ANTI-FRAUD POLICY AND FRAUD RESPONSE PLAN

Part 1: ANTI-FRAUD POLICY

1. Policy Statement

GALVmed is committed to the prevention of fraud and will uphold all applicable laws relevant to countering fraud in all the jurisdictions in which it operates. It welcomes the international community's efforts to stamp out fraud. GALVmed seeks to reduce the opportunity for fraud and will take prompt action to investigate fully and address any suspected cases.

2. Policy Purpose

The purpose of this Policy is to:

- set out GALVmed's responsibilities in observing and upholding its Policy on fraud;
- provide information and guidance to GALVmed employees, partners, agents and consultants and other connected parties on how to recognise and deal with fraud issues; and
- establish standards of conduct for GALVmed employees and connected parties to ensure that the relevant legislation is not violated.

As a UK registered charity GALVmed remains bound by the laws of the UK, including the Fraud Act 2006 and the Bribery Act 2010, in respect of its activities both at home and abroad.

This Policy is supplemented by the Fraud Response Plan (see Part 2) which establishes a framework for investigating and responding to any such events.

This Policy and the Fraud Response Plan form part of a series of related GALVmed policies and procedures developed to provide sound internal financial controls and to counter any fraudulent activity. These include: codes of conduct for staff and trustees; Anti- Bribery Policy; Safeguarding Policy; sound internal control systems; public interest disclosure (whistleblowing) procedures; and training.

GALVmed considers a breach of this Policy to be a serious violation which may result in disciplinary measures, including the dismissal of employees or the termination of its business relationship with any third party.

3. Scope

This Policy applies to all GALVmed's staff and anyone working in any capacity with GALVmed, including employees, Trustees, consultants, agents, partners or other persons or organisation who may represent GALVmed from time to time, within the UK and overseas. The Policy is provided to other partners and associates, who are required to take reasonable steps to ensure that, in carrying out activities supported by GALVmed, they and their directors, officers, employees and associates comply with all applicable anti-fraud laws.

4. Definition of Fraud

Fraud is a form of dishonesty, involving false representation, failing to disclose information or abuse of position, undertaken to gain or cause loss to another. Fraud may be carried out by someone connected to GALVmed, as well as a crime committed by entirely external individuals or entities.

The term is used to describe such acts as deception, bribery, forgery, extortion, corruption, theft, conspiracy, embezzlement, misappropriation, false representation, concealment of material facts and collusion (further examples are provided in Appendix 2).

Fraud can be committed in various ways including the following:

- False representation - false representation with the intention of making a gain or causing loss or risk of loss to another. The gain or loss does not actually have to take place. It can be stated in words or communicated by conduct;
- Theft – removal or misuse of funds, assets or cash, including physical or intellectual property;
- False accounting - 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 the intent to cause loss to GALVmed, or furnishing information, which is or may be misleading, false or deceptive;
- Abuse of position – abusing authorities and misusing GALVmed resources or information for personal gain or causing loss to GALVmed. This applies to situations where someone is put in a privileged position and by virtue of that position is expected to safeguard another's interests or not act against those interests;
- Failing to disclose information – failing to disclose information to another person where there is a legal duty to do so;
- Misuse of equipment – deliberately misusing materials or equipment belonging to GALVmed;
- Cybercrime – an umbrella term for crimes which take place online or where technology is a means and/or target for the attack.

Under the Fraud Act 2006, fraud is punishable for individuals by up to 10 years' imprisonment and if GALVmed was found to have committed an offence, it could face an unlimited fine, be excluded from tendering for public contracts, and face damage to its reputation. It therefore takes its legal responsibilities very seriously.

5. Responsibility for Fraud Prevention

GALVmed will 1) manage the risk of fraud by promoting an anti-fraud culture and developing and maintaining effective controls to prevent fraud; and 2) in the event of fraud or suspected fraud carry out prompt and thorough investigations and take appropriate legal and/or disciplinary action.

It is the contractual duty and responsibility of all *Employees, Trustees and Associated Parties* to:

- act with propriety at all times, in particular in the use of GALVmed resources;
- be alert to the possibility of fraud and take special care where unusual events or transactions occur; and
- report immediately if they suspect fraud is taking or has taken place through the Whistleblowing Policy if necessary.

