Building Bridges Programme Anti-Fraud Policy

1. Introduction

The purpose of this policy is to set out the Building Bridges Programme position on fraud and set out responsibilities for its prevention. It also refers those involved in delivering the programme to the Fraud Response Plan, which outlines the action to be taken if they discover or suspect fraud.

The Building Bridges Programme requires everyone involved in delivering the programme to act honestly and with integrity at all times and to safeguard the resources for which they are responsible.

Fraud is an ever-present threat to these resources and hence must be a concern of all members of staff and volunteers involved in the programme.

We recognise that individual organisations within the Building Bridges Partnership will have their own Anti-Fraud Policies and this Policy is intended to operate in conjunction with these in matters relating to the delivery of the Building Bridges Programme.

This Policy also operates in conjunction with the Building Bridges Programme Whistleblowing Policy.

2. What is Fraud?

The term fraud is used to describe a whole range of activities such as deception, bribery, forgery, extortion, corruption, theft, conspiracy, embezzlement, misappropriation, false representation, concealment of material facts and collusion.

Generally, however, fraud involves the intention to deceive a person or organisation in order to obtain an advantage, avoid an obligation or cause loss.

Particular regard is made to the risk facing organisations of involvement in the practice of money laundering and this policy will seek to reduce the risk of deliberate or unintentional involvement in this practice.

The term also includes the use of information technology equipment to manipulate programs or data dishonestly, the theft of IT equipment and software, and the intentional misuse of computer time and resources.

3. Building Bridges Programme Attitude to Fraud

The Building Bridges Programme takes the most serious view of any attempt to commit fraud by members of staff, volunteers, contractors, their employees and agents acting on behalf of the programme, and others.

Anyone involved in the delivery of the programme that is involved in impropriety of any kind will be subject to disciplinary action, including prosecution, if appropriate. The Building Bridges Programme will treat attempted fraud as seriously as accomplished fraud.

4. Lead Organisation and Partner Responsibilities

As the lead partner for the Building Bridges Programme, Community First has overall responsibility for the prevention of fraud on the Building Bridges programme.

Individual partner organisations will, however, remain responsible for the prevention of fraud in all of their activities relating to the delivery of the Building Bridges Programme.

The Community First Chief Executive is responsible to the Community First Board for:

- developing and maintaining effective controls to help prevent or detect fraud on the programme;
- carrying out vigorous and prompt investigations if fraud occurs;
- taking or promoting appropriate disciplinary and/or legal action against perpetrators of fraud;
- taking or promoting disciplinary action against individuals where their failures have contributed to the commission of the fraud.

5. Staff and Volunteer Responsibilities

The Community First Chief Executive, Building Bridges Programme Manager and Community First Head of Finance are responsible for the prevention and detection of fraud on the programme by ensuring that an adequate system of internal control exists within their areas of responsibility and that these controls operate effectively.

As a result, there is a need for the relevant managers in all partner organisations to:

- identify and assess the risks involved in the operations for which they are responsible in relation to the programme;
- develop and maintain effective controls to prevent and detect fraud;
- ensure compliance with programme and organisational controls; and
- ensure that agreed programme and organisational procedures are followed.

Every person involved in the delivery of the programme:

- has a duty to ensure that the Building Bridges Programme funding, its good reputation and its assets are safeguarded;
- should alert their line manager where they believe the opportunity for fraud exists because of poor procedures or lack of effective supervision;
- has a responsibility to report details of (a) any suspected or actual fraud, or (b) any suspicious acts or events, to their line manager, Finance Manager or Chief Executive - if they do not believe this route is appropriate, they should report it to the Building Bridges Programme Manager, the Community First Head of Finance, the Community First Chief Executive or the Big Lottery Funding Officer.
- assist in any investigations by making available all relevant information and by co-operating in interviews.

