Anti Fraud Policy

Introduction

This policy sets out Conciliation Resources' zero tolerance position towards fraud and other forms of dishonesty, together with the steps that must be taken where any of these practices are suspected or discovered. The policy applies to all staff, volunteers board members and any person or organisation acting on behalf of Conciliation Resources.

Principles

Conciliation Resources continually strives to ensure that it operates in a legal and ethical manner and that its decision making and all financial and administrative processes are carried out and reported honestly, accurately, transparently and accountably all sitting firmly within our charitable objectives as well as our Mission Statement, Values and Goals. We will not condone any behaviour that falls short of these principles.

Each member of staff, volunteer board member or any person or organisation acting on behalf of Conciliation Resources has a responsibility for putting these principles into practice. They should report any breaches they discover in line with this policy as a failure to report places that person, in the eyes of the law, in the same category as the person who commits, or attempts to commit, fraud, theft or any other dishonesty.

Conciliation Resources will investigate all reported instances of actual, attempted or suspected fraud involving anyone connected with, or supplying goods or services to, Conciliation Resources.

We will seek to recover funds and assets that may have been lost as a result of the fraud and may take appropriate disciplinary action against an individual or individuals, up to and including dismissal. Where appropriate we will work with police and other relevant bodies such as our external auditors or the Charity Commission as examples.

Definitions

The UK Fraud Act 2006 updated legislation and case law and defines four different ways of committing an act of fraud:

- **False representation** – dishonestly making a false representation to another person[1] (such as a donor or partner), and by doing so makes a gain for themselves or someone else, or causes another person to be exposed to a risk of, or actual, loss. Linked to this is **obtaining services dishonestly** which is an offence under section 11, where someone dishonestly obtains services for themselves or someone else and avoids or intends to avoid paying for them in full

[1] "Person" has a wide meaning and covers an individual through all types of organisations.

or in part.

- **Failure to disclose information** – dishonestly failing to disclose to another person or organisation information which one is under a legal duty to disclose, and by failing to disclose the information, to make a gain for themselves or someone else, or to cause another person or organisation to be exposed to a risk of, or actual, loss.
- **Abuse of position** – when a person who occupies a position in which they are expected to safeguard, or not to act against the financial interests of another person, dishonestly abuses that person, and intends, by means of the abuse of that position to make a gain for themselves or someone else, or to cause another person to be exposed to a risk of, or actual, loss. A person may be regarded as having abused their position even though their conduct consisted of an omission rather than a deliberate act.
- **Possession, making and supplying articles for use in frauds** – examples of this are counterfeit goods presented as genuine or forged credit cards or the equipment to make forged credit cards.

Initial guidance if you suspect a fraud

A fraud may be uncovered in a variety of ways, from your own observations, someone from inside or outside of Conciliation Resources reporting concerns, ongoing controls throwing up a discrepancy, internal review or external audit discovering a problem, or external regulators and inspectors finding something. It is important for all members of staff, volunteers or trustees to know how to deal with their suspicions.

Things to do:

- Stay calm – remember you are a witness not a complainant.
- Write down your concerns immediately – make a note of all relevant details such as what was said in phone or other conversations, the date, the time and the names of anyone involved.
- Consider the possible risks and outcomes of any action you take.
- Make sure your suspicion is supported by facts, don't just make allegations.

Things not to do:

- Do not become a private detective and personally conduct an investigation or interviews.
- Do not approach the person involved (this may lead to him/her destroying evidence).
- Do not discuss your suspicions or case facts with anyone other than those persons referred to below unless specifically asked to do so by them.
- Do not use the process to pursue a personal grievance.

Some things to remember:

- You may be mistaken or there may be an innocent or good explanation – this will come out in the investigation.
- Anyone who may be accused of being involved in committing a fraud is innocent, until proven otherwise, and should be treated as such.
- The process may be complex and you may not be thanked immediately and the situation may lead to a period of disquiet or distrust in Conciliation Resources despite your having acted in good faith.

Reporting your suspicions

The following reporting lines are to be used regardless of the potential magnitude of the fraud, which it is always difficult to quantify at an early stage. Report your suspicions as below:

Your line manager

Generally, this should be your first reporting point. Fraud prevention is everyone's responsibility however your line manager will know the systems, the people, Conciliation Resources and what might be at risk. They should know whom to bring in and the next steps that should be followed and are detailed below.

A senior manager or member of the Executive Management Committee

If you think your manager might be involved in the fraud or if you feel they have not taken your concerns seriously, then you should go to their line manager or member of the Executive Management Committee.

Fraud reporting email/intent

If you want to be assured of absolute confidentiality or wish to remain anonymous, you can report your concerns directly to the Chief Operating Officer by email to disclosure@c-r.org.