Under UK law, the *Board of Trustee*s have a legal duty and responsibility to safeguard GALVmed's money and assets and to act prudently; avoid undertaking activities that may place its funds, assets or reputation at undue risk; and must take all necessary steps to ensure there is no misuse of funds or assets.

The Finance and Risk Committee, on behalf of the Board, is responsible for ensuring procedures for preventing fraud are in place; monitoring the executive, operation and effectiveness of anti-fraud arrangements; and reviewing all reported circumstances of fraud, considering actions taken and report any serious incidents as necessary.

The *Chief Executive Officer* carries overall responsibility for implementing the Policy. This responsibility is delegated to the *Senior Director of Finance & Corporate Services* who has day-to-day responsibility for implementing this Policy and monitoring its use and effectiveness.

Managers at all levels are responsible for ensuring those employees or others reporting to them are made aware of and understand the Policy. They are also responsible for ensuring that effective internal control systems are in place and operating to minimise the potential for fraud.

The prevention, detection and reporting of fraud is the responsibility of all *individuals* working for GALVmed. You must ensure that you read, understand and comply with this Policy. You are required to avoid any activity that might lead to, or suggest, a breach of this Policy.

Detailed responsibilities in relation to fraud prevention are found in Appendix 1.

Any queries on the Anti-Fraud Policy or Fraud Response Plan should be raised with the Senior Director of Corporate Services & Finance.

6. Breach of Anti-Fraud Policy

Any employee who breaches this Policy will face disciplinary action, which could result in dismissal for gross misconduct. GALVmed also reserves the right to terminate its contractual relationship with its partners, and associates if they breach this Policy.

Should you believe or suspect that a conflict with this Policy or the Fraud Act has occurred or may occur in the future you must report your concerns to your Line Manager and/or in accordance with the Fraud Response Plan (see Part 2). At no time and under no circumstances should you voice any suspicions to the person(s) whom you suspect, otherwise, you may commit a criminal offence of "tipping off". You are encouraged to raise concerns about any issue or suspicion of malpractice at the earliest possible stage. If you are unsure whether a particular act constitutes fraud it should be reported. All matters will be dealt with in confidence and in accordance with GALVmed's Whistleblowing Policy. Examples of fraud warning signs are included in Appendix 3.

GALVmed will promptly and vigorously investigate all cases of actual or suspected fraud and take appropriate action. In the case of proven, or suspected, fraud of a serious nature, GALVmed may refer the matter to the police. The circumstances of individual frauds will vary, however GALVmed takes all fraud very seriously.

Any employee who breaches this Policy will face disciplinary action, which could result in dismissal for gross misconduct. If a trustee or associated party are found to have committed a breach of this Policy, it could lead to termination of the directorship or contractual relationship.

7. Record Keeping

GALVmed must keep financial records for six years and have appropriate internal controls in place which will evidence the business reason for making payments to third parties.

All accounts, invoices, memoranda and other documents and records relating to dealings with third parties, such as clients, suppliers and business contacts, should be prepared and maintained with strict accuracy and completeness. No accounts must be kept "off-book" to facilitate or conceal improper payments.

8. Protection

Employees who raise concerns or report another's wrongdoing are sometimes worried about possible repercussions. GALVmed is committed to ensuring no one suffers any detrimental treatment as a result of refusing to take part in fraud, or because of reporting in good faith their suspicion that an actual or potential fraudulent act has taken place or may take place in the future. Statutory protection of whistle blowers is afforded under the Public Interest Disclosure Act 1998 (see Whistleblowing Policy for further details).

9. Policy Communication

GALVmed's zero-tolerance approach to fraud will be communicated to all partners, associates, suppliers, and contractors at the outset of its relationship with them, through this document and as appropriate thereafter.

All employees will receive fraud awareness training upon commencement of employment. Annual refresher training will be provided to all employees. The Policy and Fraud Response Plan will be provided to employees yearly. It will also be provided to Trustees and other parties working on behalf of GALVmed.