6. Building Bridges Fraud Response Plan

The Building Bridges Programme has prepared a Fraud Response Plan (see Appendix 1) which can act as a checklist of actions and a guide to follow in the event of fraud being suspected. This plan includes:

- actions to be taken following the report,
- who to report to,
- how to secure the evidence,
- how to prevent losses,
- who should notify the Police and investigate the fraud, and
- who has responsibility for notifying stakeholders and dealing with external enquiries.

7. Appendices

The are four appendices to this Policy:

- Appendix 1 – Building Bridges Programme Fraud Response Plan
- Appendix 2 – Examples of Fraud
- Appendix 3 – Examples of Controls to Prevent and Detect Fraud
- Appendix 4 – Warning Signs of Fraud

8. Key Contacts

The key contacts for concerns to be raised through this policy are:

Position	Name	Email Address	Telephone Number
Building Bridges Programme Manager	Dave Potts	dpotts@communityfirst.org.uk	01380 732826 07738 883186
Community First Head of finance	Sam Beale	sbeale@communityfirst.org.uk	01380 732803
Community First Chief Executive	Lynn Gibson	lgibson@communityirst.org.uk	01380 732811 07905 679031
Big Lottery Fund Funding Officer	John Dewing	john.dewing@biglotteryfund.org.uk	0191 376 1902

9. Policy Review

This policy will be regularly reviewed by the Building Bridges Partnership on at least an annual basis to incorporate any necessary operational or legislation changes.

10. Amendment History

Version	Date	Comments
Draft	November 2017	Draft issued for comment
1.0	December 2017	Version 1.0 formally issued

Issued by:

Name: **Dave Potts**
Position: **Building Bridges Programme Manager**

Signature:
Date:

Appendix 1 – Building Bridges Programme Fraud Response Plan

Introduction

It is important that everyone involved in the delivery of the Building Bridges Programme knows what to do in the event of a suspected fraud so that they can act without delay.

The Fraud Policy covers the action required when fraud is suspected and to whom the fraud or suspicion should be reported.

The Fraud Response Plan is a guide to how and by whom the fraud suspicion will then be investigated, reported and closed.

The Fraud Response Plan provides an outline of many of the areas that will need to be considered when investigating a large and complex fraud. For smaller less complex frauds, there will be parts of the plan that will not be applicable. It is however important to keep an open mind and consider whether a small fraud is concealing a much larger fraud.

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 blowing the whistle, concerns being raised by programme participants, ongoing controls throwing up a discrepancy, internal or external audit discovering a problem, or external regulators and inspectors finding something. It is important for you to know how to deal with your 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 allege.

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 them destroying evidence)
- Do not discuss your suspicions or case facts with anyone other than those persons referred to in Section 8 this Policy 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
- The process may be complex and you may not be thanked immediately
- The situation may lead to a period of disquiet or distrust in the programme or organisation 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 would be difficult to quantify at an early stage. Report your suspicions as below:

- **Your line manager -** Generally this is your first port of call. Fraud prevention is their responsibility. They will know the systems, the people, what is at risk. They should know whom to bring in.

- **A more senior manager or Board Member** - If you think your manager might be involved in the fraud or if you feel they have wrongly dismissed your concerns, then you should go to a more senior manager or Board member within your organisation.

- **Alternative escalation routes** - If you do not believe that any of the above escalation routes are appropriate, you should report your concerns to the Building Bridges Programme Manager, the Community First Head of Finance, the Community First Chief Executive or the Big Lottery Funding Officer.

Whistleblowing
The Whistleblowing Policy provides advice on reporting criminal acts (such as fraud). Provided reports are made in good faith, you are protected by the Building Bridges Programme and the law against retribution, harassment or victimisation and your confidentiality will be preserved.

Guidance for line managers on receiving a report of fraud:
- Listen to the concerns of the person raising the concerns and treat every report you receive seriously and sensitively. Make sure that all people involved are given a fair hearing.
- You should reassure anyone raising concerns that they will not suffer because they have told you of their suspicions.
- Get as much information as possible from the person raising the concern. Do not interfere with any evidence and make sure it is kept in a safe place.
- Request the person raising the concern to keep the matter fully confidential in order that senior management are given time to investigate the matter without alerting the suspected/alleged perpetrator

Fraud Response Plan

Please note – This plan has been created for controlling any reports of Fraud to the Building Bridges Programme team, but can be adapted as necessary for concerns reported within partner organisations.