Public Interest Disclosure Policy

Conciliation Resources' Public Interest Disclosure Policy, which is available on this page of the website, provides advice on reporting past, present or future criminal acts (such as fraud). You should write to the Chief Operating Officer, Executive Director, Treasurer or Chair of the Board of Conciliation Resources with your concerns. Provided reports are made in good faith, you are protected by Conciliation Resources and the law against retribution, harassment or victimisation and your confidentiality will be preserved.

Guidance for line managers on receiving a report alleging fraud

If you receive a report of an alleged fraud, you should –

- Listen to the concerns of the person making the report and treat every report you receive seriously and sensitively.
- Make sure that the person is given a fair hearing.
- You should reassure your member of staff or volunteer that they will not suffer because they have told you of their suspicions.
- Obtain as much information as possible from them.
- Do not interfere with any evidence and make sure it is kept in a safe place.
- Request them to keep the matter fully confidential in order that senior management are given time to investigate the matter without alerting the suspected/alleged perpetrator/s.
- If you suspect the fraud involves another department then you should notify the appropriate Executive Management Committee Director for further action in accordance with this policy.
- If you believe the suspected fraud to be complex, significant, sensitive (e.g. the reputation of Conciliation Resources) or implicates a senior member of

Conciliation Resources, do not carry out an investigation yourself – this could hinder due process and any criminal enquiry.

In all instances report the matter immediately to the Executive Director, Chief Operating Officer, Treasurer or the Chair of the Board. They will decide on activation of the detailed Fraud Response Plan Conciliation Resources has in place to respond to any report of, and investigation into, a report of fraud, and if the Fraud Response Plan is activated a Fraud Response Team will be put in place. In all instances the Chief Operating Officer will talk with Conciliation Resources' external auditors and lawyers to seek appropriate guidance and support in addressing the issues raised.

Other information

Attached to this policy are three appendices.
Appendix 1 gives definitions of different types of behaviour that can be associated with fraud.
Appendix 2 provides examples of possible fraud warning signs.
Appendix 3 gives examples of controls to prevent fraud.

The best defense we have is vigilance and ensuring we follow our own processes and procedures and questioning if we are not comfortable with the information or paperwork we are presented with. This applies to both internal and our external relationships.

February 2023

CONCILIATION RESOURCES

Appendix 1

Fraud is an umbrella expression for which there is no single legal definition. Until the UK Fraud Act 2006, the definitions of fraud had developed from Common Law and case law. The definitions below are examples of how a fraud can be perpetrated.

Bribery: this implies a sum or gift given that alters the behaviour of the person in ways not consistent with the duties of that person. It includes offering, giving, receiving or soliciting any item of value in order to influence an action. For full details on Conciliation Resources Anti Bribery Policy you should see P/04/12.

Collusion: the term "collusion" covers any case in which someone incites, instigates, aids and abets, conspires or attempts to commit any of the crimes of fraud.

Conspiracy: this is an agreement between two or more persons to break the law at some time in the future. It includes breaches of regulations.

Corruption : this is a general concept describing any organised, interdependent system in which part of the system is either not performing duties it was originally intended to, or performing them in an improper way, to the detriment of the system's original purpose.

Deception : to intentionally distort the truth in order to mislead others. It would include obtaining property, services or pecuniary advantage by deception or evading liability. Deceptions include:

- Misrepresentation of qualifications to obtain employment.
- Obtaining services dishonestly via technology e.g. where a credit card that has been improperly obtained is used to obtain services from the internet, or any other situation where false information is provided to a machine.
- Possessing, making and supplying articles for use in fraud via technology e.g. computer programmes designed to generate credit card details that are then used to commit or facilitate fraud.
- Undeclared and unauthorised private and consultative work.
- Money laundering (see below).
- Providing misleading information to donors in order to obtain funds, such as overstating activity (note that this is an example of a fraud for the benefit of Conciliation Resources rather than to its detriment).

Forgery: this is the making or adapting objects or documents with the desire to deceive.

Extortion: this occurs when a person obtains money or property from another through coercion or intimidation.

Embezzlement: this is the fraudulent appropriation by a person to their own use of property or money entrusted to that person's care but owned by someone else.

False Accounting: this is dishonestly destroying, defacing, concealing or falsifying any account, record or document required for any accounting purpose, with a view to personal gain or gain for another, or with intent to cause loss to another or furnishing information which is or may be misleading, false or deceptive. It includes:

- Manipulation or misreporting of financial information
- Fraudulent completion of official documents (e.g. VAT receipts)

Money laundering: this is the term used to describe the ways in which criminals process illegal or "dirty" money derived from the proceeds of any illegal activity (e.g. the proceeds of drug dealing, human trafficking, fraud, theft, tax evasion) through a succession of transactions and deals until the original source of such funds has been obscured and the money take on an appearance of legitimate or "clean" funds.There are three internationally accepted phases to money laundering:

- **Placement** – this involves the first stage at which funds from the proceeds of crime are introduced into the financial system or used to purchase goods. This is the time at which the funds are most easily detected as being from a criminal source. Such "dirty money" will often be in the form of cash or negotiable instruments such as travellers cheques.