10. Risk Assessment, Monitoring & Review

As part of its annual risk assessment process the FRC will monitor the effectiveness and review the implementation of this Policy, considering its suitability, adequacy and effectiveness. The Senior Director of Corporate Services & Finance will carry out regular reviews of GALVmed's control systems and procedures to provide assurance that they are effective in countering fraud.

Part 2: FRAUD RESPONSE PLAN

1. Introduction

The purpose of this plan is to define authority levels, guidelines for action, and reporting lines in the event of a suspected fraud.

The Fraud Response Plan ensures that timely and effective action can be taken to:

- minimise occurrence of fraud by taking rapid action at the first signs of a problem;
- define responsibilities for action and reporting lines;
- identify the fraudsters and maximise the success of any disciplinary/legal action taken;
- prevent losses of resources or other assets where fraud has occurred and to maximise recovery of losses;
- identify any lessons which can be acted upon in managing fraud in the future;
- reduce adverse impacts on the business of GALVmed.

2. Responsibilities of Staff to Report Suspicions of Fraud

- **Reporting Incident:**

As soon as possible report suspected incidents of fraud. All matters will be dealt with in confidence and in accordance with GALVmed's Whistleblowing Policy. This Policy enables you to raise concerns about any financial, or other, malpractice in GALVmed without fear of being subject to victimisation or discrimination.

In the first instance you should protect GALVmed's assets by taking steps to minimise any immediate further loss without alerting the suspects(s), then report any suspicion of fraud to your manager as a matter of urgency. If this line of reporting is inappropriate you should report your concerns upwards in order of the following authority hierarchy:

- your Line Director
- Senior Director of Corporate Services & Finance
- Chief Executive Officer
- Finance & Risk Committee Chair (FRC)

As soon as an assertion of suspected fraud is reported to a manager, the manager must inform the Senior Director of Corporate Services and Finance, who will then inform the Chair of the FRC.

If fraud is perceived to be wide-spread or occurring at Board level the suspicion must be reported to GALVmed's external auditors.

- **Record:**

Secure and retain all evidence and record all relevant details, such as the nature of your concern, the names of parties you believe to be involved, details of any telephone or other conversations with names, dates and times and any witnesses. Notes do not need to be overly formal, but should be timed, signed and dated. Timeliness is most important to ensure accuracy and a more effective investigation.

- **Keep the matter confidential:**

Do not discuss it with any other colleagues or external party either before or after reporting it to the appropriate person. Spreading unsubstantiated concerns may harm innocent persons or the organisation. Any conversations and information given by the informer of fraud suspicions will, as far as possible, remain confidential. You may be asked to give a written statement that could be used if the fraud becomes a criminal investigation.

- **Do not investigate the matter yourself:**

Do not rush in. Establish as many facts as possible without alerting anyone and report your suspicions. If an individual or a manager has grounds for suspecting that a member of staff may be involved in fraudulent activity (e.g. a false travel expenses claim) they *should not* interview the member of staff without first seeking guidance from the Senior Director of Corporate Services & Finance. There are special rules relating to the gathering of evidence for use in criminal casesAny attempt to gather evidence by persons who are unfamiliar with these rules may undermine the case.

It is key that the creator and those receiving this report do not discuss the content of this report with anyone believed to be involved in the suspected activity described. To do so may constitute a "tipping off" offence, which under the Proceeds of Crime Act 2022 carries a maximum penalty of 5 years' imprisonment.

3. Investigation

a. Initial Investigation

The Senior Director of Corporate Services & Finance will conduct an initial fact-finding investigation to establish the substance of the allegation. This investigation is only to assess the evidence and determine whether the suspicion is reasonable i.e. not malicious or based on a clear misunderstanding/lack of knowledge. This enquiry should be carried out as quickly as possible after suspicion has been aroused, as prompt action is essential.

b. Investigating Group

If the allegation is substantiated, the Senior Director of Corporate Services & Finance will directly convene a group for further investigation ("The Investigating Group") of the following people to decide on the initial response:

- The Senior Director of Corporate Services & Finance, as nominated chair who shall chair the investigation and take charge on a day-on-day basis;
- Manager to whom the fraud was reported;
- Others as determined by the Chair, e.g. CEO, other GLT members, managers, legal or IT experts.