	Date	Comment
Actions		
Immediate Action		
Notify Building Bridges Programme Manager and Community First Chief Executive		
Record details of alleged fraud including amount		
Fraud investigation file created		
Fraud Response Meeting		
Building Bridges Programme Manager to establish a Fraud Response Team. The membership of the team may vary depending on the seriousness of the suspected fraud but may include; • Community First Chief Executive • Community First Head of Finance • Community First Board members • Relevant CEOs and senior managers from partner organisations (as necessary) • Any relevant subject experts		
The Fraud Response Team should quickly determine; • Whether an investigation is necessary • Who will lead the investigation (Lead Investigator) • Any immediate need for Police involvement • Any immediate need for legal advice • Any need for media/PR advice • Any need to suspend staff, conduct searches and remove staff access • Any need to report the fraud externally (auditors, funders, etc.) • A timetable for the Lead Investigator to report back		
The objectives of the investigation should be documented and approved by the Fraud Response team. Objectives could include: • Identify the potential culprit(s) • Identifying potential witnesses • Establishing the facts surrounding the fraud or loss • Removing the threat of any further losses • Obtaining sufficient evidence for successful disciplinary, criminal or civil action		

Actions may need to be taken to prevent further losses and the Chief Executives of Community First and any relevant partner organisation should be consulted on any action relating to staff suspension and removal of access to IT and offices.		
Date of review agreed		
Lead Investigator Plan		
The Lead Investigator should prepare an investigation plan and submit this for approval. This should be short and show clearly what work/tasks need to be completed, by whom and when.		
The Plan may cover some or all of the following: • Co-ordination with all relevant partner organisations and other parties as necessary • identification and recording of the persons involved and facts of the case • handling internal and external communications • actions to prevent further losses • actions to secure and store evidence. Normally, evidence should be secured in a way that will be least likely to alert the suspect(s) or others • liaison with HR leads (Community First and partners) and dealing with those under suspicion • interviews to be conducted • timetables for involving the Police or other external experts • analysis of evidence • internal reporting (e.g. to Management Teams, Boards) • reporting to funders, auditors and regulatory/government bodies • target dates for reporting back to the Fraud Response Team		
Securing Evidence		
In securing and handling evidence it should be assumed that all evidence may need to be presented in court and should therefore be treated accordingly. (Even if criminal or civil action is not planned, it is sensible to adopt this approach). Normally, all evidence should be kept securely under lock and key, with access limited to those working on the investigation. A record should be maintained of anyone handling evidence.		

Evidence such as computer data, transferable media etc, should only be handled by suitably trained and skilled personnel. Where there is any doubt, professional/Police advice should be sought. Where evidence, or other relevant information, is to be shared with another body, careful consideration should be given to any data protection (confidentiality) requirements. Where there is any doubt, expert advice should be sought. Evidence can take different forms and will need to be handled in different ways.		
Original Documents Good practice for management of gathering original evidence documents includes: • handle as little as possible • put in protective folder and label the folder • do not mark in any way • assign responsibility to one person for keeping the documents secure • keep a clear record of how and where the documents were obtained • keep a record of anyone who subsequently handles the documents		
Computer Held Data/Transferable Media • keep secured in an appropriate environment • data should only be retrieved from computers by those who are technically qualified		
Photocopied Documents • in some cases it may be preferable or necessary to leave original documents in situ and take photocopies for further analysis and investigation • photocopies should be clearly marked as such • photocopies should be signed and dated, and certified as a true copy of the original		
External evidence • There are potential external sources from which evidence or information to support an investigation can be obtained, such as the tax authorities, supplier records, government registers of companies, donor records etc.		

