, or disclosing private, confidential, or proprietary information to outside parties without consent.

Financial abuse: The theft of money or belongings from a British Red Cross service user who may be considered an adult at risk. Financial abuse may also include offering an unofficial service for personal financial gain, for example privately agreeing to give care or assistance to a BRC service user in return for payment or material goods.

Money laundering: How criminals make the money they have gained from a crime look legitimate. One area where a charity could be involved is by receiving donations in cash, which the charity is subsequently asked to repay by cheque. This would result in the donor receiving what is referred to as “laundered” money, as it is now from a reputable source. Gifts with unusual conditions, such as the requirement to pass money on to a third party should also be treated cautiously.

Funding Terrorism: Various activities involving money or other forms of property which in some way further the purposes of terrorism. Activities can include raising, possessing, and using money or other forms of property for these purposes. They can also include entering arrangements to make money or other forms of property available for the purposes of terrorism. Moreover, such activities can involve the laundering of terrorist property.

Violating Financial Sanctions: Breaching of prohibitions that target certain individuals, organisations and/or states, which are designed either to limit the provision of certain financial services or to restrict access to financial markets, funds, and economic resources. There are other types of sanctions which may be relevant to the British Red Cross’ work such as trade sanctions.