All allegations and reports of fraud will be investigated. The remit, responsibilities, scope of investigation and reporting deadlines should be established. The scale and format of the investigation will be determined by the Investigating Group.

c. Investigation Process

The matter should be investigated thoroughly and as quickly as possible. The Chair should ensure there are sufficient resources to carry out the review and that full access to staff, data and documentation is available. If necessary, external specialist investigative forensic auditors and legal experts may be appointed to carry out the investigation.

All interviews should be conducted in a fair and proper manner. Interview notes should be signed by all parties as an accurate record of the interview. Disciplinary procedures should be followed at all times.

The Investigating Group will consider whether it is necessary to investigate systems other than that which has given rise to suspicion, through which the suspect may have had opportunities to

misappropriate GALVmed's assets. They will also consider legal implications and whether it is necessary to inform the police.

Regular progress meetings should be held at which progress and agreed actions are documented.

d. Reporting Process

The Investigating Group should maintain a full record of the investigation which should be prepared as the investigation proceeds. This should include a chronological record of all evidence gathered including includes telephone conversations, discussions, meetings and interviews (with whom, who else was present and who said what), details of documentation reviewed, tests and analysis undertaken, the results and their significance. Everything should be recorded irrespective of the apparent insignificance at the time. These records should be maintained for six years following the conclusion of the investigation.

Throughout any investigation the Investigating Group Chair will keep the Chief Executive Officer informed of progress and any developments. The FRC and Board should also be informed. If the investigation is long or complex, interim reports to the FRC and updates to the Board should be made. These reports may be verbal or in writing but should be recorded in the written report of the Investigation. If fraud is discovered to have caused a loss to the organisation disclosure should be made to the Charities Commission/OSCR, as well as to auditors, funders and insurers.

e. Investigation Evidence

It is important, from the outset, to ensure that evidence is not contaminated, lost or destroyed. The Chair of the Investigating Group will therefore take immediate steps to secure physical assets and all potentially evidential documents. All original documentation must be preserved in a safe place for further investigation.

Evidence may take various forms, including documents, computer held data, cash, assets or video evidence. Evidence should not be accessed by anyone not appropriately trained or not part of the Investigating Group. Cash and assets should be counted by two people (preferably in the presence of the Chair of the Investigating Group) and a statement confirming the amount of cash held/assets should be signed by both parties present as a correct record.

f. Prevention of Further Loss

If there is thought to be any possibility of ongoing or recurring fraud, then action should be taken to prevent further losses, including suspending or recalling BACS payments.

Where there are reasonable grounds for suspicion of an employee, to facilitate the investigation it may be appropriate to suspend the employee against which the accusation has been made on full pay. The Chief Executive Officer will take this decision, in consultation with the Chair of the Investigating Group and the Associate Director of HR. Suspension will not be regarded as disciplinary action, nor will it imply guilt.

In these circumstances, where possible the suspect(s) should be approached unannounced and should be interviewed about the allegation prior to being informed of their suspension. Access to GALVmed's systems should be suspended immediately and they should be supervised at all times before leaving GALVmed's premises. They should be allowed to collect personal property under supervision but should not be able to remove any property belonging to GALVmed.

Any security passes and keys to premises, offices, and furniture should be returned. Laptop computers, mobile phones and associated hardware/software must also be returned. Excellimore should be instructed to immediately withdraw access permissions to GALVmed's computer systems.

g. Press and Publicity

The Chief Executive Officer, in conjunction with the Senior Communications Manager, and the Investigations Group will handle the press and publicity in all matters regarding fraud and corruption.

If any member of staff speaks to the press without the express authority of the Chief Executive Officer, it will be regarded as a breach of Employee Terms and Conditions of Service.

h. Investigation Findings

Once the investigation is completed, a report should be prepared which includes:

- Background to how the need for the investigation arose;
- What action was taken in response to the allegations;
- How the investigation was conducted;
- The facts that came to light during the investigation and the evidence in support;
- Action taken against any party where the allegations were proved;
- Action taken to recover any losses;
- Review of, and amendments to, existing controls; and
- Recommendations and/or action taken to reduce further exposure or to minimise any recurrence.