Individuals Under Suspicion		
It should always be remembered that an allegation of fraud may be unfounded and in order to respect the individual(s) and ensure good working relations after an investigation, any action taken, such as suspension, and interviewing should be handled very carefully. Suspension from work is an opportunity to protect both the programme, partner organisation and individual, providing the necessary space and opportunity to plan the investigation, investigate the facts and speak to other people without the individual being present. It should be made clear that suspension is not a judgement. The key factors in deciding to suspend individuals will normally be prevention of further losses and removal or destruction of evidence. In some cases, it may be preferable to not suspend even at the risk of further losses (e.g. to gather further evidence). Any individual(s) under suspicion who are allowed to remain at work and/or involved in delivering the programme should be closely monitored. This may include: physical surveillance of movements, monitoring of IT usage, monitoring of telephone, email and internet usage etc. (Note: it is advisable to seek legal advice regarding the use of surveillance techniques, to ensure compliance with local laws such as the Regulation of Investigatory Powers Act in the UK). Other matters to consider include: • a review of staff or volunteer records (e.g. to check references, employment history, qualifications etc, but with due regard to any data confidentiality / protection requirements) • searching the suspect's work area; desk, cabinets, files, computer etc • restricting access by the suspect(s) to files, computers etc.		
Interviews and Statements		
When interviewing individuals under suspicion, it must be made clear whether it is a formal interview or an informal discussion. It should be explained that you have no pre-set view, the suspicion should be outlined and the individual given adequate time to respond. If it is decided that formal questioning is needed because involvement in a criminal offence is suspected, then the interview should be conducted in accordance with the principles of the UK Police and Criminal Evidence Act (PACE). Guidelines can be found on the Home Office Website. PACE provides protection for the individual and ensures that any evidence collected through interviews, (including the taking of statements) can be presented in court whether or not such interviews are being carried out		

under caution. PACE covers such rights as the right to silence, to legal advice, not to be held incommunicado, to accurate recording and protection against evidence obtained through oppression. If necessary, seek legal/Police advice. (Where local legislation is more applicable then this should be referred to and followed). Interviews should only be carried out with the approval of senior management and/or the Fraud Response Team. Early consideration should be given to Police involvement, or consultation. There are strict rules relating to tape recorded interviews and investigators must be suitably skilled and experienced, where these are used. Ideally, statements should be taken from witnesses using their own words. The witness must be happy to sign the resulting document as a true record – the witness can be given a copy of the statement if desired. It is very important to keep contemporaneous notes on file, in the event that they are needed for future reference (e.g. court, tribunal, disciplinary hearing). Such notes should always show: date of interview; time started; time finished; and, be signed and dated by the interviewer.		
Police Involvement		
At some point a decision will need to be made as to whether the case is reported to the Police. For large-scale frauds, it may be appropriate to ask the Police to attend meetings of the Fraud Response Team. The Lead Investigator should prepare an "Evidence Pack" that can be handed to the Police at the time the fraud is reported. The Evidence Pack should include a summary of the fraud, highlighting (where known) the amount, the modus operandi, and the location, and including photocopies of key supporting documents and contact details of the Lead Investigator. Remember to keep a photocopy of everything that is handed to the Police. All contact with the Police should be channelled through one person (i.e. the person leading the investigation). A record should be maintained of all contacts with the Police, the details of the officers, and the crime reference number. The Police have knowledge of similar cases of fraud and their advice should be sought regarding measures to prevent further losses or future incidents.		
Prevention of Further Losses		