- **Layering** – this is where the funds pass through a number of transactions in order to obscure the origin of the proceeds. These transactions may involve entities such as companies and trusts (often offshore).

- **Integration** – this is when the funds are available via a legitimate source and allow the criminal to enjoy access to the funds again, with little fear of the funds being detected as being from a fraudulent source.

Theft: the illegal taking of someone else's property without that person's freely-given consent. Apart from the obvious theft of Conciliation Resources physical and intangible assets such as computers, and money, it includes:

- Misappropriation of funds
- Misuse of assets, including cash, stock and other assets, for example "borrowing" petty cash, excessive use of photocopiers for private purposes
- Theft from a client or supplier
- Theft of intellectual property (e.g. unauthorised use of the Conciliation Resources name / logo, our proprietary thinking and intellectual capital or images).

There are three main areas where by Conciliation Resources may become exposed:

1. A charity may be formed with the intention to undertake some form of criminal activity (which may include tax evasion). These charities are likely to be small or have a short life cycle since their affairs will be less scrutinised however they may well attempt to obtain resources from Conciliation Resources.

2. Conciliation Resources may benefit from crime by receiving a grant or completing a contract with money that could be considered to have arisen as proceed of crime.

3. Conciliation Resources may be specifically targeted for money laundering. Staff and volunteers should look out for

   - Requests from partners or consultants for funds to be paid to a third party and

no satisfactory explanation can be documented for this arrangement;
- Gifts that are subsequently asked to be repaid as though they were loans;
- Gifts with unusual conditions such as a certain amount being passed on to a particular destination;
- Loans being made in one currency and then repaid in another;
- Loans made in cash and due to be repaid in cheque.

Our mitigation for these is using the Ethical Fundraising Policy to evaluate any potential donor against agreed criteria and seek to protect Conciliation Resources reputation and ensuring we know our partners, undertaking appropriate enquiry and recording in our files the rationale for working with or continuing to work with any particular partner.

In addition following our own existing procedures as putting in place appropriate contracts or Memorandum of Understanding, Terms of Reference with clear deliverables and timeframes, paperwork requesting funds is correctly completed and received as we expect it to be i.e. from the partner organisation on their headed paper, signed appropriately with funds being paid to a bank account in the name of the partner and that all the necessary paperwork is attached and that if there are any issues they are highlighted and can be explained.

CONCILIATION RESOURCES

Appendix 2

Warning signs for fraud

There are warning signs that can indicate a fraud may be taking place, these can include:

- Staff under stress without a high workload
- Reluctance to take annual leave
- Being first to arrive in the morning and last to leave in the evening
- Refusal of promotion
- Unexplained wealth
- Sudden change of lifestyle
- Suppliers/ contractors who insist on only dealing with one staff member
- A risk taker or rule breaker
- Disgruntled at work / not supportive of Conciliation

Resources mission Fraud Indicators can include:

- Staff exhibiting unusual behaviour (see list above)
- Missing key documents (invoices/ contracts)
- Inadequate or no segregation of duties
- Documentation which is photocopied or missing key information
- Missing expenditure vouchers
- Excessive variations to budgets / contracts
- Bank and ledger reconciliations not regularly preformed and cannot be balanced
- Numerous adjustments or exceptions
- Overdue pay or expense advances
- Duplicate payments
- Ghost employees on payroll
- Large payments to individuals
- Crisis management coupled with a pressured work environment
- Lowest tenders or quotes passed over without adequate explanation
- Single vendors
- Climate of fear / low staff morale
- Consistent failure to implement key controls
- Management frequently overriding controls

CONCILIATION RESOURCES

Appendix 3

Examples of controls to prevent and detect fraud

- thorough recruitment procedures
- physical security of assets
- clear organisation of responsibilities and reporting lines
- adequate staffing levels
- supervision and checking of output
- separation of duties to ensure that key functions and controls are not performed by the same member of staff
- rotation of staff
- random spot checks by managers
- complete and secure audit trails
- performance monitoring by management
- budgetary and other financial reports
- reviews by independent bodies such as audit

Fraud Register

The Fraud Register contains the following headings:

- Case number
- Date of reporting
- Location of incident(s)
- Nature of alleged incident
- Key persons involved
- Time period over which the incident(s) occurred
- Value (estimated or actual) associated
- References to documentary and other evidence sought or acquired
- Control weaknesses identified
- Recommendations for improvement / further action identified
- Responsibilities and time frames for action