The findings of the investigation will be reported to the Chief Executive Officer, who will determine, in consultation with the Chair of the Investigating Group, what further action (if any) should be taken. Investigation findings and interviews will be used in the event of any disciplinary proceedings against an employee which will be conducted in accordance with the Staff Handbook. The fraud perpetrator may be the subject of a criminal investigation.

i. Recovery of Losses

Recovery of losses is a major objective of any fraud investigation and GALVmed will take appropriate steps, including legal action if necessary, to recover any losses arising from fraud, theft or misconduct.. The Investigating Group will ensure that, in all fraud investigations, the amount of any loss is quantified. Where the loss is substantial, legal advice may be obtained including potential action against third parties involved in the fraud or whose negligent actions contributed to the fraud.

j. Senior Management

If the allegations of fraud relate to any member of the GLT, the Chair of the FRC should be informed immediately. The Chair of the FRC will then convene and Chair the Investigating Group. No members of the GLT should be on the Investigating Group to avoid conflict of interest.

4. Completion

On completion of the investigation, a written report should also be submitted to the FRC and Board of Trustees containing a description of the incident, including the value of any loss; the people involved; the means of perpetrating the fraud; the measures taken to prevent a recurrence; and any action needed to strengthen future responses to fraud, with a follow-up report on whether the actions have been taken.

5. Review

The Anti-Fraud Policy and Fraud response plan will be reviewed every year, or after any occasion of fraud has been identified.

Version Control

Date	Activity
January 2010	Policy adopted
March 2012	Policy reviewed by FAC. No changes.
September 2016	Policy refined. Minor title changes. Full review & re-launch due.
March 2017	Significant refinement further to Finance & Audit Committee review.
September 19 & 20 & November 21	Policy refined. Minor title changes.
May 2022	High level review. No changes
August 2024	Significant review to update Fraud Response Plan to remove flexibility, add cyber fraud and indicators of fraud, and tipping off

APPENDIX 1 Responsibilities – Detailed

The *Board* delegates authority for its responsibilities for fraud to the *FRC*:

- To ensure an Anti-Fraud Policy is in place and provide an oversight and audit of its execution; and
- To ensure the Charities Commission/OSCR are advised as appropriate on fraud which results in a loss to the organisation.

The *Chief Executive Officer* carries overall responsibility for the prevention of fraud. They are liable to be called to account by the Board and Donors for specific failures. They are responsible for:

- Establishing and maintaining a sound system of internal control that supports the achievement of GALVmed's aims, objectives and policies. The system of internal control is designed to respond to and manage the whole range of risks that GALVmed faces by identifying the principal risks, evaluating the nature and extent of those risks and managing them effectively;
- Taking appropriate legal and/or disciplinary action against perpetrators of fraud.

Overall responsibility for day-to-day management of the risk of fraud is delegated to the *Senior Director of Corporate Services & Finance*. They are responsible for:

- Maintaining an effective fraud Policy and fraud response plan;
- Liaising with the Charity's appointed Auditors and Charity Commission/OSCR;
- Designing and implementing an effective control environment to prevent, and detect, fraud;
- Establishing appropriate mechanisms for reporting fraud risk issues and incidents of fraud to the Chief Executive Officer and FRC Chair as required;
- Making sure that all staff are aware of GALVmed's Anti-Fraud Policy and know what their responsibilities are in relation to combating fraud;
- Ensuring that appropriate anti-fraud training is available to all staff;
- Ensuring that prompt and thorough investigations are carried out if fraud occurs or is suspected, as Chair of the Investigating Group;
- Taking appropriate action to recover assets;
- Ensuring that appropriate action is taken to minimise the risk of similar frauds occurring in future.