Once actual or potential losses have been identified, it is important that effective and timely action is taken to prevent further losses. It may, however, be decided that a better standard of evidence can be obtained by allowing limited further losses. The Lead Investigator should, at an early stage in the process, complete a preliminary assessment of the potential for further losses and how best to prevent them. They should make recommendations to senior management within the Programme team, The Fraud Response Team, Community First and relevant partner organisations as to what if any immediate actions are necessary. Actions taken at an early stage may have to be circumspect so as not to alert suspects who have yet to be suspended or cautioned. It may also be important not to lose or compromise the forensic value of data by precipitate action. It may nevertheless be necessary to act quickly e.g. to stop salary payments to suspects who are to be dismissed. As the investigation continues, and more information emerges, further recommendations for action may be needed. At the end of the investigation the Building Bridges Programme Manager and the Fraud Response Team should review all the actions taken to prevent further losses and to report on this in the Review of Findings.		
Recovery		
Once the identity of the perpetrator (s) and the scale/size of the fraud has been determined, the programme management team, Community First and any relevant partner organisations must consider whether or not any of the loss can be recovered and take any further action that is necessary. This may require advice from the relevant organisations' insurers		
Reimbursement offered during the investigation An individual may, in the course of an investigation, offer to repay the amount that has been obtained improperly. The Lead Investigator should neither solicit nor accept such an offer (as it may be construed as having been obtained under duress). The Lead Investigator should record any offer made and refer it to the Fraud Response Team.		
Reimbursement offered during disciplinary or legal proceedings If an offer of restitution is made while disciplinary or legal proceedings are still under way, the Lead Investigator and Fraud Response Team must seek legal advice before such an offer is accepted.		
Reimbursement after completion of disciplinary proceedings		

Where a member of staff or volunteer is to be dismissed, their line management, in co-ordination with the Lead Investigator and Fraud Response Team should consider recovery of amounts due from any outstanding salary or expense payments. It will be necessary to take legal advice about the right to do this as it is unlikely to be clear in the member of staff's or volunteer's contract of employment. **Court Order** Where a criminal case is taken against an individual, a formal claim for restitution (where the court orders the defendant to give up gains) should be made through the Police. Any monies due will be recovered via a Court Order.		
Civil Action Funds lost due to fraud can be recovered from the perpetrator by suing them for damages in a civil court. The level of proof required in civil cases is lower than that required in criminal cases and management may regard a civil action as a more effective use of their time than trying to persuade the Police to investigate and the courts to prosecute. If this approach is successful the perpetrator will also have to pay any necessary legal costs for the Building Bridges Programme, Community First and/or the relevant partner organisation. A civil action can still be brought even if a criminal prosecution has failed. If a criminal prosecution is successful a civil action may be necessary to force the person convicted to repay the sums stolen. It is important to remember that the person being sued may be unable to make the repayment. In situations in which repayment is unlikely, the Fraud Response Team approval should be obtained before additional legal costs are incurred		
Commercial Negotiation Where the fraud has been committed by the employee of a contractor or supplier, all or part of the loss may be recoverable from the business concerned. It may be possible to reach an agreement that the loss can be deducted from any outstanding debts or that additional goods/services will be supplied free of charge. Third parties may want to agree a negotiated settlement in order to retain the goodwill of their customer and/or to avoid damaging publicity and legal costs. They may subsequently be able to recover these costs from their employees or their insurers		
Insurance		

The relevant insurers should be informed as soon as a suspicion is raised. In certain circumstances it may be possible, to make a claim against the insurers. The Lead Investigator should provide the insurers with any information that is required to substantiate a claim, or to support an attempt by the insurers to secure recovery from the perpetrator.		
Administration		
Careful administration of the investigation is of vital importance. A disordered investigation, without clear records and logs of events, communications, key dates etc, will cause problems at any court hearing, employment tribunal, or disciplinary panel. It is therefore important to: • Maintain a chronological record of all events on a main file. This should include all correspondence, telephone calls and emails made and received, interviews, visits, tests/checks undertaken etc. • Maintain a list of all contacts (e.g. internal, Police, charity commission, lawyer, funders, peer organisations, government bodies, technical advisers). • Maintain a list of emergency contact numbers and ensure that this is shared with all those on the list (e.g. Chief Executive). • Maintain a log of anyone who handles evidence obtained, including the Police. • Consider whether there is a need for: dedicated administrative support; dedicated phone and email address. • Do not keep any unnecessary records or copies. Carefully shred any papers that are not needed (e.g. extra copies of progress reports). • Establish internal and external communication protocols. Discourage the use of email to communicate sensitive information; avoid internal mail and hand deliver highly confidential information, opting for double-enveloped post for less sensitive information. Where email is used for communication, consider entering subject names that have no direct link to the investigation. • Provide update reports as appropriate		
Reporting		
Every investigation of suspected fraud or financial irregularity should result in a report written by the Lead Investigator. This should be done regardless of whether any members of staff are dismissed or prosecutions made. The report will record, the scale of the fraud, when and how it was perpetrated and by whom. In addition the report will record; what action has been taken against the perpetrator, the actions to prevent further similar losses and to recover what has been lost. It will also usually be		