Management has day-to-day responsibly for the prevention and detection of fraud:

- Ensuring that an adequate system of internal control exists within their areas of responsibility which minimise the opportunities for fraud and that these controls operate effectively;
- Assessing the types of risk involved in the activities, systems and procedures for which they are responsible;
- Preventing and detecting fraud;
- Reporting any suspicions of fraud to the Senior Director of Corporate Services & Finance;
- Regularly reviewing and testing the control systems for which they are responsible;
- Ensuring that controls are being complied with and systems continue to operate effectively;
- Implementing new controls to reduce the risk of similar fraud occurring where frauds have taken place.

Every member of staff is responsible for:

- Acting with propriety in the use of business resources and the handling and use of funds whether they are involved with cash or payments systems, receipts or dealing with suppliers or assets management;
- Conducting themselves in accordance with the following principles - integrity, objectivity, accountability, openness and honesty;
- Being alert to the possibility that unusual events or transactions could be indicators of fraud;
- Alerting their manager when they believe the opportunity for fraud exists e.g. because of poor procedures or lack of effective oversight;
- Reporting details immediately through the appropriate channel if they suspect that a fraud has been committed, or see any suspicious acts, without informing the suspected person or persons about their suspicions or reporting of their suspicions
- Cooperating fully with whoever is conducting internal checks or reviews or fraud investigations.

APPENDIX 2 Examples of Fraud

Theft - the illegal taking of someone else's property without that person's freely-given consent. It includes:

- Theft of physical assets such as computer equipment (peripherals and equipment);
- Misappropriation of funds;
- Misuse of assets, including cash, stock and other assets, for example “borrowing” petty cash;
- Theft from a partner or a supplier; and
- Theft of intellectual property (e.g. unauthorised use of GALVmed’s name/logo & theft of data).

Bribery (see Anti-Bribery Policy) - is the offering, promising, giving, accepting or soliciting of money, gifts or other advantages as an inducement to do something that is illegal or a breach of trust in the course of carrying on an organisation’s activities.

Corruption (see Anti-Bribery Policy) - is influencing someone to act, in the belief that they will probably do so primarily in return for an advantage directly or indirectly.

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 unauthorised private and consultative work;
- money laundering (see below); and
- providing misleading information to donors (e.g. overstating activity) in order to obtain funds.

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 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.

Cyber Crime - an umbrella term for crimes which take place online or where technology is a means and/or target for the attack, including:

- Ransomware attacks – a type of malicious software designed to block access to a computer system until a sum of money is paid;
- Phishing scams – emails sent by fraudsters seeking to obtain sensitive information such as passwords, usernames, bank details or other financial information by electronic means, from seemingly trustworthy sources; and

- Spear phishing scams – emails sent by fraudsters which appear to have been sent by a senior person within an organization instructing an employee to transfer funds or provide sensitive information.

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 recognised 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 traveller's 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.

There are also two secondary offences connected with money laundering failure to disclose any of the primary offences and tipping off. Tipping off is where someone informs a person or people who are, or are suspected of being involved in money laundering, in such a way as to reduce the likelihood of their being investigated or prejudicing an investigation.

APPENDIX 3 Fraud Warning Signs

Whilst by no means being proof alone, the circumstances below may indicate fraud, and should be treated as a warning sign:

- Emails that are out of character for the sender with instructions to make payments or disclose information, often with a sense of urgency;
- Business emails sent from a personal email account;
- Unusual discrepancies in accounting records and unexplained items on reconciliations;
- Financial documents - such as invoices, credit notes, etc. – provided as photocopies rather than originals, or frequently contain alterations or deletions. This might indicate counterfeit or falsified documents being used to support bogus account entries;
- Suppliers regularly submitting invoices electronically in non-PDF format that can be altered;
- Unexplained variances from agreed budgets or forecasts;
- Misdescription of purchase and expense items in the accounting system;
- Inconsistent, vague or implausible responses to reasonable and legitimate queries about the accounts or accounting records, and/or queries being left unexplained, or taking a long time to resolve;
- Reluctance by a member of staff involved in handling finances to accept assistance or over-protectiveness of work;
- Single member of staff with control of a financial process from start to finish with no segregation of duties;
- Member of finance staff working unsociable hours or working from home without reason, and a reluctance to take holidays;
- Sudden changes to the format of financial information presented to the Board of GLT which make them complicated or difficult to understand.