pertinent to note how the fraud was detected and whether or not existing controls were effective. The report will be issued to the Fraud Response Team and any relevant Board members for Community First and partner organisations. A copy should also be made available to the External Auditors and Funders. Since the report may be used internally for disciplinary hearings or externally for civil or criminal proceedings, conclusions and opinions should be substantiated by evidence and any defamatory statements should be avoided. It is important to strictly limit the distribution of the report. Copies will not be provided automatically to suspects or their representatives. If a disciplinary hearing takes place the individual and their representative may be entitled to receive a copy subject to obtaining legal advice.		
Review, Communication and Action on Findings		
Review of findings The findings reported by the Lead Investigator should be reviewed by the Fraud Response Team and in particular the lessons learned to avoid future frauds. If the fraud was significant the findings should be discussed by the Boards of Community First and any relevant partner organisations. The Fraud Response Team should satisfy themselves that, so far as is practically possible, a similar fraud could not occur again and /or the amount of potential loss has been minimised, the perpetrators have been properly dealt with and recovery has been pursued robustly. The Chief Executives of Community First and the relevant partner organisations must also consider how managers should be disciplined if they have not properly enforced existing controls and procedures.		
Communicating Outcomes Responsibility for communicating findings and actions to those involved and others who need to know should be set out by the Lead Investigator in the Plan. It may be necessary to manage the expectations of the person who raised concerns. The Building Bridges Whistleblowing Policy provides guidance on what may be communicated		
Action on Findings Any actions arising from the final report should be allocated by the Lead Investigator to named individuals with appropriate due dates for completion.		

The final details of the fraud should be recorded in line with the advice from the auditors, funders and Police.		
Closure		
Communication that the case has been closed It is important that any decision to close the case is clearly documented and communicated to those involved by the Lead Investigator. The case may be closed for a number of reasons, including : • All action points that arose from the final report have been completed • The Fraud Response Team decides there is insufficient evidence to support the allegations • The Building Bridges Programme, Community First and/or the relevant partner organisations do not wish to incur further costs investigating the case The decision to close the case and the reason for doing so should be documented by the Lead Investigator and should be added to the investigation file.		
Archiving All documents associated with the investigation should be archived in a secure location with adequately restricted access. Any redundant documents and papers, or duplicate copies, should be carefully shredded.		

Appendix 2 - Examples of Fraud

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

- Misappropriation of funds
- Misuse of assets, including cash, stock and other assets, for example “borrowing” petty cash, use of photocopiers for private purposes
- Theft from a client or supplier
- Theft of intellectual property (e.g. unauthorised use of programme and organisation name/logo, theft of product/software designs and participant or other confidential data.

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.

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 programs designed to generate credit card details that are then used to commit or facilitate fraud
- undeclared and unauthorized 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 Wiltshire and Swindon Sport 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)

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.

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.

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.

Appendix 3 - Examples of Controls to Prevent and Detect Fraud

Good examples of controls that can be put in place to prevent and detect fraud include:

- thorough recruitment procedures
- physical security of assets
- clear organisation of responsibilities and reporting lines
- adequate staffing levels
- supervision and checking of outputs
- 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 auditors

Appendix 4 - Warning Signs for Fraud

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

- appearing to be 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
- a person who is disgruntled at work or not supportive of the organisation's mission

Fraud Indicators can include:

- staff exhibiting unusual behaviours (see list above)

- key documents being missing (invoices, receipts, contracts, etc.)
- 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